



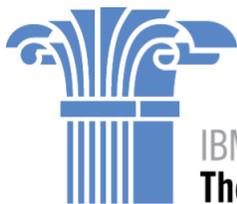
Mobilizing Cloud Computing for Public Service

FEBRUARY 12, 2023

BY AMANDA STARLING GOULD, PhD



PARTNERSHIP
FOR PUBLIC SERVICE



IBM Center for
The Business of Government

About the Partnership

The Partnership for Public Service is a nonpartisan, nonprofit organization that works to revitalize the federal government by inspiring a new generation to serve and by transforming the way government works. The Partnership teams up with federal agencies and other stakeholders to make our government more effective and efficient.

About IBM Center for the Business of Government

The IBM Center for The Business of Government connects research to practice, applying scholarship to real world issues and decisions for government. The Center stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

Table of Contents

Introduction	4
Plan	7
Test	9
Secure	11
Transform	13
Optimize	15
Conclusion	17
Our Experts	18
Project Team	19

Introduction

Federal agencies are increasingly employing secure and scalable cloud solutions to transform how the government operates, and how it provides effective and equitable digital public services.

To understand how agencies are mobilizing cloud computing for public service, the Partnership, in collaboration with the IBM Center for The Business of Government, hosted a series of events in 2022 featuring federal IT leaders. Over the course of three webinars, we heard from the Census Bureau; the departments of Agriculture, Defense and Veterans Affairs; the Federal Emergency Management Agency; the Government Accountability Office; the National Institutes of Health; the National Oceanic and Atmospheric Administration; and the Office of Personnel Management.

This brief offers key cloud computing strategy insights from individuals at each organization, while highlighting the stories of five:



how the Census Bureau, FEMA and NOAA have planned for transformed field work and workforce by creating ‘hybrid’ ecosystems—which distribute data across multiple cloud and other computing environments—that employees can access on the ground, afloat at sea and in the eye of a hurricane;



how the VA is making veterans’ experience more customer-centric and secure through sophisticated cloud services; and



how the NIH is optimizing multiple cloud systems to reduce cost and maximize performance, resulting in “vastly accelerated discovery and innovation in science and medicine,” according to Andrea Norris, NIH’s former chief information officer.

Keys to Successful Cloud Computing

Plan: Careful planning and strategic collaboration make cloud computing ready for use in the field.

Test: Agile testing catches critical issues before cloud deployment.

Secure: “Zero-trust” and security-focused teams protect cloud data.

Transform: Support for people using the cloud fosters innovation.

Optimize: Cloud optimization strategies reduce cost and maximize performance.

Keys Insights Summary

Plan

Agencies will be more successful at developing strategy if they understand:

- **Data:** what data needs to be stored, and how it will be used.
- **Access:** where, when, how and by whom that data will be accessed.
- **Tools and Problem Solving:** what problems the cloud is solving, and what tools and services it enables.
- **Future Scenarios:** forecasted future needs for storage, access and tools.

Test

Strategy development and deployment will be aided by:

- **Collaboration:** bringing agency stakeholders to the table for mission-driven decision-making.
- **Partnerships:** establishing cross-government and public private partnerships.
- **Testing:** intentionally iterating a strategy through careful testing to help catch critical issues, identify resource limits and predict workforce friction before a cloud strategy is deployed.
- **Measurement:** undertaking a conscious and conscientious strategy for measuring and demonstrating the need for cloud solutions.
- **Buy-in:** eliciting support for the effort from early adopters and agency leaders.

Secure

Cybersecurity is most successful when these key elements of cross-team culture change are in alignment:

- Cybersecurity mindset: Cybersecurity is centered in all considerations of technology.
- Security-first culture: Security-focused culture ensures safety protocols inform all aspects of cloud-related decision-making, from procurement to workforce training.
- Coordination: Cybersecurity is a team sport requiring cooperation across all of IT.
- Structure: Establishing a team such as the VA's Application Hosting, Cloud, and Edge Solutions unit can institutionalize cross-agency collaboration.
- Leadership: Security-aware agency leadership and highly skilled cybersecurity leaders are in place.
- Partnerships: Distributing responsibility for data with contractors and other partners can enhance security.

Transform

A top strategy for optimizing the cloud is to equip the people who use it. To keep them on pace with technology, workforce strategies should include:

- Awareness and attention to current staff strengths and gaps.
- Promotion of early adopters and skilled users within the agency who can use their knowledge to lead culture transformation.
- Structured support—in the form of resources, training, incentives and mentors—for users unfamiliar with using cloud services.
- Deliberate strategies for identifying and attracting established and emerging technical talent.
- Strong leadership focused on change management.

Optimize

Optimizing for cost savings and capacity is aided by an intentional strategy for tracking cloud usage that includes staff or staff time dedicated to:

- Monitoring and maintaining access and usage.
- Ensuring data and reports on cloud usage and spending are accurate.
- Managing relationships with service providers.
- Forecasting future needs, enabling agencies to expand access to the cloud and improve mission delivery.



Photo Credit: Shutterstock

Plan

Careful planning and strategic collaboration make NOAA's cloud ready for the field

In the fall of 2022, Florida was struck by the deadliest hurricane to hit the state since 1935. NOAA aerospace engineer Nick Underwood was at that time aboard a four-engine hurricane hunter aircraft nicknamed Kermit, gathering and transmitting data about [Hurricane Ian](#) to cloud databases at NOAA's National Centers for Environmental Prediction and the National Hurricane Center. There, it was integrated into global weather models and used for real-time hurricane prediction that would enable people to evacuate to safety. Since 2019, NOAA has made it a priority to use data, like that gathered by Underwood, [to reduce the severest impacts](#) of extreme weather events.

In 2020, NOAA developed a cloud strategy to better coordinate data across the organization. The agency adopted a multi-cloud solution—combining commercial cloud with government cloud and on-premise private data systems for a hybrid cloud configuration—enabling the agency to manage information that spans “from the sun all the way down the deepest part of the waters,” said Captain Joseph Baczowski, acting director of NOAA's Cloud Program Management Office.

In addition to private cloud systems that store data and services on-site, NOAA partners with cloud vendors to democratize its data—from weather data to whale sounds—making it free and open to everyone. “Unlocking the full utility and potential of NOAA's massive and diverse data” drives the agency's new [cloud strategy](#), according to a NOAA statement.

A team at NOAA coordinated with the Cloud Acquisition Team at the General Services Administration to create what the GSA calls “[a model effort for smart cloud migration](#).” NOAA's success came in large part from careful customer-centric planning and collaboration with strategic partners. NOAA knew it needed a system that could serve its multipurpose mission to gather, analyze and publicly share knowledge. Its computing had to be ready to match the conditions where it would be used, Baczowski said. Important agency work could be stalled or lives endangered if a marine biologist on a boat were to receive an “unable to connect”

message or a hurricane chaser needed to spend precious time on a specialized, multistage login midflight.

Armed with these strategic requirements, NOAA used [a capability-based acquisition](#) approach—one employing a [statement of objectives](#) instead of a statement of work—to guarantee the cloud products and services procured fit the agency’s intended purpose. For example, instead of asking for a specific product using a statement of work, NOAA solicited “cloud storage services that will provide persistent storage, backup service, long-term storage, continuity of operations, and disaster recovery services.” This has resulted in a multiple vendor strategy, whereby NOAA contracts with several different corporate vendors to give the agency optimal flexibility and distributed technical capability. With a mission to serve both the NOAA scientists who collect data and the public that consumes it, NOAA’s strategy had to address both audiences.

In 2022, with commercial cloud capabilities in place, NOAA released its [NOAA Open Data Dissemination](#) program, opening the [tens of terabytes of data it collects daily](#) (and that includes data about “real” clouds!) and sharing it freely with the public to foster discovery and innovation. Former acting NOAA administrator, Neil Jacobs, [attributes](#) the success of such projects to “creative partnerships” with a range of commercial cloud providers, according to a NOAA statement.

Today, NOAA’s commitment to delivering world-class science is buoyed by its innovative multi-cloud strategy.

PLAN: INSIGHTS FOR AGENCIES FROM OUR EXPERTS

Agencies will be more successful at developing strategy if they understand:

- Data: what data needs to be stored, and how it will be used.
- Access: where, when, how and by whom that data will be accessed.
- Tools and Problem Solving: what problems the cloud is solving, and what tools and services it enables.
- Partnerships: what cross-government and public private capabilities are available, and how to leverage them to meet objectives.
- Future Scenarios: forecasted future needs for storage, access and tools.



Photo Credit: The Federal Emergency Management Agency

Test

Agile strategies equip FEMA's cloud for deployment

The Federal Emergency Management Agency, whose teams deployed on the ground during 2022's Hurricane Ian while NOAA scientists were midair, is early in its cloud journey. Its cloud services support first responders who need real-time data access to make urgent life-saving decisions, and its cloud-based artificial intelligence and data analysis tools predict disaster scenarios to position resources in advance. FEMA's response teams, however, still carry their own IT infrastructure into the field.

"We're going to take all of that out the equation with the cloud," said James Rodd, cloud portfolio manager in FEMA's Office of the Chief Information Officer. Cloud adoption paired with sophisticated mobile networking capabilities will enable FEMA teams to respond faster and more efficiently, he added. "Any place we go, any place we serve, we need to improve our response to the citizens," Rodd said, "and that's the goal of our cloud adoption."

A full cloud program will help FEMA speed its response to disasters and enable the agency to rapidly increase capacity when disaster strikes and scale down when the pace of response permits. Its services—from ground support to the [FEMA GO](#) cloud-based disaster-response grant system—need to be able to scale up in a matter of hours, during and immediately after disaster situations, to support potentially tens of thousands of survivors.

The agency's agile framework for full deployment of the cloud includes performance testing, incremental updates and iterative redesign. Early tests revealed performance issues, Rodd said, and those tests, resulted in improvements in latency—the speed at which data travels through a system. Rodd's tests are aimed to ensure "equitable and exhaustive solutions are in place," in terms of usability, scalability and security, before all operations are moved to the cloud. FEMA's tests, Rodd said, also aim to guarantee the transition is frictionless, since cutting someone's access to data or software during the conversion is simply not an option.

Agile ways of working are relatively new to FEMA, and Rodd’s team is leading the transformation. It will be well worth the process, according to Rodd, as the savings of resources, time and cost anticipated with a thoroughly tested cloud system will ultimately bring “incredibly positive changes” to FEMA offices and field work.

TEST: INSIGHTS FOR AGENCIES FROM OUR EXPERTS

Strategy development and deployment will be aided by:

- Collaboration: bringing agency stakeholders to the table for mission-driven and agile decision-making.
- Testing: intentionally iterating a strategy through careful testing to help catch critical issues, identify resource limits and predict workforce friction before a cloud strategy is deployed.
- Measurement: undertaking a conscious and conscientious strategy for measuring and demonstrating the need for cloud solutions.
- Buy-in: eliciting support for the effort from early adopters and agency leaders.



Photo Credit: Shutterstock

Secure

“Zero-trust” culture and security-focused teams protect the VA’s Cloud

Operating round-the-clock from Puerto Rico to the Philippines, the Department of Veterans Affairs has an always-on global IT infrastructure linking its 1,400 facilities. A secure multi-cloud strategy enables the VA to manage sensitive data at more than 100 major medical centers, and to offer modern, accessible digital services to veterans—of paramount importance given the medical and personal data the VA accesses to serve veterans and their families.

The VA’s Office of Information and Technology aims to be “[the best IT organization in government](#)” with a vision-driven, people-focused, security-first approach. Recognizing the importance of collaboration to enhance its expertise, the VA created a unit within its infrastructure operations group, called Application Hosting, Cloud, and Edge Solutions. The group aims to help organize the department’s cloud administrators into one common corps to deliver coordinated and consistent service. At the VA, security has been “baked in” by design from the beginning, said David Catanoso, acting director of the unit, and continues to drive the department’s cloud strategy and the decisions it makes about cloud architecture.

The unit works from the assumption that it is in a high-threat environment, so the security dimension is “part of our bloodstream now at the VA,” Catanoso said. New daily cybersecurity threats have increased, and these threats are both easier to create and harder to contain. In response, the unit is adopting a calculated approach following [the National Institute of Standards and Technology’s “zero trust”](#) guidelines wherein “no implicit trust [is] granted to assets or user accounts based solely on their physical or network location.”

This strategy reflects guidance recommended by all our agency experts: from Timothy Persons, former Chief Scientist at the Government Accountability Office, who described security as “a team sport,” to DOD’s Robert Vietmeyer who finds success in cybersecurity hinges on cross-team collaboration embedded in agency culture.

At the VA, cybersecurity starts at the level of data and moves through the “bloodstream” of its cloud environment: All data entering the VA’s system—from telehealth data to veterans’ financial information—goes through a [protocol](#) that protects it “at rest,” within the VA’s information repositories, and “in transit” as it is electronically shared or transmitted to trusted providers.

The department also regulates control of access, authentication and authorization to all VA networks, tools, applications, equipment and physical locations. With its responsive, flexible cloud structures and zero-trust blueprints for cybersecurity accountability, the VA can secure the highly sensitive data it protects.

SECURE: INSIGHTS FOR AGENCIES FROM OUR EXPERTS

Cybersecurity is most successful when these key elements of cross-team culture change are in alignment:

- **Cybersecurity mindset:** Cybersecurity is centered in all considerations of technology.
- **Security-first culture:** Security-focused culture ensures safety protocols inform all aspects of cloud-related decision-making, from procurement to workforce training.
- **Coordination:** Cybersecurity is a team sport requiring cooperation across all of IT.
- **Structure:** Establishing a team such as the VA's Application Hosting, Cloud, and Edge Solutions unit can institutionalize cross-agency collaboration.
- **Leadership:** Security-aware agency leadership and highly skilled cybersecurity leaders are in place.
- **Partnerships:** Distributing responsibility for data with contractors and other partners can enhance security.

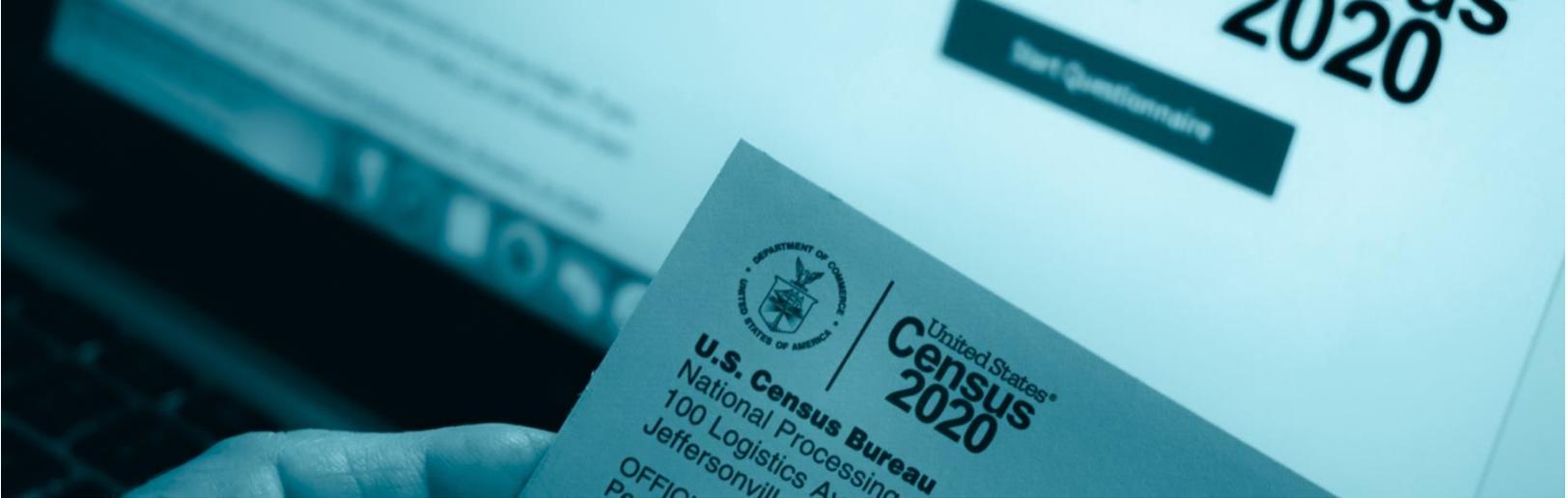


Photo Credit: Shutterstock

Transform

Prioritizing people spurs cloud-enabled innovation at the Census Bureau and the Office of Personnel Management

The Census moved to the cloud in 2020, enabling individuals to account for themselves in the census's first self-serve online survey. In addition, hundreds of thousands of enumerators, armed with cloud-equipped handheld devices, deployed to neighborhoods in every U.S. state and territory, assigned to count every resident. Due to technological advances made possible by the bureau's cloud systems, the survey was for the first time available online and in 13 languages.

To achieve this feat and other agency processes, the Census Bureau employs cloud-enabled tools and software-as-a-service models. These "let us focus on providing value by using more of the technology, not spending our time maintaining the infrastructure that supports it," said Brock Webb, technology strategist for the Computer Services Division in the bureau's Office of the Chief Information Officer. In Webb's experience, installing new technology is only 10% of the process; the other 90% is people and culture.

Webb's human-centered technology strategy, from design to implementation, focuses on the people who use the technology, as he knows people will not adopt new technology if they cannot figure out how to use it. This strategy, Webb told us, led to a roadshow across the agency "to talk about cloud computing and understand the needs and problems cloud might solve from the perspective of the mission and business areas." Ongoing employee-focused priorities include offering training through the Census Bureau Data Academy, attracting new talent through recruitment to the bureau's Secure Cloud Team, and adjusting cloud services in response to what the business and mission area partners need.

At the Office of Personnel Management, the strategy for deploying cloud initiatives is also “closely tied to the employee experience and employee enablement” said Akanksha Sharma, senior advisor on human capital technology transformation at OPM. By intentionally empowering their early adopters through training and professional development, OPM is structuring a culture of innovation so that technology, people and practices move forward in tandem.

With modern tools like cloud computing and an empowered workforce, agencies can now better serve the public.

TRANSFORM: INSIGHTS FOR AGENCIES FROM OUR EXPERTS

A top strategy for mobilizing cloud computing is to equip the people who use it. To keep them on pace with technology, workforce strategies should include:

- Awareness and attention to current staff strengths and gaps.
- Promotion of early adopters and skilled users within the agency who can use their knowledge to lead culture transformation.
- Structured support—in the form of resources, training, incentives and mentors—for users unfamiliar with using cloud services.
- Deliberate strategies for identifying and attracting established and emerging technical talent.
- Strong leadership focused on change management.



Photo Credit: Shutterstock

Optimize

Cloud optimization reduces costs and accelerates discovery at the NIH

The National Institute of Health’s cloud strategy unlocks its potential to deliver exemplary science. The NIH’s Science and Technology Research Infrastructure for Discovery, Experimentation, and Sustainability Initiative, or STRIDES, “aims to modernize biomedical research by reducing economic and process barriers in utilizing commercial cloud services,” according to the initiative’s website. The strategy enables science and empowers scientists while also ensuring cybersecurity and standardizing data stewardship.

NIH’s journey with the cloud started several years ago in response to the changing nature of science and biomedical research. With new tools to capture data, from medical imaging to wearable biometrics, the agency collected an unprecedented wealth of data and needed to move their national biomedical research community to the cloud to enable collaboration across datasets. More and better data allow for more and better analysis leading to more informed decision-making.

During the COVID-19 pandemic, for example, the NIH’s cloud environment made it possible for researchers around the globe to collaborate in real time. “When COVID hit, and we first received the genetic details of COVID, our National Library of Medicine, [which] manages a global genomic database, put that data in our cloud STRIDES program and made it accessible to researchers around the world within a day, so that people could begin to do the science,” said Andrea Norris, former chief information officer and director of the NIH Center for Information Technology, adding that the move accelerated the pace of discovery. “Technology has changed the way we do science,” Norris said, and “the cloud is changing the platforms and tools we use to do it.”

NIH’s cloud strategy calls for modernizing standard data practices by mandating data sharing policies within its cloud environment. In January 2023, NIH will require anyone it funds to have a data management and sharing plan, according to Norris. The goal is to couple the equally important values of open access and data privacy—“open access to data with appropriate controls”—to support discovery while ensuring best practices for data security and privacy.

Recognizing that discoveries are enabled by more diverse participation, the STRIDES cloud strategy brings new researchers into the community by reducing barriers to entry. NIH is changing the denominator of who conducts biomedical research, Norris said, broadening it from the pool of researchers at the largest, wealthiest institutions. Now, researchers just need access to the internet to find an abundance of data and findings to advance their work.

Part of that increased access is achieved through cost savings from cloud optimization. Quickly scaling up service to meet need (“rapid elasticity”) and monitoring usage (“measured service”) are two benefits that come with cloud adoption and maturation. By taking advantage of both, the NIH has saved tens of millions of dollars in the three years since moving more than 200,000 terabytes of data to the cloud, Norris reports. Money previously spent on maintaining in-house systems and on unused storage capacity is now shifted directly to NIH research and researchers. More researchers now have greater access to NIH data with more efficiency and in less time at cheaper costs.

Cloud “has had tremendous impact on the kind of science we're doing, and the kind of innovations we're seeing,” Norris said. And the agency is only just beginning to optimize the cloud in support of the mission.

OPTIMIZE: INSIGHTS FOR AGENCIES FROM OUR EXPERTS

Optimizing for cost savings and capacity is aided by an intentional strategy for tracking cloud usage that includes staff or staff time dedicated to:

- Monitoring and maintaining access and usage.
- Ensuring data and reports on cloud usage and spending are accurate.
- Managing relationships with service providers.
- Forecasting future needs, enabling agencies to expand access to the cloud and improve mission delivery.



Photo Credit: Shutterstock

Conclusion

LOOKING AHEAD: What comes next for agency use of cloud computing?

Concurrent to our webinar series, the GAO published [a report](#) detailing four primary challenges they identified for federal agencies adopting cloud computing practices: “Ensuring cybersecurity; Procuring cloud services; Maintaining a skilled workforce; Tracking costs and savings.” We note these are the same challenges our experts are already facing head-on.

What comes next for agency use of cloud computing? In the short term, our experts predict:

- More agencies move more data and operations to the cloud.
- An increase in government-wide use of cloud computing and applications.
- Innovation on the ground as agencies develop cloud capabilities.
- Public-private partnerships developed with the goal of optimizing the cloud environment.
- A targeted focus on workforce training to enable employees to successfully use cloud services to support their agency’s mission.
- Use of cloud capabilities and multi-cloud systems to transform customer-facing digital services.
- More fluid data sharing across agencies and increased public access to agency-generated data.

Longer term, these changes could revolutionize how our government functions and serves the people. Digital transformation involves modernizing technology to provide more effective, equitable and accessible services. Carefully developed cloud environments, secure and optimized for performance, provide the foundation for a more modern federal government that offers better service to the public.

The challenge today is designing for tomorrow’s opportunity. The agency stories highlighted above preview the future and forecast what is to come.

Our Experts

Jonathan Alboum

Federal Chief Technology Officer at ServiceNow and CIO SAGE at the Partnership for Public Service

David Catanoso

Acting Director, Application Hosting, Cloud, and Edge Solutions, Department of Veterans Affairs

Timothy Persons

Former Chief Scientist and Managing Director, Science, Technology Assessment, and Analytics, Government Accountability Office

Akanksha Sharma

Senior Advisor on Human Capital Technology Transformation, Office of Personnel Management

Brock Webb

Technology Strategist, Computer Services Division, U.S. Census Bureau Office of the Chief Information Officer

Joseph Baczkowski

Acting Cloud Program Management Office Director, National Oceanic and Atmospheric Administration Office of the Chief Information Officer

Andrea Norris

Former Chief Information Officer and Director, Center for Information Technology, National Institute of Health

James Rodd

Cloud Portfolio Manager, Federal Emergency Management Agency Office of the Chief Information Officer

Robert Vietmeyer

Director for Cloud and Software Modernization, Department of Defense Office of the Chief Information Officer

Project Team

PARTNERSHIP FOR PUBLIC SERVICE

Emma Shirato Almon
Manager, Tech & Innovation

Amanda Starling Gould
Manager, Technology & Innovation

Mark Lerner
Director, Tech & Innovation

Audrey Pfund
Creative Director

Samantha Donaldson
Vice President, Communications

Jason Labuda
Design and Video Content Manager

Ellen Perlman
Senior Editor

Max Stier
President and CEO

IBM

Dan Chenok
Executive Director, IBM Center for The
Business of Government

Chris Egan
Partner, Cybersecurity and Biometrics, IBM
Consulting

Scott Robertson
Senior Partner and Vice President, Hybrid
Cloud Strategy and Services, IBM Consulting

Trista Colbert
Senior Partner and Vice President, Hybrid
Cloud Management, IBM Consulting

Rasheedat Osei-Acheampong
Partner and Delivery Executive, Federal
Hybrid Cloud Transformation, IBM Consulting

Sherri Sirotzky
Field Marketing Manager, IBM Consulting



600 14th Street NW
Suite 600
Washington, DC 20005

ourpublicservice.org
(202) 775-9111

 [partnershipforpublicservice](https://www.facebook.com/partnershipforpublicservice)
 [@PublicService](https://twitter.com/PublicService)
 [rpublicservice](https://www.instagram.com/rpublicservice)



600 14th Street, NW
Second Floor
Washington, DC 20005

(202) 551-9342
businessofgovernment.org

 [IBM Center for The Business of Government](https://www.facebook.com/IBMCenterforTheBusinessofGovernment)
 [@BusOfGovernment](https://twitter.com/BusOfGovernment)
 [businessofgovernment](https://www.instagram.com/businessofgovernment)