Q&A

Today's Government CIO

Evolving roles, new technologies and high expectations

"It's an exciting time to be a CIO — but it's also one of the scariest and most challenging."

So says Teri Takai, former CIO of the U.S. Department of Defense and the States of California and Michigan. Takai, now the Executive Director of the Center for Digital Government, joined Sreeram Visvanathan, Global Managing Director, Government, Healthcare & Life Sciences at IBM, during the IBM Government Cloud Virtual Cloud Summit to discuss the evolving role of the CIO.

What resulted was a wide-ranging conversation that touched on everything from the soft skills IT leaders need to thrive, to how they can best manage and secure multi-cloud environments, to what new technologies like artificial intelligence (AI) mean for the future of government work.

How do you see the role of the government CIO evolving?

TERI: Ten years ago, CIOs were back-office employees. It was about keeping things running and keeping costs down. Some CIOs then were doing breakthrough things, but now it's no longer a choice. They must do breakthrough things. Additionally, CIOs must not only keep up with emerging technologies but also maintain close relationships with other agency leaders and business partners.

They also can no longer take a back seat. They must be brave and be willing to have a seat at the table. In many many cases, CIOs are going to have to stand up and say, "I believe this is a direction the business needs to go in," or "I believe that agency services can and should be different than they are today."

SREERAM: CIOs also have external influences with which they must contend. The fundamental role of IT is to serve citizens and shape society for future generations. But government agencies are dealing with critical issues like preparing for population growth, dealing with climate change and natural disasters, and providing robust social services. They are also competing more heavily to attract businesses and investors to operate in their jurisdictions. In this macro environment, the role of the CIO is even more difficult as agency policy makers and process owners expect CIOs to operate with agility and speed, just like in the private sector. It is an exciting opportunity for CIOs to force the pace of innovation within government.

How much have we achieved in terms of digital transformation?

TERI: I think we are at the beginning. Transformation to me means transitioning from traditional siloed operations to thinking instead about how citizens look at services.

Teri Takai, former CIO of the U.S. Department of Defense and the States of California and Michigan

Sreeram Visvanathan, Global Managing Director, Government, Healthcare & Life Sciences, IBM

SREERAM: I agree with you. While we have put in massive systems of record and implemented a lot of mobile services, the way we deliver services hasn't changed behind the scenes. In a lot of cases, digital technologies have been used to reinforce existing processes rather than replace or reimagine them. That's what we see as the next step in the evolution.

Cloud has often been viewed as a cost-driven decision. Is this still the case?

TERI: I think that has changed and will continue to change even more dramatically. CIOs are now seeing cloud as an opportunity for increased flexibility, but also as tool that gives them better access to data. It's faster; it's cheaper; and it provides the opportunity to apply new technologies to data that was not possible before.

SREERAM: I think your point about data is massive. If you look at how governments leverage data, less than 20 percent of the data that could influence a policy or operational decision is being used. Data is not only in our systems of record or in a structured format, it's also unstructured. It's also not necessarily within government IT environments alone. It could be open source data or belong to a third party. The ability for governments to mine data and use it in real time to change what they do and how they do it is huge.

What are some of the trends as government agencies shift away from on-premises infrastructure?

TERI: At the federal level, programs like FedRAMP — which endorsed and certified government clouds — encouraged governments to move from their own data centers to government clouds and then slowly to public clouds. While state and local governments are interested in what the federal government has done, they have been bolder in looking at where they can move into the public cloud and what that really means. There is also a move to multi-cloud. In many cases the CIO may not know what those multi-cloud entities are going to be. Sometimes business leaders across the enterprise may procure those services themselves.

SREERAM: The reality is that you aren't in control of how many cloud environments exist in any enterprise today. They tend to creep up on you. Every single enterprise has a multi-cloud environment. Organizations are gravitating toward figuring out how they manage this multi-cloud environment. What capabilities do they need? What operational tools do they need to provision the right capacity when they need it to manage security?

Is security in a multi-cloud environment a key concern?

TERI: There are two ways of looking at it. There is a conversation around cloud being more secure in some cases than what a state, local or even federal government can provide in their own data centers. However, multi-cloud environments can complicate this. How do agencies ensure security when they are moving data from different clouds from different companies that may have different security standards?

In multi-cloud environments, government leaders also need to focus on things like identity management. CIOs must continue to think about insider risks, but their perimeter extends as they offer citizens the opportunity to utilize their data.

SREERAM: Yes, and cybersecurity isn't just about cybersecurity tools. CIOs need to look at their entire infrastructure and everything they are buying and using and figure out how it fits together to make sure it's secure. They also need to look at relevant policies, standards and enforcement that goes beyond just the tooling.

How do you see open standards and open source play out in this multi-cloud environment?

TERI: I think the role of open source is going to change and the questions will be around how CIOs can easily take services out of one cloud and move to another while maintaining security. Third-party data sources are also going to be important. The central question will be around how agencies bring open data together.

SREERAM: One of the positions we have taken at IBM is that it's ultimately about our customers having the choice so they can make decisions quickly, deploy applications from on-premises infrastructure to cloud and different cloud environments, and access different data sources no matter where they are to provide citizen services quickly and robustly.

Where are we in adopting AI today?

TERI: Our research points to a significant increase in government AI adoption. To some extent, that is because there are more tools in the market and there's more conversation about what governments can do with the technology, but it seems to be increasing at a rate that we haven't seen before and that I wouldn't have anticipated. It's moving so quickly that it's going to be tough for CIOs to keep track of it and not be chasing it as opposed to leading it.

SREERAM: Augmented intelligence — as we refer to it at IBM — has gone beyond proof of concept and trials and is becoming mainstream. Now the questions are around how we can embed the capabilities of man and machine to reimagine existing processes and workflows, especially when there is a lot of data involved.

This session is part of the IBM Government Cloud Virtual Summit, a free, online event featuring 17 sessions with insightful keynotes, illustrative case studies and deep dives into job-critical topics for government leaders. To view any of these sessions, visit govtech.com/ibmvirtualsummit