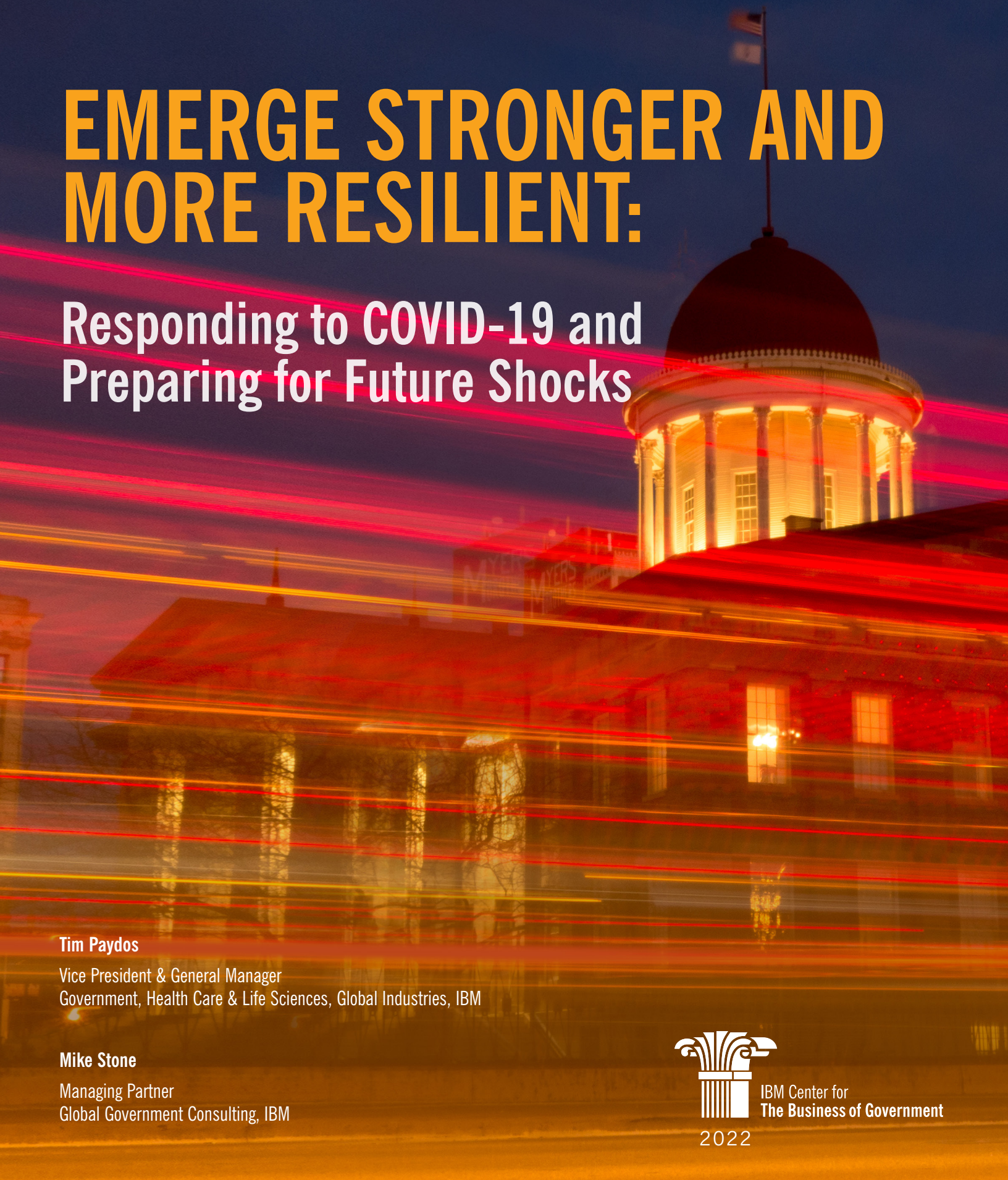
SPECIAL REPORT

IBM Center for The Business of Government

EMERGE STRONGER AND MORE RESILIENT:

Responding to COVID-19 and Preparing for Future Shocks



Tim Paydos

Vice President & General Manager
Government, Health Care & Life Sciences, Global Industries, IBM

Mike Stone

Managing Partner
Global Government Consulting, IBM

IBM Center for
The Business of Government

2022

Special Report

Emerge Stronger and More Resilient: Responding to COVID-19 and Preparing for Future Shocks

Tim Paydos

Vice President & General Manager
Government, Health Care & Life Sciences
Global Industries
IBM

Mike Stone

Managing Partner
Global Government Consulting
IBM

IBM Center for
The Business of Government

2022

Table of Contents

Embracing the new urgency to harness technology (during the pandemic), leading governments scaled to meet demand, delivered entirely new services, and supported new ways of working.

Foreword

Daniel J. Chenok
Executive Director
IBM Center for
The Business of Government
chenokd@us.ibm.com

In responding to the unprecedented challenges of a global pandemic, stable and effective government action has been key to managing through the crisis and addressing longer-term implications for the health and safety of nations. Moreover, collective strategies have led to identification and resolution of challenges in way that brings together government leaders, scientists, data analysts, health care organizations, academic institutions, and industry.

This new report, *Emerge Stronger and More Resilient: Responding to COVID-19 and Preparing for Future Shocks,* is by IBM Global Government leaders Tim Paydos and Mike Stone, as well as a set of contributing authors and IBM experts in a broad range of public sector issues. It builds off a series of blog posts to frame a roadmap for the public sector on strategies and actions to move forward.

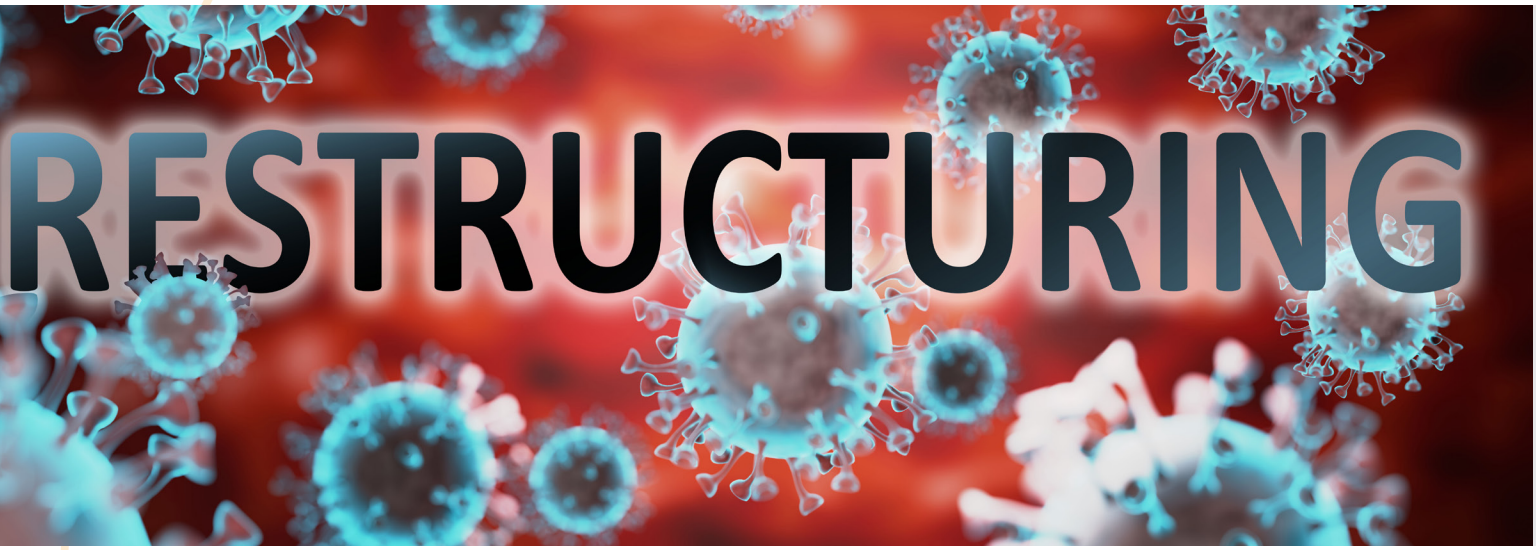
The report emerges from the context of this unanticipated, often wrenching historical moment. As governments have led response activity through a global emergency, they have sought to manage impacts to their agency missions and citizenry. At the same time, the advent of emerging technologies has catalyzed action, both to respond to current conditions and to build capacity for the aftermath of COVID-19, as well as for preparation of future crises. Some of these technologies include:

- **Artificial intelligence and cognitive analytics** to help focus testing and vaccine distribution, predict where the virus will spread, and match resources to demand
- **Hybrid cloud computing models** that allow new systems to link with existing infrastructure seamlessly
- **Mobility tools and infrastructure** to ease the intensifying strain on citizen services and to enable distance work
- **Self-service tools** for the public to access and receive services to help maintain physical and mental health, income, and public safety

This technical infrastructure of the twenty-first century provides a strong foundation for advancing government actions to move forward from COVID-19 in a way that advances the health of nations. In the longer term, such movement can enable the public, private, and nonprofit sectors to work together in addressing important challenges for society, including:

- **The changing nature of remote and hybrid workplaces** that provide opportunities for reskilling and addressing worker health and safety
- **The transformation of government organizations** and operations to focus on cross-boundary collaboration and shared analytics to develop policies and programs around public needs
- **The building of trust** among government and the public interests, based on well-delivered services that are effectively communicated from agencies to the citizenry

The report provides insights and highlights opportunities for government to address these challenges. It includes essays that focus on promoting digital enablement of citizens, modernized supply chains, strong cybersecurity, and emerging analytics frameworks. The report concludes with a call to action for governments and their partners to work together—in an effort to emerge stronger and more resilient from our collective experience—and build a better society.



COVID-19's final phase: How governments can emerge stronger, more resilient

Authored by Mike Stone

As the pandemic consumes less of their bandwidth going forward, governments must therefore continue to invest and reinvest in emergency preparedness, including the policies, relationships, communication streams, technologies, and physical infrastructure that will expedite future response efforts.

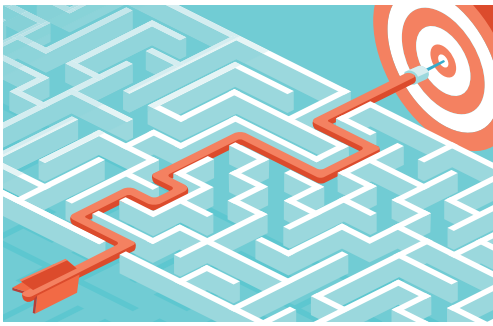
In the nineteen months since the World Health Organization announced a peculiar coronavirus-related pneumonia in Wuhan, China, COVID-19 has turned families, businesses, and communities upside-down and inside-out. And also governments. From the U.S. to the U.K., from France to the Philippines, and from South Korea to South Africa, they were as thrown off-guard as anyone. More so, even. While the rest of us were mere passengers, they were the public-health pilots of an aircraft that had to be designed, engineered, and rebuilt—all in mid-flight.

There was ample turbulence, to be sure. Remarkably, though, government leaders managed to keep the plane aloft through the first two phases of what was predicted to be a three-phase pandemic.

Top challenges: Then and now

Phase I was devoted to emergency response and business continuity. Together, organizations and governments collaborated to track the pandemic's spread, to support underprivileged students who suddenly shifted to virtual learning, and to modernize unemployment agencies' systems to accommodate surging requests for citizen benefits.

Phase II was all about recovering and rebuilding. Again, organizations teamed up with their government partners to tackle mission-critical problems like contact tracing, return-to-workplace, and exposure notification.



Now, most of the world finds itself waist-deep in Phase III, during which governments must build strength and resilience in order to emerge from the pandemic more ready for the next global crisis than they were the last. But that's easier said than done. Before they can graduate from near-term reaction to long-term resilience, governments of all sizes and types must contend with at least four grand challenges that the pandemic has exposed like open wounds that need swift dressing:

- **Exploding demand for—and a near breakdown of—services.** The public health implications of the pandemic and their economic consequences made citizens around the world more dependent than ever on governments for critical information and services. In March 2020, for example, Australia's federal human services department, Services Australia, directed citizens to file claims for welfare payments online. When nearly 100,000 people tried to access it simultaneously just after nine a.m., however, the government's MyGov website crashed. In the U.S., twenty-six state unemployment websites likewise had crashed by April 15, 2020.
- **A shift in fiscal priorities.** Exploding demand for support and services during the pandemic forced governments to pivot from fiscal austerity, such as reducing spending to make government more efficient, to citizen stewardship, such as increasing spending to make government more effective. In fact, governments around the world collectively added nearly $20 trillion to the global debt load in 2020 alone. And it will not be long before a shift back to reduced spending and debt recovery begins to emerge.
- **An adapting workforce.** It's no secret that the pandemic changed how people work. But remote working is only one chapter in a bigger story. The deep and lasting changes that the pandemic has created in homes, businesses, and social institutions require new knowledge and skills that many workers—including government workers—need to develop. In fact, a recent global survey of more than 10,000 employees found that 80 percent of them had to learn new ways of working during the pandemic, and three out of four had to learn new technologies. Meanwhile, the World Economic Forum says that 40 percent of current workers' core skills will change within the next five years, and that half of all workers will have to be reskilled by 2025.
- **Eroding trust in government.** The pandemic has required the public sector not only to provide more and better services, but to do so in a way that keeps economies afloat, protects national security, preserves personal liberty, and improves equity across the population. In that context, trust in government has become a defining challenge for governments. And so far, they're failing at it. Only 41 percent of people say they trust government leaders to do what is right.

Core themes to transform government

These are big challenges. And big challenges demand big solutions. As we reflect on the many lessons learned during Phases I and II of the pandemic, we can distill this new knowledge into four core themes that will be fundamental to transformation of government in Phase III.

- **Rapid innovation and agility.** Many governments, even those caught off-guard by the pandemic, quickly shifted to rapid innovation and modernization.
- **Trust and transparency.** Providing essential services and averting economic collapse are further complicated by demands from citizens for protection, personal liberty, and equity.
- **Security.** The stress of the pandemic exposed existing gaps in security infrastructure and created new ones.
- **Talent and transformation.** The workers of today need to become the workers of tomorrow by learning the new skills and technologies that will become ubiquitous among government workforces.

Against the backdrop of the grand challenges facing governments today, informed by lessons learned during the pandemic, these four underpin the highest priorities for governments as they continue the fight against COVID. We believe that there are seven implications government leaders need to consider to emerge from Phase III with strength and resilience.

Becoming stronger and improving resilience

1. **Renew investment in emergency preparedness.** COVID-19 may be a once-in-a-century pandemic, but emergencies of its size and scale are not once-in-a-century events. Given the myriad threats confronting governments in the twenty-first century—everything from cybersecurity to climate change, for example—local, national, regional, and global disruptions are a near certainty. As the pandemic consumes less of their bandwidth going forward, governments must therefore continue to invest and reinvest in emergency preparedness, including the policies, relationships, communication streams, technologies, and physical infrastructure that will expedite future response efforts.

2. **Balance faster innovation with stronger governance, control, and cost takeout.** An oft-cited "silver lining" of the pandemic is that it forced governments to innovate and modernize at breakneck speeds. Governments that are used to moving slowly learned that they're quite capable of moving quickly. Unfortunately, they sometimes embraced speed at the expense of other critical priorities, like security.

   Going forward, governments must learn how to maintain a rapid pace of innovation while also exercising strict governance and controls that allow them to be good stewards of data and dollars—for example, by moving to a hybrid cloud approach that facilitates DevSecOps in a way that marries innovation with control and governance. And considering the need to pay down the debt accumulated throughout the pandemic, avoiding shortsighted decisions to cut or constrain digital programs will not only deliver greater citizen engagement, but also deliver cost savings in the mid- to long-term.

3. **Accelerate modernization of supply chains for control, integrity, and dynamic agility.** From shortages in consumer products, to the price of commodities, to insufficient access to N95 masks and ventilators, the pandemic exposed the fragility and interdependence of global supply chains. The public and private sectors must collaborate to modernize and regionalize supply chains in ways that make them more agile, adaptive, and resilient. In addition, governments need to design with a focus on supply chain integrity.

   The pandemic exposed just how dependent organizations were to singular sources of supply. Essentially, governments and private sector organizations alike are now rightly seeking to diversify their supply chains. But in the case of governments, they also need to consider industrial strategies to protect sovereign needs.

4. **Reimagine citizen engagement models and supporting government operations.** Even before the pandemic, consumers were pampered with unprecedented levels of convenience. From online shopping and streaming media to ridesharing and mobile banking, they've gotten used to getting what they want, when they want it, and with a frictionless customer experience. That became especially apparent during the pandemic, when quarantined consumers became even more reliant on convenience, thanks to services like food delivery and telehealth.

   Big steps forward have been taken, but much more can be done. And through this, governments will have an opportunity to become more efficient, more effective, and even more trusted.

5. **Build a robust analytic foundation for increasing situational awareness, predicting potential policy impacts, and providing transparency.** The actions required to respond and recover from the pandemic underscore the importance of both quantity and quality of data. To gain visibility into both problems and solutions, the public sector needs strong systems and governance, both to capture and organize information for situational awareness, and to turn it into actionable, shareable intelligence that can inform decision making at all levels of government. More than that, though, it needs to commit to data integrity and data transparency as a means of rebuilding citizen confidence and trust in government.

6. **Amplify the security imperative.** Government modernization during the COVID-19 pandemic has yielded essential new systems and services. The speed at which governments stood them up, however, means security in some cases might have been overlooked, ignored, or abridged. As a result, government infrastructure has become a vulnerable and attractive target for cyberattacks. The lesson is clear: Governments can no longer afford to treat security as an afterthought and must bake it into new services and systems from their inception—preferably with a zero trust posture.

7. **Upskill and reskill the workforce through adaptive learning programs.** Many governments that began the pandemic in an analog world are poised to emerge from it in a digital world. Just because their technology has evolved, however, doesn't mean their workforce has done the same. In government agencies where it hasn't, legacy employees can be just as handicapping as legacy systems. To bridge the gap, governments must invest in public servants by giving them the knowledge and skills they need to be effective in a post-COVID world. Adaptive learning that uses artificial intelligence (AI) to tailor training and education to individual workers is one tool that can help them do so.

To be successful, we believe governments should approach these seven objectives from the vantage point of four architectural touchstones:

- **Predict** outcomes
- **Automate** at scale
- **Secure** everything
- **Modernize** with ease

How does this look in practice? Consider, for example, supply chain modernization. Healthcare providers and governments need to collaborate with manufacturers of ventilators, for instance, to mine for data, model and simulate—and, ultimately, *predict*—the impacts of potential changes and future scenarios. Next, they need to *automate* response processes with AI-assisted workflows to achieve increased reliability and resilience, build in *security* to protect it from physical and cyber threats, and *modernize* industrial operations and policies to support automation and sovereignty.

Whether they produce ventilators or citizen services, businesses and governments alike should embrace the challenges and opportunities before them with exactly this type of framework. If they do, they'll be positioned to emerge from COVID-19 stronger and more resilient than they were before it.

Author

Mike Stone
Managing Partner
Global Government Consulting
IBM
mike.stone@ibm.com

Digital citizen services

Authored by Paul A. Dommel, Nicholas Holmes, and Mike Stone

In many countries, the COVID-19 pandemic exacerbated the long-present and wide gap in service quality between the private and public sectors.

Governments suddenly faced enormous pressures on some services. For example, as many as one in four workers—more than forty-six million people—received a form of unemployment insurance.

System failures across the U.S. and countries around the world were common. After a crush of newly jobless residents overwhelmed Florida's online and phone systems, citizens lined up to obtain paper applications for unemployment benefits. Australia and other countries experienced similar hardships. Many people had never filed for unemployment benefits or interacted with unemployment insurance systems or processes. Few were impressed.

Both private and government organizations had to adapt—and quickly. Research from the IBM Institute for Business Value found that the pandemic accelerated digital transformation at 59 percent of surveyed organizations. Similarly, given the pandemic's impact on government, just over half of government executives surveyed said digital transformation was a priority.

Although their initial response was slow, many public sector organizations made significant strides to resolve service issues. Numerous governments achieved years of changes in months. Leaders identified new ways to educate students and shift work from offices to homes.

Administrations implemented massive changes in process and technology to scale up and meet unprecedented demand for social benefits services. Skyrocketing fraud added to the challenges, but investigations and counter-fraud solutions have led to hundreds of indictments and convictions.

Digital engagement across all industries jumped ahead by years during COVID-19, and government was no exception. Governments need to build on this progress to cost-effectively improve service delivery going forward. By capturing lessons learned, they can continue their advancements to drive further impact.

Innovating with modern technology to meet citizen needs

Embracing the new urgency to harness technology, leading governments scaled to meet demand, delivered entirely new services, and supported new ways of working. For example, governments across the globe set up AI-powered virtual assistants to answer millions of questions per day. Some agencies went even further and used the technology to seamlessly conduct transactions like scheduling appointments, paying for licenses, or even processing paper benefit applications. This approach cannot only improve citizen service, but, according to Gartner, effective self-service channels can be 80 to 100 times less costly than time-consuming live interactions.

The U.S. Department of Veterans Affairs applied process automation and intelligent workflows to help improve citizen service and cut administrative costs associated with manual, paper-driven processes. The VA used AI and process automation to digitize incoming benefits packages and correspondence, cutting processing time from five to sixty days to hours. Within just eight months, 200 people handling piles of paper were retrained for new positions.

Improvements continued and the VA began to use a similar solution to speed Freedom of Information Act (FOIA) Request processes. While modern technology played a huge role, these changes were underpinned by a fundamental culture shift that embraced innovation. Innovation was a must. There was no other way.

Keep moving forward with lessons learned

Not every new system deployed during the pandemic was a success. In fact, some vaccine scheduling tools were considered difficult to use. What's more, many citizens lacked access to broadband internet and were not able to easily get into these systems.

The more successful governments identified critical priorities and rolled up their sleeves to build resilient solutions. They created diverse teams of people from across their organizations and communities to define issues and opportunities for improvement. They used design thinking to focus on end users and develop solutions that people would adopt. They kept things simple, often eliminating steps that should not exist. Finally, they teamed with technology partners that brought insights, experience, and tools for the journey.

The transformation imperative and need for continued investments is not over. In fact, leaders in both government and the private sector are continuing to focus on customer experiences and efficiency. IDC reports that the top three focus areas for the future, for all organizations, are customer satisfaction, operational efficiency, and innovation.

Yet, as governments have become more comfortable with transformation at pace, some have experienced unsettling new challenges: security gaps, expanding complexity, and a sense of losing control. All of these can be addressed. Disciplined approaches can drive fast results and address important considerations for long-term success.

Authors

Paul A. Dommel
Global Director for Public Service
IBM
pdommel@us.ibm.com

Nicholas Holmes
CTO
Global Government Data and AI
IBM
nicholas.holmes@us.ibm.com

Mike Stone
Managing Partner
Global Government Consulting
IBM
mike.stone@ibm.com

The new urgency in modernizing supply chains for control, integrity, and dynamic agility

Authored by Rob Cushman, Tim Paydos, Mike Stone, Jonathan Wright, and Nikki Zimmerman

The globalized supply chain is a "hidden hand" underpinning our economy and society.

For the last several decades, a vast ecosystem of suppliers, logistics providers, and buyer brokers has partnered to optimize this extended supply chain and increase efficiency while cutting the cost of capital.

We all depend on this global supply chain for our food, clothing, fuel—indeed, our very livelihoods and security. And it has become increasingly complex, integrated, and fragile.

The domino effect

In March 2021, strong winds helped cause a single ship, the *Ever Given*, to run aground and block the entire Suez Canal—through which 12 percent of global trade passes each day, representing 30 percent of all global container traffic and over $1 trillion worth of goods annually. As a result, 369 massive cargo ships came to a complete standstill—holding up an estimated $9.6 billion in trade along the waterway per day. What's more, the global price of oil spiked 4 percent, and commodity price indices in Europe grew 5 percent.

The fact that a single vessel can impact the cost of beef on the other side of the world underscores supply chain interdependence in a globalized world.

That had become clear a year earlier, when the Black Swan COVID-19 hit with all its attendant challenges. Almost overnight, we saw disruptions to the supply of goods that were unimaginable just days prior. As consumers, we all have our personal stories to tell—perhaps you were unable to purchase paper products or eggs at your local grocery store.

The problem was not that the world had run out of toilet paper or poultry, but rather that we had too much product packaged in transit in the commercial supply chain—hotels, restaurants, and office buildings—and not enough in the retail and consumer supply chain.

On March 12, 2020, demand for consumer paper products jumped 734 percent. The following month, U.S. dairy farmers reportedly were dumping 3.7 million gallons of milk a day. The worldwide crude oil surplus reached an all-time high. And while the global food distributor Sysco furloughed 33 percent of its workforce in the summer of 2020, Amazon hired 100,000 new employees, mostly in delivery and logistics.

Given the complexity of our interdependent supply chain, 80 percent of the failures we saw were in the second and third sub-tier ecosystem of raw material and component suppliers.

Bearing the brunt

Leaders in healthcare and government, more than any other sector, faced the full force of this disruption. The most visibly impacted area was the medical equipment supply chain, as demand skyrocketed for personal protective equipment (PPE), ventilators, and even hospital beds. But the impact to the public sector went far beyond that, as government leaders sought to keep the economy open and the supply of goods flowing. As a result, leaders faced four core challenges:

- **Volatile demand:** Extreme volatility in critical materials and supplies that public sector leaders needed to address the pandemic, and entirely new demand patterns the world had never seen.
- **Inventory fluctuations:** Stockouts of high-demand goods and stockpiles of low-demand items, with little visibility in inventory count and location.
- **Logistics constraints:** Partial loads, capacity-constrained warehouses, lower fill rates, fewer on-time deliveries, and constrained labor flexibility.
- **Increased global supply network complexity:** The supply chain became even more dependent on tier two and tier three suppliers, creating limited visibility into raw or work-in-progress (WIP) inventory, coupled with a rising need to onboard new suppliers and a growing concern around supply chain integrity.

Forging stronger supply chains

Government and healthcare leaders have been focused on supply chain issues for decades. More than twenty years ago, when the September 11 terrorist attacks shook the world and shaped an entire generation, agencies became much more aware of how global risk and uncertainty affect supply chains. Those events moved the issue of supply chain resiliency to the fore.

As the global community focuses on rebuilding and emerging from the most recent crisis, there are four key actions that governments must take to modernize and strengthen supply chains. These actions can help ensure increased agility and resiliency for the future and protect against foreign adversaries and other potential risks:

1. **Harness data and build visibility across multitier supply chains to smooth volatility.** Organizations gather vast amounts of data to monitor and measure risk. That trove of information can, with improved transparency, provide the ability to identify both relationships and resulting dependencies in integrated chains.

   A trusted data exchange secured and enabled by blockchain technology can allow organizations to collect internal and external data from partners across their extended supply chain ecosystem. Once synthetized, that data can offer vital insights shared across partner networks on critical transactions, external and internal events, and shared risks.

2. **Monitor the supply chain and drive collaboration to actively plan for future disruption.** No supply chain is without risk. But increased access to information in a timely manner provides greater decision-making options. Before an agency can craft a strategy, it must identify the risks inherent in its integrated supply chain. From suppliers and production flows to transactions and operations, organizations must examine the details of each interconnected relationship and segment of the supply chain to pinpoint vulnerabilities and bottlenecks. By creating a common operating picture based on information from all suppliers, organizations can model and test different scenarios to evaluate the plans of action that best align with shared goals.

   Increased visibility into supply chain disruptions enables organizations to be better prepared. Moreover, this information can provide organizations insights to help achieve essential supply chain objectives (such as sustainability or supplier diversity) by surfacing information on where and by whom commodities are sourced.

3. **Build integrity and trust by measuring performance and risk, and compare results over time.** Measuring the supply chain is as critical as monitoring it. Organizations must identify measurements to gauge and quantify risks, and to better understand the impact and potential exposure of disruptions across their integrated supply chain. Data management solutions can help categorize certain aspects of supply chain risks as high, medium, or low. Transparency across ecosystem partners provides shared insights on the reliability of the entire integrated supply chain.

   Extending a measurement system to external partners allows organizations to benchmark themselves against leading organizations in both the public and private sectors—and drive continuous improvement efforts. Regardless of the data collection frequency, a regular measurement and analysis cadence helps ensure quality findings. This data set is pivotal to shaping a risk management strategy and prioritizing resources for the greatest return.

   Combining these findings with the right analytics tools can further enhance the reliability, quality, and repeatability of organizational processes.

4. **Improve the resiliency and reliability of supply chains.** With a foundation of data-driven insights for monitoring and measuring the integrated supply chain, organizations can put preventive and proactive strategies in place and continuously iterate to improve reliability and resilience. With a robust data set, organizations can better monitor their integrated supply chain as they implement new strategies and evaluate the results of new initiatives and interventions.

   Introducing new technologies such as artificial intelligence (AI) can further amplify results. AI can help identify suppliers that have room for improvement, prioritizing based on highest impact and predicting new scenarios through simulations.

   Improving resiliency also requires building a diverse supplier base. Understanding and mitigating supply chain risks involves gaining visibility into tier two and tier three suppliers which—as we've seen—can quickly and significantly disrupt production and delivery. Over 90 percent of Fortune 1000 companies depended on tier two suppliers in regions most affected in the initial phase of the global COVID-19 pandemic or operated in potentially adversarial nation states. Impediments to interaction and engagement with these suppliers greatly complicate risk management.

   Governments should pursue policies and strategies that reduce dependence on single sources of supply (suppliers and regions) for critical goods and services, and limit geopolitical exposure. Supply chain repatriation should be part of the discussion.

Critical capabilities

Building a deep and comprehensive understanding of your organization's integrated supply chain strengths and weaknesses can enable business continuity planning and rapid response strategies. The last nineteen months have been a harsh reminder of the risks inherent in our interconnected world and further demonstrated the criticality of supply chains to economies, organizations, and individuals. As such, it's imperative that governments can crowdsource feedback from stakeholders across the extended value chain—from suppliers to citizens—on what they need and what changes impact them most.

Additional thoughts

The IBM Center for The Business of Government and the Shared Services Leadership Coalition recently held an engaging virtual roundtable discussion around shared services and supply chain management. The objectives for the roundtable were to help: frame the government's supply chain challenges more specifically; develop a model by which world-class commercial entities approach similar challenges; conduct a gap analysis between government and industry models; and consider the crucial role of informal networks and "backdoor bureaucracies" in addressing complex national challenges.

Authors

Rob Cushman
Senior Partner
Supply Chain Transformation
IBM
Rob.Cushman@ibm.com

Jonathan Wright
Managing Partner and
Service Line Leader
IBM
Jonathan.Wright@ibm.com

Tim Paydos
Vice President & General Manager
Government, Health Care &
Life Sciences
Global Industries
IBM
tpaydos@us.ibm.com

Nikki Zimmerman
Global Leader
Supply Chain Resilience
IBM
nezimmer@us.ibm.com

Mike Stone
Managing Partner
Global Government Consulting
IBM
mike.stone@ibm.com

Amplifying the security imperative

Authored by Miro Holecy, Julian Meyrick, Tim Paydos, and Mike Stone

In the heat of the moment, governments around the world responded to the COVID-19 crisis with rapid innovation—by creating more frictionless citizen experiences, accelerating digital business transformation, expanding cloud footprints, transitioning to hybrid or remote work models, and integrating global supply chains.

In many cases, government leaders surprised themselves with their ability to rapidly innovate. In the rush to launch new capabilities to meet increased demand, however, critical security and protection measures may have been deprioritized, overlooked, or ignored altogether. As a result, many government organizations have further increased their exposure to security threats. The trick now is to sustain the pace of innovation and build even more momentum, while simultaneously closing any security gaps.

Moving government services, communication, and personal interactions to digital has significantly increased potential attack surfaces, resulting in a dramatic surge in cybersecurity incidents, including the recent series of ransomware attacks and exposure of personal and sensitive citizen data. This risk has intensified even more as a result of organizations leveraging data and artificial intelligence to accelerate COVID-19 recovery plans across multiple levels of government. This required moving workloads to the cloud—along with their associated threats and vulnerabilities. In fact, research indicates upwards of 90 percent of cyber-related incidents originated in cloud environments in 2020.

In addition to increasing risk, cyber incidents also had significant financial impacts on governments. According to a recent report, public sector organizations are the sixth most frequently attacked among all industries, and the average cost per cybersecurity incident is nearly $2 million. And what's even more alarming is that attacks on public sector organizations have the second longest attack lifecycle, with the average organization taking 330 days to contain a breach once identified. While you can't point to a singular cause, a dearth of security experts with the right skills is a key gap and a likely contributing factor to the security woes of many public sector organizations.

Securing critical infrastructure with zero trust principles

The very nature of critical infrastructure implies a dynamic relationship between trust and risk. Understanding the amount of risk governments carry and being able to quantify that risk into financial terms provides a clear picture for implementing security in the most efficient and effective way possible. This is even more important when government operations move online, exposing both IT and operational technology (OT) networks to potential compromise. The May 2021 Colonial Pipeline ransomware attack led to fuel shortages across the East Coast of the U.S. Reliance on IT and OT environments means mission-critical infrastructure is increasingly vulnerable to new threats. For example, GPS-enabled navigation systems that we take for granted are at risk of breakdown, which can negatively impact the deployment of emergency services vehicles, maritime navigation, and operation safety of many services consumed by citizens every day.

With the number of risks and security events growing exponentially, government security operation teams are adopting the zero trust security approach. The IBM Institute of Business Value concluded that organizations with mature zero trust capabilities have reduced their security capital and operational expenditures and increased the effectiveness of their cybersecurity operations. This zero trust approach enables the protection of the IT and OT at the foundation of government services by adopting key zero trust principles:

- **Preserve citizen private and sensitive data** with a focus on simplifying and securing user onboarding, managing user preferences and consents, and enforcing privacy regulations controls.
- **Reduce the risk of insider threat** by enforcing least privilege access, discovering risky user behavior, and embedding threat intelligence.
- **Protect the hybrid cloud** by managing and controlling all accesses, monitoring cloud activity/configurations, and securing cloud native workload.
- **Secure the remote workforce** by securing bring your own (BYO) and unmanaged devices, eliminating VPNs, and providing "passwordless" experiences.

Cognitive roadmap to zero trust

Government organizations can't simply spend or hire their way to a healthy security posture. To close critical capability and skills gaps, several approaches and technologies are needed. As security technologies have evolved over the years, they have moved from simple perimeter controls (such as focusing on static defenses) to more advanced security intelligence capabilities (such as focusing on real-time threat information and deviations from patterns).

These new technologies have ushered us into the **cognitive** era of security. Cognitive security solutions can understand context, behavior, and meaning by analyzing both structured and unstructured data. Cognitive security looks to unlock a new partnership between security analysts and their technology. These solutions can interpret and organize information and offer explanations of what it means, while offering a rationale for conclusions. They also learn continuously as data accumulates and insights are derived from interaction.

These next-gen cognitive security solutions can enable government security teams to:

- **Enhance the capabilities** of junior security operations center (SOC) analysts by giving them access to best practices and insight that used to require years of experience.
- **Improve the response speed** by applying external intelligence from blogs and other sources in an effort to take action before threats materialize.
- **Quickly identify threats** and speed detection of risky user behavior, data exfiltration, and malware infections using advanced analysis methods.
- **Gain greater context around security** incidents through automation of local and external data gathering and reasoning.

Cognitive security solutions can be used in combination with automated, data-driven security technologies, techniques, and processes to help ensure the highest levels of context and accuracy.

Improving collaboration for better security

While traditional approaches to cybersecurity relied on permissions and discrete network boundaries, today's networks are defined by dynamic services and diffuse boundaries. Today's digital platforms generate value by virtue of being interconnected, by sharing information across multiple parties. One leading example is the LA Cyber Lab, a first of its kind threat intelligence sharing platform, which allows city government officials, businesses, and private citizens to share cyber threat intelligence.

This collaborative approach to security helps governments increase their responsiveness while reducing complexity. Cognitive security technology helps to identify primary cyber weaknesses and vulnerabilities across government operations and government-controlled supply chains. Success requires a holistic approach and a deep understanding of the value that cognitive security solutions can provide.

Read my previous report, "*Phase III: The essential role of government in response to COVID-19.*"

Authors

Miro Holecy
Government Industry Executive &
IBM Distinguished Engineer
miro.holecy@se.ibm.com

Julian Meyrick
Managing Partner & Vice President
Security Strategy Risk & Compliance
IBM
julian_meyrick@uk.ibm.com

Tim Paydos
Vice President & General Manager
Government, Health Care &
Life Sciences
Global Industries
IBM
tpaydos@us.ibm.com

Mike Stone
Managing Partner
Global Government Consulting
IBM
mike.stone@ibm.com

Building a robust analytic foundation

Authored by Cristina Caballe Fuguet, Tim Paydos, and Mike Stone

Public sector leaders must build a robust analytic foundation for increasing situational awareness, predicting potential policy impacts, and providing transparency

As governments and healthcare leaders have strained to respond to the COVID-19 "black swan" event, they quickly realized the need to not only provide expanded and better services. This had to be accomplished in a way that keeps economies afloat, helps protect national security, preserves personal liberty, and improves equity across the population. At the end of the day, trust in government has become a defining challenge—only 41 percent of people say they trust government leaders to do what is right.

In reflecting on the four themes that have emerged over the past several months, a key implication has become clear—public sector leaders must build a robust analytic foundation for increasing situational awareness, predicting potential policy impacts, and providing citizen transparency. In this way, data serves as the new raw material that institutions need to mine and refine to rebuild trust.

Digital data is now virtually everywhere—across sectors, countries, organizations, and in the billions of digital devices that citizens and businesses use daily. And now with 5G, the amount of data globally is expected to nearly triple. The challenge is that more than two-thirds the amount of data available to enterprises goes unused or is effectively wasted. The act of creating insights and value from this increasingly abundant resource is essential.

However, governments, healthcare institutions, and societies are still facing significant headwinds that prevent them from fully capitalizing on this opportunity. To address these challenges, governments should continue to invest in data preparedness, including the policies, relationships, communication streams, technologies, and physical infrastructure. This can not only expedite future response efforts, but also contribute to increased economic vitality and prosperity.

Public sector leaders need to:

- Develop robust data management and analytics capabilities built for situational awareness, decision support, and greater transparency.
- Better understand potential policy impact on economy, personal liberty, and equity through modeling.
- Identify and target underserved communities.
- Embrace data sharing and data interchange standards.
- Protect citizen privacy as social services evolve.
- Integrate eligibility by transferring entitlements amongst agencies effectively.
- Create services that are accessible for those most in need (for example, the elderly).

The challenges of closing the data understanding gap

During the early phases of the pandemic, we may have felt like a sailor on a stranded ship, where water (data) was everywhere yet **there was not a drop (of information) to quench our thirst**. While the curve of available data continues to grow at an exponential rate and many governments struggle to help ensure the curve of "understood data" keeps pace, it is imperative for public sector institutions to address two key questions:

1. How can we connect data from different sources, agencies, and departments and combine it in such a way where anyone—with the right authorization—can access it, and extract insights to inform critical decisions?

2. How can we simplify the underlying complexity of data silos and advance citizens to an era where they can ask direct questions and get relevant answers at virtually any time, any place?

These are not easy challenges to address. And they're further complicated by the fact that the data needed to build and operate an end-to-end view of the citizen is unlikely to reside in any single platform.

What public sector leaders need is a robust data fabric

Tackling this problem will take a **data fabric**. Fabric is literally the structure of something—the parts that hold it together and make it what it is. In a textile fabric, it is defined as fibers made by either weaving or knitting. In a data fabric, it is the connection and unification of data points that lead to the whole structure.

A data fabric provides seamless access across hybrid clouds, data centers, and edge systems to ingest, explore, prepare, manage, govern, and serve petabyte-scale data for organizational-ready AI. This enables dynamic and intelligent data orchestration across a hybrid cloud, creating a network of near-instantly available information. The data fabric helps us consume the data when it is the most relevant and valuable to support mission-critical decision making. In other words, because data quickly ages, it needs to be consumed at the right time.

The perfect marriage between data and AI

Data is a foundation from which both governments and businesses can drive smarter decisions. However, it is AI that unleashes the full power of that data. This is why AI is poised to transform governments, organizations, and enterprises with the potential to add almost 16 trillion dollars to the global economy by 2030. It is our belief that, in the very near future, virtually all data will be infused with AI—the linchpin capability that will help deliver automation and actionable insights from the data, close the "understanding gap," and unleash innovation.

The lessons we have captured during the pandemic underscore **the importance of both quantity and quality of data.** To gain visibility into both problems and solutions, the public sector needs strong systems and governance. This is to capture and organize information for situational awareness, and to turn it into actionable, shareable intelligence that can inform decision making across levels of government. More than that, though, the public sector needs to commit to **data integrity and data transparency** as a means of rebuilding **citizen confidence and trust in government and turning lessons captured into lessons learned**.

Authors

Cristina Caballe Fuguet
Executive Director
Global Public Sector
IBM
Cristina.Caballe@es.ibm.com

Mike Stone
Managing Partner
Global Government Consulting
IBM
mike.stone@ibm.com

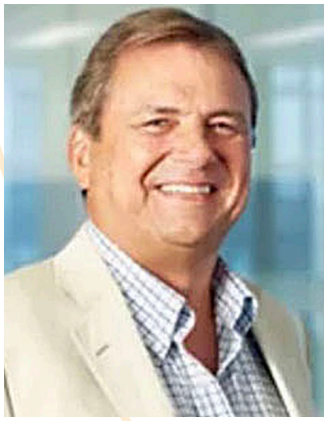
Tim Paydos
Vice President & General Manager
Government, Health Care &
Life Sciences
Global Industries
IBM
tpaydos@us.ibm.com

About the Authors

Tim Paydos

Tim Paydos has spent twenty-two years at IBM working mostly in the government industry, though not contiguously. He left briefly in 1999 to try his hand at a startup, catching the dotcom implosion at just the right time before rejoining IBM three years later. Tim has a degree in government from Harvard University, where he studied international relations, deterrence theory, and nuclear war-gaming. He first joined IBM in 1995 as an industry solution consultant.

Tim has had the honor of working personally with hundreds of government agencies both in the United States and abroad, at both the national, provincial, and local levels. His particular passion lies in helping public safety, emergency management, intelligence, and defense protect the society they serve. Throughout his career at IBM, Tim has led a range of strategy and marketing, solution sales, and solution management teams across services and technologies at IBM.



Mike Stone

Mike Stone is the Managing Partner for Global Government Consulting with IBM. His experience includes roles as Global Lead for Defense and National Security & Global Head of Technology Transformation for Infrastructure, Government and Healthcare, KPMG International, Chief Digital and Information Officer for the UK MOD, CEO of Defence Business Services, CEO of the MOD's Information Systems and Services organization, Group EVP & Chief Client Officer of Mastek, President Service Design and CIO of BT Global Services, COO of BT International and CEO of BT OpenAccess.

Key Contact Information

Tim Paydos

Vice President & General Manager
Government, Health Care & Life Sciences
Global Industries
IBM

Email: tpaydos@us.ibm.com

Mike Stone

Managing Partner
Public Sector
Global Government Consulting
IBM

Email: mike.stone@ibm.com

RECENT REPORTS FROM THE IBM CENTER FOR THE BUSINESS OF GOVERNMENT

For a full listing of our publications, visit www.businessofgovernment.org

Agility

Adopting Agile in State and Local Governments by Sukumar Ganapati

The Road to Agile GOVERNMENT: Driving Change to Achieve Success by G. Edward DeSeve

Transforming How Government Operates: Four Methods of Change by Andrew B. Whitford

Agile Problem Solving in Government: A Case Study of The Opportunity Project by Joel Gurin, Katarina Rebello

Applying Design Thinking To Public Service Delivery by Jeanne Liedtka, Randall Salzman

Digital

Artificial Intelligence in the Public Sector: A Maturity Model by Kevin C. Desouza

Aligning Open Data, Open Source, and Hybrid Cloud Adoption in Government by Matt Rumsey, Joel Gurin

Innovation and Emerging Technologies in Government: Keys to Success by Dr. Alan R. Shark

Risk Management in the AI Era: Navigating the Opportunities and Challenges of AI Tools in the Public Sector by Justin B. Bullock, Matthew M. Young

Effectiveness

Managing The Next Crisis: Twelve Principles For Dealing With Viral Uncertainty by Katherine Barrett and Richard Greene, Donald F. Kettl

Other Transactions Authorities: After 60 Years, Hitting Their Stride or Hitting The Wall? by Stan Soloway, Jason Knudson, Vincent Wroble

Guidance on Regulatory Guidance: What the Government Needs to Know and Do to Engage the Public by Susan Webb Yackee

Federal Grants Management: Improving Outcomes by Shelley H. Metzenbaum

Government Reform: Lessons from the Past for Actions in the Future by Dan Chenok, John Kamensky

COVID-19 and its Impact: Seven Essays on Reframing Government Management and Operations by Richard C. Feiock, Gurdeep Gill, Laura Goddeeris, Zachary S. Huitink, Robert Handfield, Dr. Rodney Scott, Sherri Greenberg, Eleanor Merton, Maya McKenzie, Tad McGalliard

Insight

Delivering on the Vision of Multi-Domain Command and Control by Dr. David Bray

Using Technology and Analytics to Enhance Stakeholder Engagement in Environmental Decision-Making by Jenna Yeager

Making Federal Agencies Evidence-Based: The Key Role of Learning Agendas by Dr. Kathryn E. Newcomer, Karol Olejniczak, Nick Hart

Improving Outcomes in Government through Data and Intelligent Automation by The IBM Center for The Business of Government, Partnership for Public Service

Silo Busting: The Challenges and Successes of Intergovernmental Data Sharing by Jane Wiseman

Integrating Big Data and Thick Data to Transform Public Services Delivery by Yuen Yuen Ang

People

The Age of Remote Work: How COVID-19 Transformed Organizations in Real Time by David C. Wyld

Reskilling the Workforce with Technology-Oriented Training by Stacie Petter, Laurie Giddens

Sustaining a Distant Vision: NASA, Mars, and Relay Leadership by JW. Henry Lambright

Distance Work Arrangements: The Workplace of the Future Is Now by John Kamensky, Emily G. Craig, Michaela Drust, Dr. Sheri I. Fields, Lawrence Tobin

Risk

Emerging Technology for Response and Recovery: An International Dialogue by Kevin C. Desouza

The Rise of the Sustainable Enterprise by Wayne S. Balta, Jacob Dencik, Daniel C. Esty, Scott Fulton

Managing Cybersecurity Risk in Government by Anupam Kumar, James Haddow, Rajni Goel

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Consulting

With consultants and professional staff in more than 160 countries globally, IBM Consulting is the world's largest consulting services organization. IBM Consulting provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington, D.C. 20005
(202) 551-9342

website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

Stay connected with the IBM Center on:

or, send us your name and e-mail to receive our newsletters.

IBM Center for **The Business of Government**