Cloud is a critical enabler of digital transformation and must be accompanied by supportive leadership as well as agile and streamlined customer-focused processes that allow secure multichannel access to information, services, and benefits. It’s important that agency leaders take a structured, roadmap-driven approach to leveraging existing datacenters to ensure that initiatives and investments deliver maximum value and produce consistent results for employees, customers, and partners in the government ecosystem.

The following questions were posed by Cisco to Adelaide O’Brien, research director of IDC’s Digital Transformation Strategies for IDC Government Insights, on behalf of Cisco’s customers.

Q. Government agencies start with an existing IT infrastructure and governance. As cloud technologies become more pervasive, what issues are government enterprises facing?

A. The trend to place more workloads in the cloud is steadily increasing, allowing agencies to update to the latest versions, enable rapid deployment of new functionality, spin up new features, support fully functioning disaster recovery sites, and develop an easier way to test and deploy applications. While cloud services add tremendous value, they don’t install and run themselves. Cloud services require careful, thought-out, and well-executed steps, including an awareness of application dependencies and the ability to ensure successful and cost-effective application rollouts and ongoing service performance. Challenges that agencies face include:

   ■ **Security.** Perhaps the most important decision that government CIOs must address is ensuring that cloud solutions provide appropriate security and privacy. Government concerns around security have long been an adoption inhibitor for cloud solutions, even though cloud providers can demonstrate that the levels of security provided by cloud solutions are often superior to what many organizations can achieve on their own. IDC has observed success where cloud advocates work across functions such as CISO, LOB, and HR and change the security conversation from compliance (mandatory for consideration of a vendor) to managing acceptable risks.
Lack of documented standards. Cloud environments rely on well-defined standards to enable workload and information portability across a wide range of heterogeneous internal and external resources. This may not come naturally for government organizations accustomed to nonstandard legacy applications and may complicate cloud deployments as a result. Effective management of datacenters and multicloud architectures requires clear IT service definitions and policies including standard configurations, SLAs, security, and governance to ensure consistent service delivery and service levels regardless of the infrastructure resources supporting the workload.

Lack of a cloud-first architecture. A cloud-first architecture is key, and agencies should be architecting continuity, disaster recovery, compliance, and security on cloud-first platforms and shifting workloads to the most appropriate mix of IaaS, PaaS, and SaaS while continuing to support existing datacenters as needed to enable mission-critical business requirements.

Lack of advanced analytics. Agencies need to proactively identify risk and compliance across the entire IT infrastructure via monitoring and analytics tools that help track and broker multicloud usage based on real-time application performance and SLAs.

Q. The definition and understanding of "cloud" have evolved over the years. As agencies try to define their unique cloud strategies, what should they consider?

A. Defining an enterprisewide cloud strategy is key to ensuring successful outcomes. In fact, IDC Government Insights predicts that 60% of federal IT cloud spending in 2018 will go toward transition strategies that address key workload needs. These transition strategies should include a road map of the steps needed now and in the coming years, including an assessment of mission needs, technology readiness, staff skills, and external partner viability and track records.

Some legacy systems contain decades of citizen information siloed within disparate and disjointed servers, and transitioning these workloads to the cloud needs to be part of an overall long-term strategy. Transition plans should include cost and level of effort required to move to cloud, data sanitization (cleansing data) before moving data to the cloud, timing of transition to provide continuity of services and information, determining which cloud provides required agility and scalability, readiness of staff, and capability and security certifications of vendors. IT departments will need application development tools, environments, and methodologies that allow them to accelerate development in multiple environments, including various cloud and on-premises datacenters.

By transforming infrastructure and moving applications in a way that avoids disruption to the agency and constituents, organizations can address their most pressing challenges while planning and preparing for future deployment of most workloads to cloud.

Q. What are best practices to ensure that datacenters are ready for these changes, without having to forklift their entire datacenter infrastructure?

A. For existing datacenters, agencies need to ensure they deploy an architecturally flexible datacenter network and leverage a full range of integrated solutions in their datacenters. These include the ability to scale the data link and network layer via a multipath network (e.g., enabling workload flexibility for improved business agility) and the ability to deploy virtualization to increase capacity (e.g., enabling a single switch to perform as multiple virtual switches). Single-pane-of-glass management can provide increased application visibility and life-cycle management and assurance. As government matures in its hybrid IT journey, agencies will deploy common monitoring and configuration tools including legacy system plug-ins to enable broader integrations.
As the use of cloud solutions in government increases, business and IT leaders are recognizing that the safety and success of their business depend on finding ways to take full advantage of cloud innovation while ensuring consistent service levels, data management and privacy, and user experiences. Hybrid IT management includes aligning the organization around service levels, cost control, security, and IT-enabled innovation. A hybrid approach combines the right mix of traditional datacenters, private cloud, and public cloud to meet mission goals and allows agencies to integrate new technologies where needed and maintain legacy systems where appropriate. In the past, agencies deployed cloud in response to mandates, with compliance as a key driver.

Today, for many agencies, the question is not whether to move to cloud but what services can be deployed more efficiently via cloud versus traditional IT, provide the agency with additional capability, and better serve citizens, often with less internal up-front cost and fewer resources.

Q. How can legacy datacenter architectures assist agencies as they move to a modern application development methodology, allowing IT to keep up with the speed of an agency's mission and the changes impacting that mission?

A. Legacy datacenter architectures that standardize applications and the IT environment for minimum downtime, that are virtualized wherever possible, and that automate asset performance and operations provisioning are poised to assist agencies in delivering on their mission. As the operational complexity of multicloud environments expands to encompass a broad variety of legacy and cloud-native applications, such as open source infrastructure, open API-based integrations, and mobile and social human interactions, agency IT decision makers should consider processes and tools that can simplify operations, maintain end-to-end service levels, and ensure that resources adapt seamlessly to dynamic changes in workload, processing, storage, and network requirements.

Q. How must traditional datacenter governance and infrastructure change as agencies move to a multicloud environment?

A. A major obstacle for agencies moving to cloud is the ability to procure/acquire cloud solutions. Agencies are addressing their procurement models and making changes that need to occur in skills and policies to move to acquiring on-demand services versus hardware and software. IDC Government Insights has observed that aligning governance with technology orchestration can deconflict many long-standing acquisition challenges. Agencies are deploying several tools that can assist in creating workflows, such as chargeback payment streams to facilitate use of contract vehicles.

Governance should also include stewardship of funding that optimizes infrastructure expenditures and frees up budgets for reinvestment. This aspect of governance is particularly important in light of recent legislation that provides a $500 million central modernization fund that agencies can borrow against to update aging, unsecure systems. Agencies that have working IT capital funds are allowed up to three years to use savings gained from streamlining and replacing legacy systems.

As cloud usage grows and starts to reflect a more significant portion of the organization’s IT budget, the move to a multicloud environment shifts the focus of IT management away from the simple configuration, provisioning, and support of individual IT components to managing multiple clouds. Cloud service operations — such as provisioning and monitoring — will need to evolve to a structured and consistent framework. This need becomes even more significant in a multicloud environment where different providers have different APIs, workflows, and tools to manage their services. In a multicloud environment, the focus of IT staff shifts to adopting
automated, policy-based optimization of resource utilization, workload consumption, and user self-service across a range of diverse cloud services and on-premises datacenters. The use of DevOps and Agile development methodologies that drive more frequent application updates and blur the line between development, test, and production allows IT organizations to automate provisioning resources to users, share tools, leverage APIs, standardize production environments, and automate repetitive tasks. These key aspects of DevOps make deployments predictable and free IT staff for more creative and challenging work.

Additionally, as servers move closer to the edge, IoT-driven network integration and visibility become more critical. Cloud resource management, an automated method of keeping pace with changing mission needs and demands for more resources, and integration of resources across cloud platforms via automation and orchestration tools will grow to become critical technical capabilities at IT organizations driving digital transformation. Ultimately, agencies must integrate the network, collaboration systems, and security infrastructure to automate processes and monitoring and deploy advanced analytics to proactively identify risks and to maintain compliance across hybrid cloud resources.

ABOUT THIS ANALYST
Adelaide O'Brien is research director for IDC Government Insights responsible for U.S. Government Digital Transformation. Ms. O'Brien's core research coverage includes digital approaches in creating and delivering services with increased agility, flexibility, and scalability. Ms. O'Brien's research also includes a particular emphasis on maturity models in big data/analytics and cloud as well as benchmarking government maturity levels.

ABOUT THIS PUBLICATION
This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC Government Insights, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC Government Insights content available in a wide range of formats for distribution by various companies. A license to distribute IDC Government Insights content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS
Any IDC Government Insights information or reference to IDC Government Insights that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC Government Insights. For permission requests, contact the IDC Custom Solutions information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC Government Insights. For more information on IDC, visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc-gi.com