How Open Innovation Can Transform the Government Technology Playing Field

By Daniel Chenok

"Open" tournaments in sports—such as the U.S. Open in tennis or golf—bring together the best players in the world, and the public sees high performance achieved as the field narrows. But a key feature of open competitions is the possibility of new entrants who bring innovative play to qualifying tournaments that precede the main tournament. These new entrants can develop approaches that allow them to raise the level of play for all players based on creative strategies, and strong execution.

While not a perfect analogy, a similar spirit is enabling open innovation in the development of new technologies by players in the government IT market. The past decade has seen a rapid shift to open government and open data as key principles for agencies, starting with the advent of the Open Government policies of the Obama Administration in 2009. These policies have been supported through the recent passage of legislation, including the OPEN Government Data Act of 2018 and the highly visible expansion of the Federal Data Strategy in the President's Management Agenda. The implementation of these efforts has brought new entrants to the development of new applications that add value to government data.

Government is now at the cusp of a similar leap forward through the advancement of open digital platforms that drive new technologies, which allow agencies to achieve better and more efficient results in serving the public. Open IT transformation rests on three pillars, expanded on below:

- **An interoperable infrastructure** allows agencies to access and integrate across multiple, secure cloud-based systems.
- **Cloud-based platforms,** in turn, speed the secure development of new technology applications, including robotics process automation (RPA) and artificial intelligence (AI).
- **Advanced technologies like these** set up the next wave of innovation and massive expansion of accessible data that will arise with the advance of 5G wireless networks and even quantum computing.

Interoperable Infrastructure

The government's use of cloud computing has evolved considerably since this term became associated with the ability of agencies to access their IT through providers that were not housed within their internal networks. It was 10 years ago this month that the IBM Center published one of

***Daniel Chenok** is Executive Director of the IBM Center for The Business of Government.*

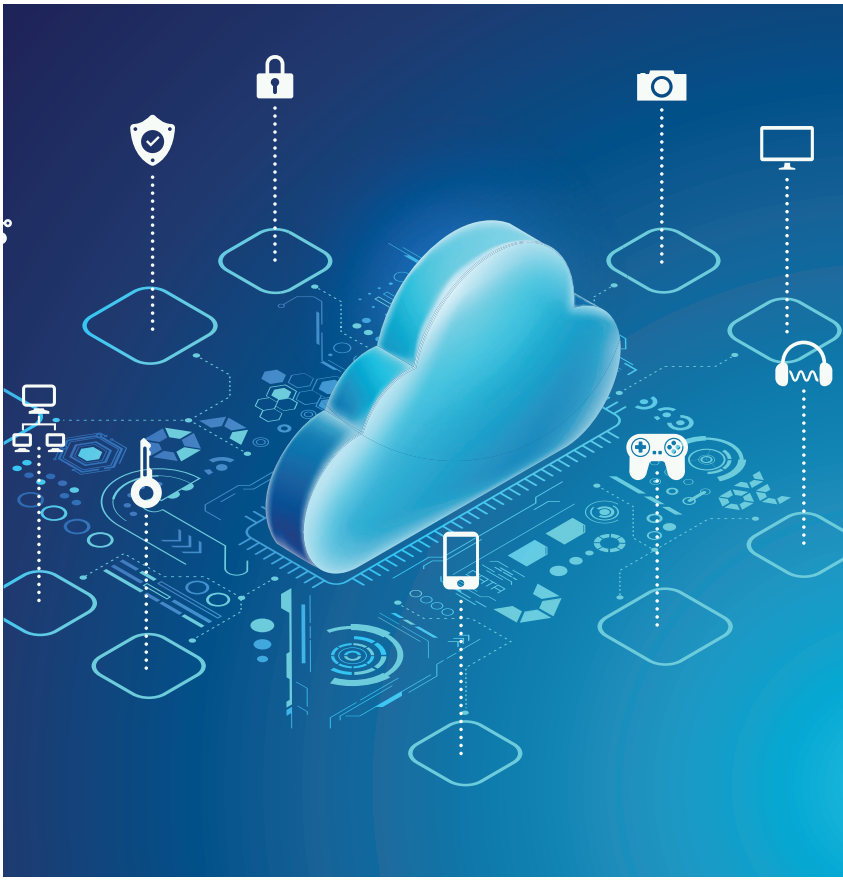
the first studies on government use of cloud computing, *Moving to the Cloud: An Introduction to Cloud Computing in Government,*[1] which described early applications, challenges, and opportunities from this emerging paradigm. The report noted that a key challenge to effective implementation was "the need for open standards and interoperability."

In 2011, the Office of Management and Budget (OMB) issued a Federal Cloud Strategy that included the "Cloud First" policy.[2] This policy provided guidance to agencies to leverage the cloud-based approaches of infrastructure, software, and platform as a service as first preferences for new IT investments. OMB noted that migration to the cloud would enable agencies to "tap into private sector innovation" and encourage an "entrepreneurial culture"— both of which are also benefits of open networks.

Cloud First remained in place until OMB updated the policy as "Cloud Smart"[3] in September. 2018. Cloud Smart focused on expanded agency capacity to bolster security in the cloud, procure effective and leading-edge commercial solutions, and enhance the skills of IT workers in cloud-based applications. The update also called on agencies to "conduct regular evaluations of customer experience and user needs" and to "track their growth in areas where decisions about technology intersect other disciplines." Both of these actions are optimized only if done as part of an open ecosystem promoting feedback and engagement.

The technology behind cloud platforms now available to government has advanced to the point where secure, effective operations can be achieved over multi-cloud networks that rely on open standards to achieve interoperability and improve portability of workloads and data between clouds. This trend applies regardless of whether agencies rely on "public" commercially available systems, "private" systems that reside inside agency computing environments, or "hybrid" systems that link the two across an agency enterprise. Importantly, multi-cloud approaches enable development of new innovation that does not rely on a single network, expanding the scope of application development resources across open networks.

This is a key success factor behind IT modernization for agencies often still dependent on legacy systems. As noted in the IBM Center's March 2018 report *A Roadmap for IT Modernization in Government,*[4] federal agencies can learn from the experience of commercial and state government CIOs who embraced open innovation strategies to modernize outdated infrastructure in a phased "two-speed" approach. Such an approach enables modernization toward the cloud to proceed in phases of rapid change followed by stabilization of that change.



New Applications

Government has made recent and significant progress in building networks of practitioners interested in collaborating across a broad suite of emerging technologies. Within the government, new communities of practice have advanced around RPA and AI. In addition, government-industry collaborative associations have seen a surge of interest in groups like the American Council for Technology and Industry Advisory Council (ACT-IAC) Emerging Technology Community of Interest.[5]

Several IBM Center reports have helped identify early innovators in government use of AI and other emerging technologies, including:

- Delivering Artificial Intelligence for Government: Challenges and Opportunities[6]
- More Than Meets AI and More Than Meets AI—Part II[7]
- Financial Management for the Future: How Government Can Evolve to Meet the Demands of a Digital World[8]

A common theme across these reports involves the need to build new applications over modernized and cloud-based infrastructure. As noted in *Delivering Artificial Intelligence,*[9] "upgrading IT infrastructure to support AI systems, leveraging cloud computing strategies" can help agencies better identify "data intensive applications that can benefit from AI." Similarly, the *Financial Management for the Future*[10] report finds that development of RPA applications alongside AI can drive advanced analytics through "intelligent automation"—enabling government "digital workers" who work in an open eco-system as part of an "orchestrated team capable of decision making, evaluating, and self-healing to continuously improve."

As with the benefits of open approaches to the cloud discussed above, open application development can leverage open source software networks to accelerate the pace of innovation by bringing IT professionals together to work across an enterprise and access commercial best practice. If an agency's IT workforce is saddled by static infrastructures and closed systems, then the introduction of new technologies will be constrained by the capacity of those systems for change. In contrast, an open approach to application development expands the playing field of ideas, prototypes, and pilots for new innovation considerably. In addition, from a workforce perspective, openness helps increase the job pool of qualified professionals as opposed to siloed applications that only a few know how to use and maintain. This is growing in importance as government employees reach retirement age at an ever-increasing rate and the public sector competes for talent with the private sector.

Government teams and stakeholders often face questions about security in an open technology ecosystem. A traditional approach to managing IT risk involves closing the aperture at the technology perimeter—building strong firewalls that protect agencies from online threats. In the evolving era of open innovation, security must be addressed as part of—rather than separate from—infrastructure and application development. The longstanding principle of "security by design" is more important than ever before in implementing open strategies for both industry and government, and remains a key element of cybersecurity risk management for government. As noted in last year's IBM Center report, *Managing Cybersecurity Risk in Government,*[11] "Setting up a disconnected intranet is expensive and could stymie innovation and efficiency that occur by leveraging solutions developed on the open Internet."

This concern is not new. In 2011, I wrote in this space an article entitled "Secure Transparency: Why Cybersecurity is Vital for Long-Term Success of Open Government,"[12] noting that if open, "public-facing information systems are disrupted through a cyberattack or their information is compromised through cyber 'exfiltration' . . . the online foundations of open government will be called into question as pressures mount to increase security walls and limit citizen access." Rather than being antithetical, security must be a key part of open innovation.

The Next Phase: Advanced Computing Power

The open innovation strategies outlined above will only rise in importance, as speed and access over open networks increases considerably with the emergence of 5G to share information and quantum computing to develop systems and process data. The speed of technological change will continue to accelerate, as will government, industry, and public demand for faster response times, personalized services, and security. By embracing the benefits of open infrastructure and application development, agencies can provide a secure channel for engaging with their government and industry counterparts—enabling the development of open data that in turn fuels new innovation.

Making government open to innovation across open platforms will clearly enable everyone to be a winner in any "Innovation Open."

Footnotes

1. http://www.businessofgovernment.org/report/moving-cloud-introduction-cloud-computing-government
2. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf
3. https://cloud.cio.gov/strategy/
4. http://www.businessofgovernment.org/report/roadmap-it-modernization-government
5. https://www.actiac.org/emerging-technology-community-interest
6. http://www.businessofgovernment.org/report/delivering-artificial-intelligence-government-challenges-and-opportunities
7. http://www.businessofgovernment.org/report/more-meets-ai and http://www.businessofgovernment.org/report/more-meets-ai-part-ii
8. http://www.businessofgovernment.org/report/financial-management-future-how-government-can-evolve-meet-demands-digital-world
9. http://www.businessofgovernment.org/report/delivering-artificial-intelligence-government-challenges-and-opportunities
10. http://www.businessofgovernment.org/report/financial-management-future-how-government-can-evolve-meet-demands-digital-world
11. http://www.businessofgovernment.org/report/managing-cybersecurity-risk-government
12. http://www.businessofgovernment.org/sites/default/files/Chenok.pdf