Delivering on Mission Priorities: New Pathways to Achieve Key Government Outcomes

By Daniel Chenok
(with contributions from IBM colleagues Chris Ballister, Chris Trainor, Matt Spaloss, and Mark Fisk)

Effective and innovative approaches for managing people, processes, and technologies can support agencies to deliver critical missions effectively, bolstering the government's ability to serve the citizen and protect the nation.

Enabling the public sector to deliver on its mission priorities remains a major research theme of the IBM Center for The Business of Government. Making this vital connection between outcomes that agencies strive for on behalf of the citizens they serve and the good management needed to achieve those outcomes is a critical link for effective government.

As we collaborate with government stakeholders in meeting this objective, a number of specific mission areas have great importance for the nation and call for further work to identify pathways for strengthening performance. Each of these areas features several distinguishing elements:

- They have broad impact on citizens, businesses, and other governments, and in some cases international partners.
- They are implemented through networks of agencies working together. None are the province of a single organization; all rely on a strong collaborative approach.
- Partners from outside government can be a source of innovation and creative solutions to help government succeed.
- Achieving positive outcomes depends on bringing together people, process, and technology in a strategic management framework that enables the mission.

Developing approaches that help agencies find new pathways to achieve key mission outcomes will be a high priority for the IBM Center over the next several years. We will seek to do so in new ways to engage government through joint exploration of innovative ideas, interaction around potential solutions, and the ability to foster rapid action and iterative learning. Especially as a new administration takes office in January 2017, we will work with colleagues across government, academia, industry, the non-profit community, and IBM to jointly develop thought leadership and actionable recommendations that help government serve the nation efficiently and effectively. Moreover, we welcome ideas from government stakeholders about specific issues to address—ideas that can help frame the art of the possible.

These activities focus on four areas that share the distinguishing elements described above, and address two of the most important roles for government: to serve the citizen and to protect the nation. Specifically, this focus includes helping government across the following mission areas:

- Engaging Citizens to Meet Evolving Needs
- Transforming Operations to Improve Programs

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

- Strengthening Threat Prediction and Prevention
- Enhancing Cybersecurity

Each will be discussed in more detail below.

Engaging Citizens to Meet Evolving Needs

In the last several years, innovative ways to provide services have enabled a revolution in engagement in the private sector. Self-service, new approaches to raise customer satisfaction, analytics, and cognitive computing platforms have all combined to improve user experience across many parts the economy and society. Government is starting to do the same via increased use of design thinking and similar techniques, in order to successfully deliver services within an agile enterprise.

These approaches can be harnessed to streamline benefits for citizens in need; enhance the experience of those working with government to better match what they have come to expect when interacting with the best companies in the private sector; and involve the public in framing public policy through crowdsourcing, sentiment analysis, and similar innovations. Working with citizens and with advocacy organizations that represent citizen interests allows agencies to take advantage of these new approaches and digital interactions with government agencies as a key engagement point.

Commercial enterprises—for example, leading retail firms—have already developed best practices to engage citizens—termed "consumer engagement points." Within government, one could define a set of specific Citizen Experience Points (CEPs) where a citizen's or an advocate's input would be sought for the co-creation process. Leveraging these CEPs would be a great place to begin a dialogue among the various stakeholders in the process, whether it is agency mission, agency IT, citizen, or other organizations. Moreover, new technologies available through cognitive and analytics are gaining in maturity, making them ideal candidates for consideration as viable solutions within the public sector. And new initiatives (such as the Federal Front Door program) are being developed to address customer service, customer satisfaction, and to improve public-government interactions.

Government can move forward with positive, citizen-focused engagement in developing policies and applications that touch millions of Americans. Consider the streamlining of the Free Application for Federal Student Aid (FAFSA) that is filled out by millions of Americans seeking financial support for higher education each year. The Obama Administration's recent announcement of a Core Federal Services Council to focus on improving performance in key citizen-facing programs provides a great opportunity to help agencies better serve their constituents. The OMB Memorandum announcing this body states, "The Council will improve the customer experience by using public and private sector management best practices, such as conducting self-assessments and journey mapping, collecting transactional feedback data, and sharing such data with frontline and other staff."

Transforming Operations to Improve Programs

Government has moved forward with initiatives that leverage modern operating practices in the private sector to improve productivity, including shared services, IT modernization, data management, and program integrity to reduce fraud and waste. Less clear has been the connection between these best practices and how they might bring about measurable improvements at the program level, especially social programs that deliver critical health, education, workplace, and other benefits. Evolving process and technology platforms that leverage cloud, agile, and cognitive computing can help agencies to improve operations, increase visibility into both current assets and costs, and support compliance with legal and policy requirements.

Modernizing these platforms can enable agencies to better understand citizen satisfaction and subsequently design improved services that make a real difference in the lives of people who interact with government.

- **New Platforms, New Ideas, New Approaches.** Digital transformation has the potential to replace obsolete models for delivering government services. It's not merely more process improvement or another IT upgrade; it's about significantly transforming the way government delivers services. We have already seen digital transformation disrupt industries and transform businesses, and we expect a similar transformation from our government: services delivered anytime, anywhere, on any device. This transformation includes cloud-enabled capabilities, with strong cybersecurity, as well as the use of analytics and cognitive capabilities to improve mission delivery. It also means using new methods, like design thinking and agile computing, to more precisely focus on mission value (more on these two areas below).

- **Design Thinking, Agile, and Enterprise Scale.** Design thinking starts with the user experience. It provides a framework to deliver great user outcomes at an enterprise scale. It brings a multidisciplinary team and a spirit of restless reinvention. The result is a powerful behavioral model and a set of key practices to scale design thinking to even the most complex projects. Agile combines leadership, collaboration, and delivery practices to implement those user outcomes on digital platforms. Technology might be an enabler, but the focus on user outcomes is the key to success.

- **Cognitive and Big Data Transformation.** Today, 80 percent of the world's data is unstructured, meaning it is contained in documents and images. Until recently, computers could only record and store this data. Cognitive systems understand, reason, and learn to make sense of it. Now think about regulatory agencies and their need to use unstructured data to enforce compliance. The potential to find and resolve public safety and legal issues is tremendous. But agencies need to process massive datasets to discover and prioritize potential regulatory issues. Cognitive solutions can sift through massive amounts of unstructured industry data and analyze it across multiple dimensions, without bias. This allows regulators to focus on higher value analysis and investigation. And as government datasets continue to grow over the next several years, cognitive solutions can scale with them.

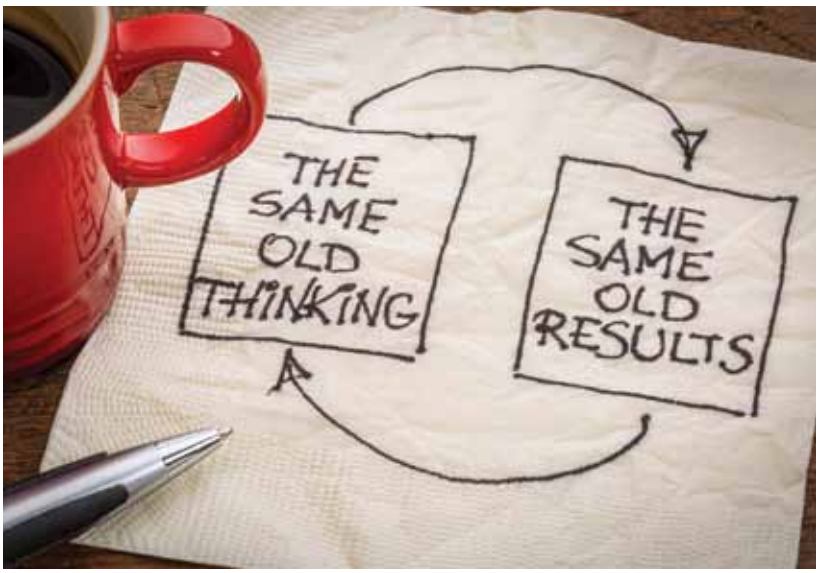
- **IT Modernization.** President Obama requested $3.1 billion in next year's budget for IT modernization, and OMB is developing a policy and putting together a plan for that funding. The idea is to invest in aligning government services with the latest technology practices. This has the potential to improve government services by focusing on modernizing the underlying technology. This includes migrating to cloud platforms, integrating cyber security into applications, and breaking down application and data silos. It is also intended to cut costs. The

hope is that the savings generated by this $3.1 billion investment yields reduced operating costs, which the government can spend on additional IT modernization in subsequent years. Done right, this could be a self-sustaining investment that yields returns for decades to come. Since current legacy systems often limit the capability to securely scale and bring enterprise services to the citizen, modernized systems will allow new capacity for citizen-facing capabilities.

- **Shared Services at Scale.** Government shared services have the potential to improve outcomes, increase compliance, and reduce cost. Such services also allow employees to be redirected to mission-critical tasks. Yet a recent McKinsey & Company article shows significant underinvestment in this realm. Only 22 percent of the shared-services organizations studied are building capabilities in automation. Less than 20 percent of them are streamlining internal operations through analytics. And only about 10 percent are using analytics for external use to support the business. Shared services hold the promise of being a key contributor to the government digital transformation.

Strengthening Threat Prediction and Prevention

There is perhaps no more urgent mission for government than public safety and national security. Global threats require collaborative approaches to leverage organizational and technical innovation across the national security, homeland security, and law enforcement communities. Moreover, they require all levels of government to work in concert with civic and community leaders and advocacy organizations. Approaches like image recognition and social media analysis can be managed as part of a larger strategic framework to help identify early warning signs of radicalization threats; better target potentially dangerous people and cargo while increasing the speed and overall experience for the vast majority of travelers; improve management of emergencies and related incidents; and support enhanced performance in correctional institutions to foster reduced recidivism and other desirable outcomes. A strong government approach to threat prediction and prevention will address more specific acts or instances of crime, national security or border security threats, and military preparedness—all by identifying patterns that exist in disparate data feeds, and combining them to generate new insights.



Another aspect of threat prediction and prevention is to help a human analyst monitor vast and increasing stores of data. Today's data sources are so numerous that an analyst cannot possibly track all of the relevant information needed. Machine assistance and cognitive computing approaches will help government sort through all of the available data sources, and point human analysts relevant information that they can act on in a timely way to get ahead of threats before they arise, and respond more rapidly and precisely to address incidents that may occur.

By assessing government data feeds into alongside open source, social media, and similar information resources, agencies can generate anticipatory intelligence that can be acted upon to predict, prevent or mitigate threats. Industry can work in partnership with government to ensure that what we create is useful to solve government challenges.

Enhancing Cybersecurity

Like the private sector, the government must detect and respond to threats in cyberspace at an increasing rate, from a growing and complex landscape of malicious actors. Yet it must do so in a way that enables and does not impede the technologies that serve citizens, businesses, state and local governments, and other partners. Threats arise from a range of places: insiders to commercial hackers to organized crime to foreign actors. Today's CIOs and CISOs have a dual challenge of achieving effective security protection while meeting compliance requirements—all against a backdrop of shrinking budgets.

In order to evolve from reactive protection into proactive and predictive security, agencies require systems that analyze,

predict, and defend against problems in real time; provide protection for large IT systems as well as handheld and other "edge" devices; understand how personnel risks from employees or contractors can manifest into broad cyber risk, and how to identify and respond to minimize those risks; and leverage new approaches like biometrics to enable efficient access for legitimate users while impeding access for those who would bring harm. And all of these responses depend critically on providing for privacy of information held by government on behalf of its citizens.

To be effective in their security efforts, agencies must be proactive—using cyber analytics and cognitive-based systems to develop true security intelligence. No longer can security programs rely on an "If it's not broke, don't fix it" approach; adversaries could already be inside systems, stealing data or probing for weaknesses. Too many CIOs and CISOs have considered their systems and data secure when in fact they were riddled with vulnerabilities.

Security programs need effective protection of valuable information and systems to prevent data breaches and to comply with the ever-increasing federal compliance requirements. Among others, there are the Federal Information Security Management Act (FISMA); the Privacy Act, policy and guidance from the Office of Management and Budget and the National Institute for Standards and Technology; the General Services Administration's Federal Risk Authorization and Management (FedRAMP) program; and the Federal Acquisition Regulation (FAR) to be considered.

With massive increases in data, mobile devices and connections, security challenges are increasing in number and scope. The aftermath of a breach, which can result from internal or external threats, can be devastating to an organization in terms of both reputational and monetary damages.

- **External threats.** The nation faces a proliferation of external attacks against major companies and government organizations. In the past, these threats have largely come from individuals working independently. However, these attacks have become increasingly more coordinated, and are being launched by groups ranging from criminal enterprises to organized collections of hackers to state-sponsored entities. Attackers' motivations can include profit, prestige, or espionage. The vector known as Advanced Persistent Threat requires specialized continuous monitoring methods to detect threats and vulnerabilities prior to breaches or loss of sensitive data.
- **Internal threats.** In many situations, breaches come not from external parties, but from insiders. They might be employees, contractors, consultants and even partners and service providers. The causes range from careless behavior and administrative mistakes (such as giving away passwords to others, losing backup tapes or laptops, or inadvertently releasing sensitive information) to deliberate actions taken by disgruntled employees. The resulting dangers can easily equal or surpass those from external attacks.

A strong security program must include capabilities to predict both external and internal threats and assess their mission impacts, validated by cognitive technology and cybersecurity experts serving mission operators.

To address external, internal, and compliance challenges through a proactive approach, mission-oriented cognitive cybersecurity capability is needed. To achieve such capability, four key areas must be addressed:

- **Security architecture effectiveness.** Agencies must focus on rapidly accessing vulnerabilities in the security architecture and developing a prioritized road map to strengthen cyber protection that plugs security gaps and meets policy expectations. Ensuring the identity of users and their access rights while reducing the number of privileged users is critically important to effective security architecture.

- **Critical data protection.** Agencies must focus on rapidly accessing the data architecture and uncovering shortfalls in tracking and protecting critical data. Prioritized action plans can reshape data architecture for more focused security protection and improved continuous monitoring.

- **Security compliance.** Agencies must focus on quickly addressing compliance gaps and establishing a roadmap to prioritize issues, develop appropriate policies and controls, and achieve compliance.

- **A holistic security program.** Effectively implementing the first three areas above enables agencies to lay the foundation of a program that addresses risk management and IT governance at the enterprise level. Organizations can then identify risks to critical business processes that are most important to mission success, as well as threats and vulnerabilities that can impact critical business processes.

Conclusion

Each of these four areas will benefit from reports, discussion, rapid development of ideas, and co-creation of solution approaches to help government manage more effectively and achieve positive outcomes. The IBM Center for The Business of Government looks forward to developing thought leadership and creative approaches to support agencies in addressing these critical mission imperatives. In this ongoing effort, we seek to enable government leaders and managers with innovation that will both serve the citizen and protect the nation. ◘