Government Business Council

Crawl, Walk, Run

Agencies Find the Right Pace for Cloud Innovation

Underwritten by

IRONBOW TECHNOLOGIES

In the nearly 10 years since the Obama administration first introduced its Cloud First policy, the conversation around cloud has steadily evolved as federal IT leaders have discovered that, though cloud is critical for digital transformation, it is not a destination. With this in mind, government agencies are shifting their focus from launching a handful of cloud-native applications to a more holistic approach, in which they make technology decisions based on mission needs and outcomes.

The Trump administration codified this mentality in its recent release of the Cloud Smart policy: "Agencies should assess their requirements and seek the environments and solutions, cloud or otherwise, that best enable them to achieve their mission goals while being good stewards of taxpayer resources."[1]

To find out how Cloud Smart has manifested in practice amidst these changes and tradeoffs, Government Business Council (GBC) interviewed federal technology leaders at the Department of Health and Human Services, Department of State, and the Defense Information Systems Agency on their top cloud initiatives, priorities, and challenges for 2019 and beyond. Together, their observations and best practices offer a striking glimpse into how the adoption of cloud is fundamentally reshaping the way government agencies operate in the modern era.

.

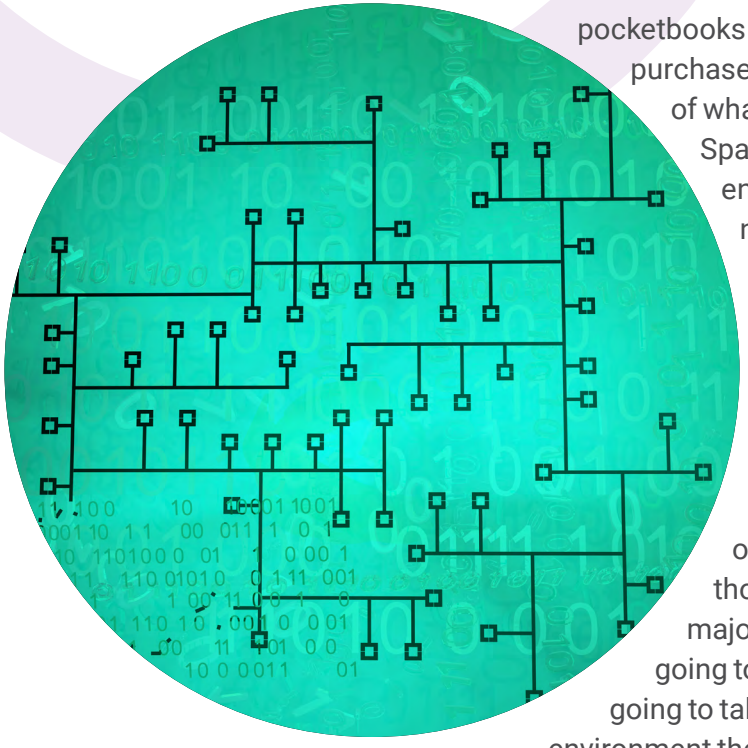
Moving Beyond the One-Size-Fits-All Mindset

The early years of cloud migration forced agencies to make the transition with limited resources, in terms of their IT personnel, infrastructure, and overall strategy. As Federal Chief Information Officer Suzette Kent put it, "Cloud Smart is about equipping agencies with the tools and knowledge they need to make these decisions for themselves, rather than a one-size-fits-all approach."[2]

Some agencies, for example, are large and federated in nature, with no centralized IT authority, while others are small and find it easier to take an enterprise view of their IT architecture. Todd Simpson, Chief Product Officer at the Department of Health and Human Services (HHS), represents the former. "I'm in a very reactive state right now because the federation is so strong and the budget authority is at the lowest common level. So the OPDIVs [operating divisions] are really out there driving the business, and I'm coming in after the fact suggesting 'maybe we should clean this up."

While it may be less 'clean,' Simpson doesn't view these highly autonomous OPDIVs as an obstacle. Instead, he believes that through intense collaboration and transparency, he can start proactively addressing agency needs. "Everyone wants to do the right thing, we just need to work together to understand the opportunities waiting to be exploited."

Michelle Sparrow-Walker, Director of the Cloud Program Management Office at the Department of State, has had a different experience with federated IT. She says she's been able



to use State's distributed structure to her advantage and usher in an enterprise multi-cloud ecosystem. "Everybody was moving out under the cloud on their own. And as a result, we had a lot of early adopters of different types of cloud capabilities that had the ability to meet individual business needs. So what we did was look at where customers basically voted with their pocketbooks in terms of what they went out and purchased individually." With the knowledge of what products were widely-used, Sparrow-Walker was able to create enterprise license agreements, negotiate better price points, and ultimately consolidate services.

At the Defense Information Systems Agency (DISA), Chief of Cloud Services John Hale encountered a different set of challenges. "When we started our cloud migration efforts, we thought - probably naively - that the majority of our mission partners were going to 'lift and shift.' They were actually going to take their application from whatever environment they were in and they were just going to copy it into the cloud and run it. And while we have done some of our applications that way, where we are seeing the bigger benefit is when applications are actually refactored or re-engineered to take full advantage of the cloud." Hale attributes the success of this approach to the agency's use of automation to build and maintain its applications. "When you shift into more of a commercial model where applications and servers are built and rebuilt and thrown away on a routine basis as part of your security plan, automation has played a key role in being able to do that at the scale that we need it to happen."

Identifying Solutions for Agency-Specific Contexts

For agencies looking to balance the need for robust cybersecurity with the desire to maximize speed, innovation, and flexibility, experts have identified multi-cloud as the path forward. However, it's not a silver bullet. The ability to adapt solutions as they see fit can also be a double-edged sword, because an increase in flexibility also means an increase in the number and complexity of options. So how should agencies decide which solution makes the most sense for a given application?

Before agencies can even begin to ask that question, they must first justify the continued existence of the app. Application rationalization – a process more explicitly emphasized in the most recent version of the Cloud Smart policy – is a means of "reducing an application portfolio by 1) assessing the need for and usage of applications; and 2) discarding obsolete, redundant, or overly resource-intensive applications."[3]

Hale explains what this looks like in practice within the Department of Defense (DoD). "The DoD's IT systems and infrastructure overall is actually really old in the grand scheme of technology. We are at a point where,

as we start to make things move to cloud specifically, we have to really look hard at each individual application and mission and determine whether it's really needed to be successful in the warfighting mission anymore."

Once the redundancies have been removed, Sparrow-Walker says her first order of business is categorizing the data. When a customer comes to her with a business need, she needs to know how sensitive the data is ("If this were exposed, how vulnerable does it make the department?"), who the user community is ("will it stay internal, or will it be used/processed by external groups?"), and the interconnectivity requirements.

From there, Sparrow-Walker turns her focus to developing solutions. "To the extent that we can, we try to organize our sequence of recommendations - look at the SaaS [software as a service] capabilities first, and then PaaS [platform as a service], and then as a last resort, custom application development in an IaaS [infrastructure as a service] environment." The goal of all recommendations, Sparrow-Walker says, is to identify cloud capabilities that are aligned with the business mission.

For Simpson, it's all about requirements traceability — a process that ensures that a requirement can be tracked all the way from origin to implementation. "Requirements traceability and ATO [Authority to Operate]/FedRAMP status drive everything for me. My job is to review the alternatives and help my customers find the best solution for the business problem they are trying to solve. I have nothing else in this other than making my customer happy and adding immediate value so we try to keep things simple and not reinvent the wheel if we don't have to."

Cloud's Payoff and Potential

Even though the cloud can reduce capital expenditures and save money, Hale is quick to say that cost savings have not been DISA's primary goal for migrating to the cloud. "To be honest, while we are seeing cost savings, that is not the key driver for us, really. The big drivers are really about elasticity and utility-based billing."

> "It has been a huge benefit from an application rationalization standpoint, to be able to have the true cost of ownership for running each application."
>
> — John Hale
> Chief of Cloud Services
> Defense Information Systems Agency

Elasticity, in Hale's words, is the "ability to increase the workforce and horsepower behind an application at any given time to meet division needs, and then have the application shrink back down to a traditional operational state." He says this has been hugely beneficial for mission owners within DISA.

At HHS, Simpson is focused on the benefits of increased interconnectivity and interoperability, as well as the opportunities presented by new cloud-enabled analytic capabilities. One of his chief initiatives as the inaugural Chief Product Officer has been to build an administrative data hub for all of HHS. [4] "All of this stuff was invisible to us before, but thanks to this big data analytics project, leadership at HHS are now asking [new] questions," says Simpson. "If FDA wants to know the impact of hurricanes in Puerto Rico, they come to me." Sparrow-Walker says that the State Department's decision to adopt a "virtualization first" policy early on has had tremendous benefits. "We realized that the more we moved away from physical infrastructure and into a virtual environment, the more it would ease migration to the cloud." For example, by acquiring SaaS and PaaS and implementing an electronic application, State was able to replace over 800 paper forms used to make a variety of employee requests, and they estimate that this saved more than 50,000 hours of staff time.[5]

Maximizing the Value of Cloud

To capitalize on the new capabilities multi-cloud environments present, Simpson suggests that agencies follow a "crawl-walk-run approach" and exercise patience.

> "Focus on solving one business problem at a time and focus on the low-hanging fruit. Your accomplishments will amass quickly."
>
> — Todd Simpson
> Chief Product Officer
> Health and Human Services

Similarly, Hale encourages leaders to "start small and scale fast." He says he's had a lot of success turning pilots into full-blown production capabilities within a very short time period "by demonstrating to mission partners the actual capabilities, rather than just talking about it." Additionally, Hale urges agencies not to fear vendor lock-in. "It held us back for quite a while," he said, but once they moved past that, they were able to take advantage of the unique benefits of each cloud provider within their specific context. "Leverage the vendors you want to leverage and, when the time comes, there will be a way to get your data and application off of that and move it to a different provider if that's what you choose to do."

Cloud Smarter, Not Harder, with Iron Bow Technologies

Cloud First. Cloud Smart. Software-Defined. Regardless of the mandate or method, Troy Massey, Director of Enterprise Engagements at Iron Bow Technologies, knows that cloud technology plays an integral role in the future of federal IT. To realize this future, he says, it can be challenging for agencies to find the best approach to moving their legacy applications and technologies to the cloud.

"That's where Iron Bow's simple, secure, and flexible multi-cloud infrastructure solution, as well as our experience and cloud experts can help," Massey says. "Iron Bow leverages our expertise with leading hardware and software solutions to create the right configurations within IronTarget™ to meet each client's unique needs. With an assessment, our experts analyze the environment and can identify good candidates for public cloud, which applications are more suitable for on-premise environments, and which should be left alone."

IronTarget is designed to virtualize a variety of workloads, from server-based applications to virtual desktops. It is based on the tried and true hardware technologies combined with a hyper-converged platform, allowing for extreme scalability and growth, while maintaining the highest levels of performance and resiliency. As a complete, turn-key solution, IronTarget's automation creates an on-premise cloud, ready to connect to -- and share workloads with -- public clouds, enabling hybrid and multi-clouds.

With IronTarget, getting your agency what it needs when it needs it becomes easy. It is the only cloud solution you need.

Troy Massey

Director of Enterprise Engagements

Iron Bow Technologies

IRON BOW® TECHNOLOGIES

Simpson goes a step further when discussing vendors, saying that having an established relationship with a vendor can actually prove beneficial, because it means they have a 'tactile sensitivity' to your environment. "These vendors may have more intimate dealings and experience with us so they understand some of the connecting fiber more than those vendors coming in cold. There are often nuances surrounding our solutions that impact the one-size-fits-all scenario. Often these nuances are not intuitive."

Looking at the migration process more broadly, Sparrow-Walker stresses the importance of thinking about data architecture and how all of the business systems fit together holistically; and to do so upfront. "Moving really quickly can create challenges, because cloud solutions that have been implemented in a vacuum without consideration for how they fit into an overall architecture will be limited in terms of interoperability. But moving too slowly when implementing enterprise capabilities can be problematic, because my constituents - people across the department - they're not going to wait. But they're also missing out on opportunity costs."

> "Find the right balance tempo, so you're meeting customer needs quickly enough, but also still giving thoughtful concern to the architecture of the cloud."
>
> — Michelle Sparrow-Walker
> Director of the Cloud Program Management Office
> Department of State

Research Methodology

GBC and Iron Bow launched a qualitative research campaign in May and June of 2019 that included a series of 30-minute interviews with federal government leaders regarding cloud migration efforts. The list of featured interviewees is as follows:

Michelle Sparrow-Walker — Director of the Cloud Program Management Office, Department of State

Todd Simpson — Chief Product Officer, Department of Health and Human Services

John Hale — Chief of Cloud Services, Defense Information Systems Agency

About Government Business Council

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 40 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

Report Author: Lucy Bierer

About Iron Bow Technologies

Federal agencies need to upgrade existing IT infrastructures to serve a connected citizen base and support a technology-driven warfighter. They must do this with austere budgets and legacy procurement processes that do not easily support the acquisition of modern technology and services. Iron Bow bridges this gap and provides leading solutions and expertise to help Civilian, Department of Defense (DoD), and DoD Healthcare agencies evolve. With over 30 years working with federal clients, we understand the unique technology, operations and procurement challenges the government market faces. Our technology solutions are designed with both compliance and security in mind, making integration into existing IT infrastructures seamless. Learn more at https://ironbow.com/irontarget/.

Endnotes

1. Federal Cloud Computing Strategy: "From Cloud First to Cloud Smart." https://cloud.cio.gov/strategy/. June 2019.
2. Ibid.
3. Ibid.
4. Department of Health and Human Services: "Overview of the Office of the Chief Product Officer." https://admin.govexec.com/media/cio_council_ocpo_20190419.pdf. May 2019.
5. GAO: "Cloud Computing - Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked." https://www.gao.gov/assets/700/698236.pdf. April 2019.