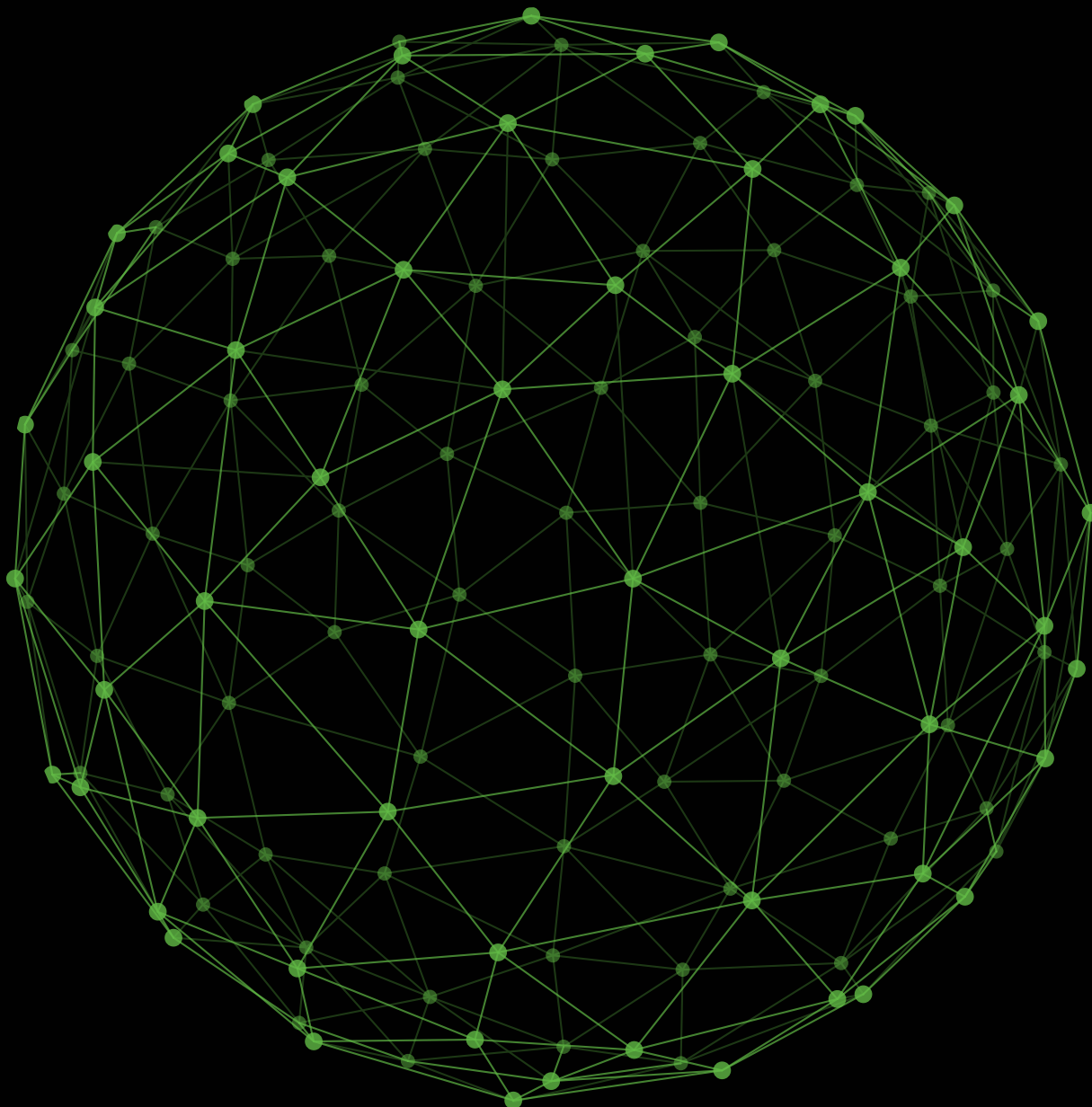


Deloitte.



**Federal Civilian Agencies
Industry Perspective**

Executing missions and fulfilling
expectations in the digital age

How are civilian agencies positioned in terms of their missions and expectations?

While their basic missions have remained essentially unchanged, the pressures on civilian agencies have intensified due to three forces. First, citizens now expect service experiences akin to those they encounter every day in the commercial sector; that means being able to access services and their information instantly and easily from any device, anytime, anywhere. Second, agencies face an explosion in the volumes and types of data they must deal with; this provides tremendous opportunities for data-driven decision making as well as new risks. Third, the industries that agencies regulate – such as banking, investing, transportation, energy, telecommunications, health care, and agriculture, among others – are undergoing disruption; agencies not only need to keep abreast of those changes, they also must play new roles as those industries transform themselves.

What's driving these changes?

The main drivers are the widespread digitalization of processes, transactions, relationships, and even currencies, and the digital transformation agencies must undergo to respond to those developments. Digitalization will continue to transform virtually all sectors. Telecom and broadcasting have been revolutionized. Smart cities and autonomous vehicles are becoming realities. Healthcare is adopting digital monitoring of treatment outcomes. These and similar developments, along with constantly evolving regulations and technologies, mean that civilian agencies should consider enhancing their decision making and mission execution through digital transformation.

Given that, what are the key issues for civilian agencies today?

They come down to opportunities and risks. Opportunities to enhance mission delivery through advanced analytics enabled by cognitive technologies, such as scanning, artificial intelligence, and machine learning, are there for the taking. These capabilities can be accessed in various ways, notably through cloud services. The risks arise because as an agency becomes more digital, its cyber footprint and threat surface expands, creating the need to reassess and strengthen its cyber posture. Also, digitalization creates new models, for example hybrid on-premises and cloud-based data storage and systems, so agencies must identify and manage new cyber threats.

In general, civilian agencies need to adapt cognitive technologies to their missions and scale them up quickly, while updating cyber security to meet the challenges of an evolving digital landscape.

1 [A government perspective: Tech Trends 2018 – The symphonic enterprise](#), 2018 Deloitte Development LLC

2 *ibid.*

3 *ibid.*

How are agencies moving beyond identifying opportunities to executing them?

Agencies have begun to realize that transformation must be among their top priorities and that cognitive technologies can enable mission execution. That realization seeped into civilian agencies from business and the culture, and from the defense and intelligence sectors. Specific drivers such as the President's Management Agenda (PMA), the executive order on AI, and the General Services Administration's (GSA's) IT Centers of Excellence have also ripened the agency ecosystem for digital transformation. Now, most civilian agencies are moving from identifying opportunities and experimenting with cognitive technologies, to putting innovations into production and scaling up.

For example?

The Census Bureau created an "enterprise data lake" to support the goal of applying secure, scalable data science to enable survey processing and analysis, research, data linking, and predictive analytics. This enabled Census data scientists to spin up analytics tools on demand and analyze gigantic data sets to draw conclusions, find new patterns, and more.¹

The USPS Informed Delivery™ capability created a digital reflection of the supply chain, enabling users to preview their mail and manage their packages through email, an online dashboard, or a mobile app. This gave consumers a view of their physical mailbox through digital channels.²

The Department of Treasury researched and prototyped the use of blockchain to digitally trace its smartphones, computers, and other physical assets. This replaced a manual process that took months, while providing an instant view of inventory to improve audits and asset management.³

In each of these examples, likely next steps would center on putting these capabilities into production, embedding them more broadly into operations, and scaling them up to achieve greater reach and impact across the agencies' respective missions.

What are the keys to success in digital transformation?

It really requires leadership, clarity about the challenges, and the right resources. Given the complexity of a civilian agency, it's natural to see transformation as complex, but those who succeed tend to take action, with the understanding that it will be an iterative journey. They also take a broad view in that digital transformation is not primarily about the technology. It's about your mission, strategy, operating model, processes, and people and culture.

Taking action starts with defining specific, achievable goals related to what you need to learn, monitor, control, and deliver, and to other dimensions of your mission. Then, you can identify early, easy wins, launch pilot programs, develop business cases, and create successes you can replicate across the organization.

You also have to get ahead of the funding cycle and allocate budget to execution. The people with the ideas and know-how in an agency aren't necessarily positioned to allocate budget and get things done. The leadership has to identify those people and their best ideas and provide the needed funds.

What can help accelerate the journey?

Among other things, moving to the cloud and tapping the right people. The cloud can help agencies leapfrog the limitations of their legacy systems and scale up new capabilities faster. FedRAMP provides a standardized approach for agencies using cloud services, but the cloud is never “set-it-and-forget-it” when it comes to security. Agencies need clear, specific definition of their—and their service providers’—roles and responsibilities, plus continuous monitoring of security and performance.

Tapping the right people is essential. For example, there's a shortage of experts in cognitive technologies, advanced analytics, and data protection. Agencies should consider independent contractors, co-sourcing, outsourcing, and even crowdsourcing, which some have used. The workforce of the future will increasingly consist of professionals working in processes augmented by cognitive technologies. The sooner an agency gets comfortable with those technologies, the sooner it will be able to leverage them to create the workforce of the future.

Cybersecurity teams need to understand the risks around new technologies and ways of assessing, managing and monitoring them. Otherwise, they may perceive those risks as unfamiliar and unmanageable and resist accelerated adoption. This often represents a cultural shift as well as an upskilling challenge.

An agency looking to accelerate its progress should also consider application modernization. An “app mod” initiative creates an understanding of legacy code and its business functions, and—when done right—facilitates automated transformation of legacy code into modern coding languages. This can enable an agency to accelerate adoption of cloud, mobile, digital business, advanced data analytics, and other technologies.

What about the opportunities and risks associated with the workforce of the future?

The opportunities include exponential gains in efficiency. For example, text scanning technology coupled with a bot programmed to, say, process a tax return, a loan application, or an insurance claim can eliminate hours, days, or weeks of repetitive tasks. This frees up human resources to engage in higher-value intellectual work requiring judgment and emotional intelligence. Once an agency makes a process more efficient, it can move to making it more effective through further process improvement.

The risks include exponentially replicated errors. If a bot can process thousands of applications compared with dozens handled by humans, then it may generate thousands of errors even faster. Also, as a cognitive technology “learns,” it can start to discriminate for or against citizens in certain groups or with certain characteristics in ways that would be undesirable, unfair, or even illegal. So, the human factor will remain essential.

Critically, to help employees understand and embrace the improvements for them, agencies must engage in active change management, develop talent strategies, reallocate human resources, and invest in reskilling workers.

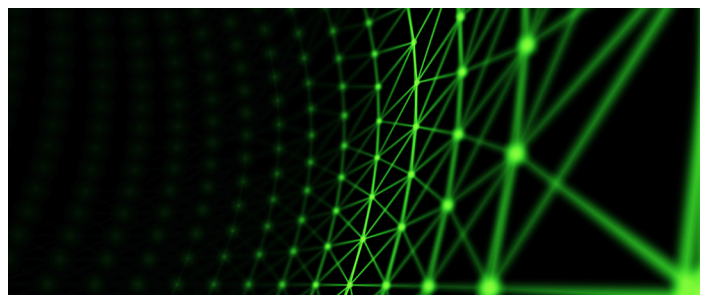
Where does cybersecurity fit in all of this?

As agencies move to delivering services how, when, and where citizens want to access them, security threats and vulnerabilities inevitably increase. When providing access through online, phone, email, and other channels, digital identity becomes more important. How can the agency always know who it is dealing with? How can it provide the secure but frictionless customer experience that private-sector ecommerce usually provides? Getting the right answers is essential to achieving security while meeting increasing expectations.

In addition to regulating industries that are themselves being disrupted, civilian agencies play a key role in protecting critical infrastructure. Given this, we believe they will often need to work more closely, and differently, with the industries they oversee and serve. To ensure that our increasingly interconnected—and therefore increasingly vulnerable—infrastructure remains safe and resilient, they need to set standards, share information, and coordinate responses. This implies that transformation means not only delivering existing services in better ways, but also the possibility that the nature of the services may change.

What would you say are potentially the most impactful steps a civilian agency can take to advance its strategic agenda?

Most agencies could see the greatest impact by setting a vision for their future, applying cognitive technologies and data-driven decision making to achieving that vision, and accessing needed talent in an efficient manner. At the tactical level this entails identifying areas that can provide early wins, launching pilot programs, developing business cases, and then scaling up and replicating successful initiatives across the organization.



Author



Kavitha Prabhakar

Government & Public Services Civilian Sector Leader

Deloitte Consulting LLP

kprabhakar@deloitte.com

+1 773-620-0784

<https://www.linkedin.com/in/kavitha-prabhakar-ba823a77>

https://twitter.com/kavitha_prbhkr

Deloitte.

This document is confidential and it is not to be copied or made available to any other party. Deloitte LLP does not accept any liability for use of or reliance on the contents of this document by any person save by the intended recipient(s) to the extent agreed in a Deloitte LLP engagement contract.

If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities).

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NWE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NWE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.