Government Business Council

BROCADE

A NEW NETWORK ACQUISITION MODEL FOR THE FEDERAL GOVERNMENT

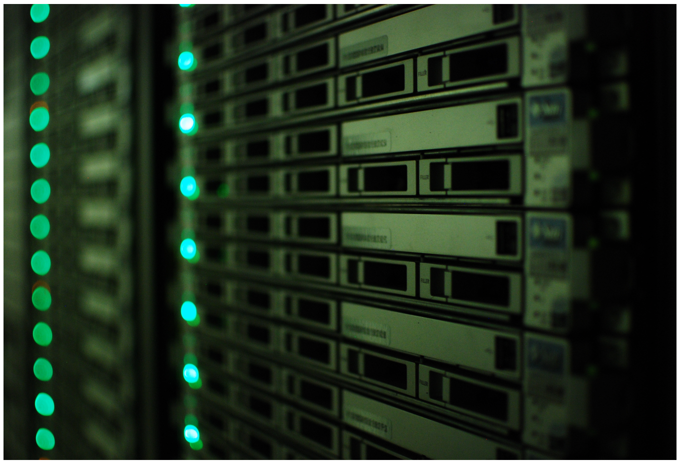
FEDERAL AGENCIES TODAY FACE A STRATEGIC INFLECTION POINT IN HOW THEY MANAGE ENTERPRISE OPERATIONS.

On one hand, the pressures to cut costs and operate more efficiently are as intense as ever. On the other, increasingly dynamic operational environments, both domestically and internationally, demand that agencies become more agile to achieve their missions. President Obama's Fiscal Year 2015 budget request succinctly sums up this dual challenge, claiming it will "maximize the value of every taxpayer dollar while increasing productivity and the quality of services throughout," all while decreasing funding for 13 major agencies.[1] How agencies approach these compounding challenges will have long-lasting effects on their ability to achieve their missions.

At the core of both the efficiency and agility imperatives is the IT network agencies rely on to operate. It is becoming increasingly clear that maintaining current network infrastructures is more costly than many believe. Moreover, as agency operations depend more and more on their ability to access and leverage IT networks, achieving mission will require agile and flexible networks. A different approach to network acquisition, known as Network-as-a-Service, offers a new way forward.

The True Cost of Network Ownership

Federal IT spending has stagnated over the past several years. From FY 2001 to FY 2009, federal IT spending had a compound annual growth rate



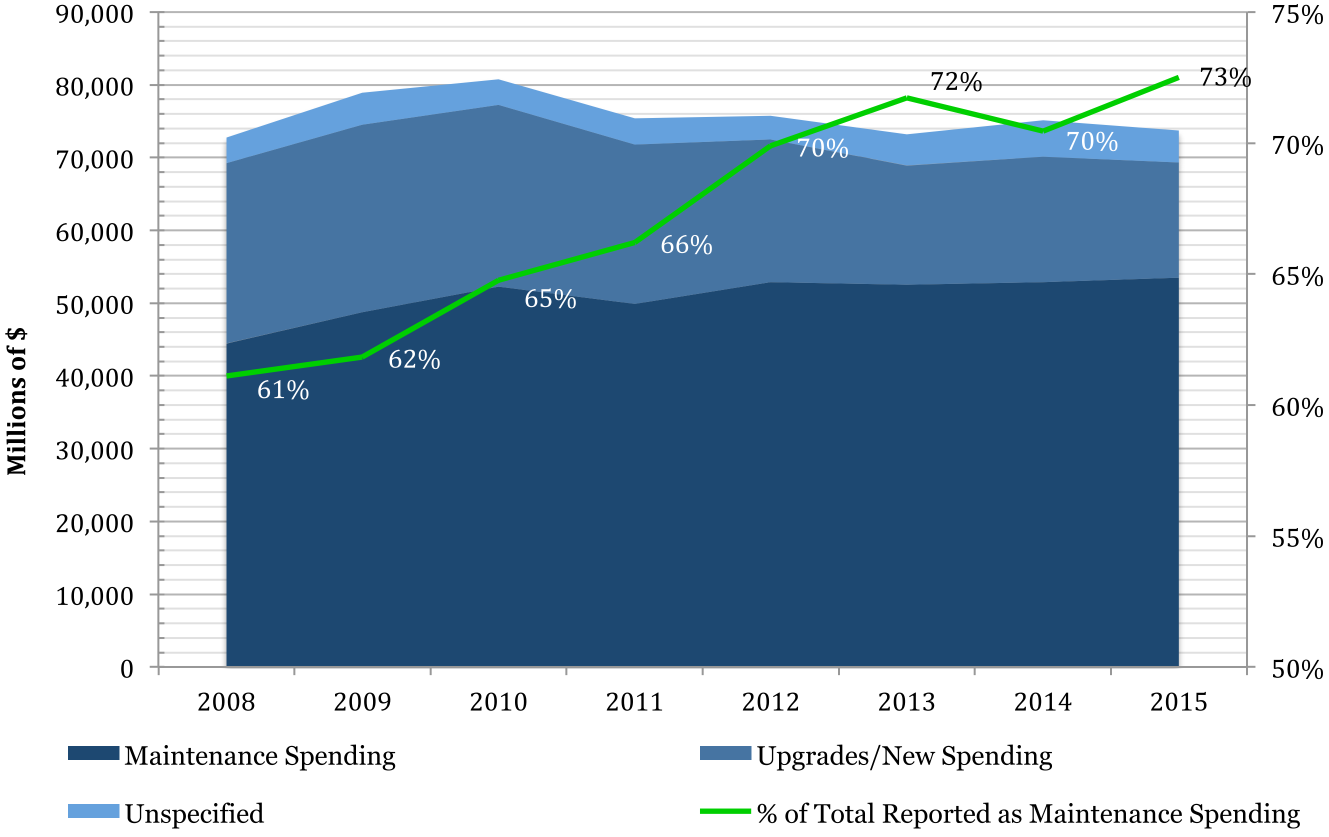
of 7.09 percent. Over the last five years, this rate has fallen to just 0.78 percent.[2] For FY 2015, the President's budget shrinks spending to $79 billion from $81.4 billion in FY 2014.[3] As expectations for federal IT continue to rise while budgets do not, agencies will face pressure to realize efficiencies.

AT THE CORE OF BOTH THE EFFICIENCY AND AGILITY IMPERATIVES IS THE IT NETWORK AGENCIES RELY ON TO OPERATE.

For many, the first step is evaluating the true cost of IT network ownership.

Most of what agencies spend on IT goes to maintaining the status quo. A recent Government Accountability Office analysis found that agencies spent $59 billion on operating and maintaining systems in FY 2014, $30 billion of which is spent on upkeep for "steady state" (i.e., legacy) systems.[4] However, this figure only includes maintenance spending for IT infrastructure, or support for common user systems, security, computing infrastructure, and IT capital planning, and may therefore understate the true cost of maintaining legacy systems.

Percentage of Total Federal IT Spending* Reported as Maintenance Spending, FY 2008-2015



*Not including classified DoD IT spending (approximately $6 billion per year)

Source: ITDashboard.gov

Agencies also spend a substantial portion of their IT budgets on mission area maintenance, or upkeep of IT that directly supports agency-designated mission delivery (e.g., military intelligence, surveillance, and reconnaissance). Thus, the combined total cost for maintenance of all federal legacy IT systems for FY 2014 was actually $52.9 billion, or 70 percent of total IT spending (with the exemption of classified DoD IT spending).[5] Moreover, this proportion has been increasing in recent years and is expected to reach 73 percent in FY 2015. Even as total IT spending stagnates, maintenance spending is growing.

Network breaches and outages also generate tremendous costs that are often overlooked when considering cost of ownership. The United States Computer Emergency Response Team (US-CERT) reported a 33 percent increase in cyber incidents disclosed by federal agencies from 2010 to 2013. In one instance, personally identifiable information on more than 100,000 individuals was stolen from a Department of Energy computer network, a breach estimated to cost more than $3.7 million to resolve.[6]

Network outages, which are often self-inflicted, can be just as consequential. In January 2014, legacy system failures were blamed for a "catastrophic network technological outage" affecting the Pentagon Force Protection Agency. The outage left the agency "without access to mission-critical systems."[7]

The true cost of owning IT networks, however, transcends fiscal and direct mission setbacks for federal agencies. Government network failures also damage public trust and federal employee morale. The troubled rollout of healthcare.gov offers a potent example. The website's crash on October 1, 2013 contributed to a significant loss of confidence in the government. A December 2013 poll found 70 percent of Americans lack confidence in the government's ability to address major problems, with most identifying health care reform as a top priority.[8] Federal employees were similarly negatively affected by the very public failure. As a March 2014 Government Business Council/*Nextgov* poll found, just 32 percent of federal technology executives are confident in their agency's ability to execute IT priorities.[9]

Examined carefully, the true cost of ownership for federal IT networks is much higher than generally accounted for.

The Agility Imperative

Realizing IT network efficiencies is certainly a major priority for federal agencies, but even more important is their ability to achieve mission in increasingly dynamic environments.

Having completed its Quadrennial Defense Review in March 2014, the Department of Defense provides a salient case in point.

"THE MILITARY THAT MAINTAINS THE MOST AGILE AND RESILIENT NETWORKS WILL BE THE MOST EFFECTIVE IN WAR."

After more than a decade of large-scale, prolonged operations in Iraq and Afghanistan, the military is rebalancing for a broader spectrum of conflict that requires much greater agility and adaptability. The strategy's force structure projections provide concrete evidence: while the Army is set to shrink to roughly 450,000 soldiers from a wartime high of 570,000, Special Operations Forces will grow to nearly 70,000 personnel.[10] IT networks form a critical component of this rebalancing. Assessing the ongoing evolution of global threats and technological change, Chairman of the Joint Chiefs of Staff, General Martin Dempsey said, "the military that maintains the most agile and resilient networks will be the most effective in war."[11]

The Air Force, in particular, has embraced the strategic agility concept. Its most recent 30-year strategy, released in July 2014, emphasizes that "agility is the counterweight to the uncertainty of the future and its associated rapid rate of change." In order to maintain the Air Force's edge in the emerging operational environment, the strategy asserts that it will move away from large, long-term acquisition programs that limit flexibility and "begin designing agility into capability development."[12]

Strategic agility is not just an imperative for DoD; civilian agencies are also tasked with meeting the expectations of a 21st century citizenry. The President's FY 2015 budget identifies the speed and ease with which individuals and businesses can complete transactions with agencies as being critical to the government's ability to deliver the "world-class service that citizens expect."[13] Agencies must also be prepared to cope with extreme variations in demand for services. During extreme weather events, outbreaks of disease, and even tax seasons, civilian network capacity needs vary greatly.

A New Network Acquisition Model

To bring down the true cost of IT network ownership and meet demands for more agile operations, federal agencies can look to a new model for IT network acquisition: Network-as-a-Service.

Traditionally, agencies have considered IT an asset requiring upfront capital to purchase and long-term planning to maintain. This ownership model may permit the utmost control of network infrastructure, but it also limits flexibility and impedes innovation. By contrast, an “as-a-service” approach to network acquisition would allow agencies to pay for use based on consumption. Although agencies would no longer own their networks outright, they would actually have greater control over how they leverage them.

“Network-as-a-service” facilitates five main improvements:

1. *Scalability* - Agencies can increase and decrease network capacity as needed, allowing for quick adaptations to sudden changes in requirements and unpredictable environments.
2. *Efficiency* - Agencies can invest money they would otherwise spend on maintaining legacy systems in enhanced IT capabilities, helping them make the most of taxpayer dollars.
3. *Upgradability* - Agencies can upgrade or downgrade their networks as needed to maintain top quality while ensuring compatibility with legacy systems
4. *Security* - Agencies can maintain up-to-date security features, helping them stay ahead of evolving cyber threats.
5. *Responsiveness* - Agencies can quickly respond to fluctuations in service demands, allowing them to adopt a “just in time” strategy to deliver services to citizens.

The key to successfully navigating the inflection point the federal government faces in enterprise operations is strategic agility. Agencies can start by reassessing their approach to network acquisition.

About GBC

Government Business Council (GBC), the research arm of Government Executive Media Group, is dedicated to advancing the business of government through analysis and insight. GBC partners with industry to share best practices with top government decision-makers, understanding the deep value inherent in industry’s experience engaging and supporting federal agencies. For more information, please visit: www.govexec.com/gbc.

About Brocade

Brocade® networking solutions help federal agencies achieve their critical initiatives as they transition to a world where applications and information reside anywhere. Today, Brocade is extending its proven data center expertise across the entire network with open, virtual, and efficient solutions. To deploy new technology without appropriating CapEx, agencies can utilize Brocade Network Subscription, an OpEx acquisition model that aligns with federal directives and provides network-as-a-service flexibility with limitless network scalability and upgradability. (www.brocade.com)

Sources

1. *Fiscal Year 2015 Budget of the U.S. Government*, Executive Office of the President, March 2014. http://www.whitehouse.gov/sites/default/files/omb/budget/fy2015/assets/budget.pdf
2. *Federal Information Technology: FY 2014 Budget Priorities*, Steven VanRoekel, Executive Office of the President, April 2013. http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/2014_budget_priorities_20130410.pdf
3. "Federal IT Spending Slashed in Proposed 2015 Budget," *InformationWeek*, March 2014. http://www.informationweek.com/government/cybersecurity/federal-it-spending-slashed-in-proposed-2015-budget/d/d-id/1114126
4. "Agencies Need to Strengthen Oversight of Multibillion Dollar Investments in Operations and Maintenance," Government Accountability Office, November 2013. http://www.gao.gov/assets/660/658794.pdf
5. IT Dashboard, FY 2015 Edition
   www.itdashboard.gov/export/trends_report
   "Agencies Need to Improve Cyber Incident Response Practices," Government Accountability Office, April 2014.
   http://www.gao.gov/assets/670/662901.pdf
6. "Pentagon Policy Agency Hit by 'Catastrophic' Network Outage," *Nextgov*, May 2014
7. http://www.nextgov.com/defense/2014/05/pentagon-police-agency-hit-catastrophic-network-outage/83842/
8. "Poll: Americans Have Little Faith in Government," *AP*, January 2014. http://bigstory.ap.org/article/poll-americans-have-little-faith-government
9. "Federal Tech Execs Pessimistic About White House IT Priorities," Government Business Council, April 2014. http://www.govexec.com/gbc/federal-tech-execs-remain-pessimistic-about-white-house-it-priorities/82213/
10. *Quadrennial Defense Review 2014*, Department of Defense, March 2014. http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf
11. "DOD Must Stay Ahead of Cyber Threat, Dempsey Says," *American Forces Press Service*, June 2013. http://www.defense.gov/news/newsarticle.aspx?id=120379
12. *America's Air Force: A Call to the Future*, United States Air Force, July 2014. http://airman.dodlive.mil/files/2014/07/AF_30_Year_Strategy_2.pdf
13. *Fiscal Year 2015 Budget of the U.S. Government, Executive Office of the President, March 2014.* http://www.whitehouse.gov/sites/default/files/omb/budget/fy2015/assets/budget.pdf

First image*: Flickr user Beraldo Leal (Creative Commons)*
Second image: *Flickr user U.S. Pacific Air Forces (Creative Commons)*