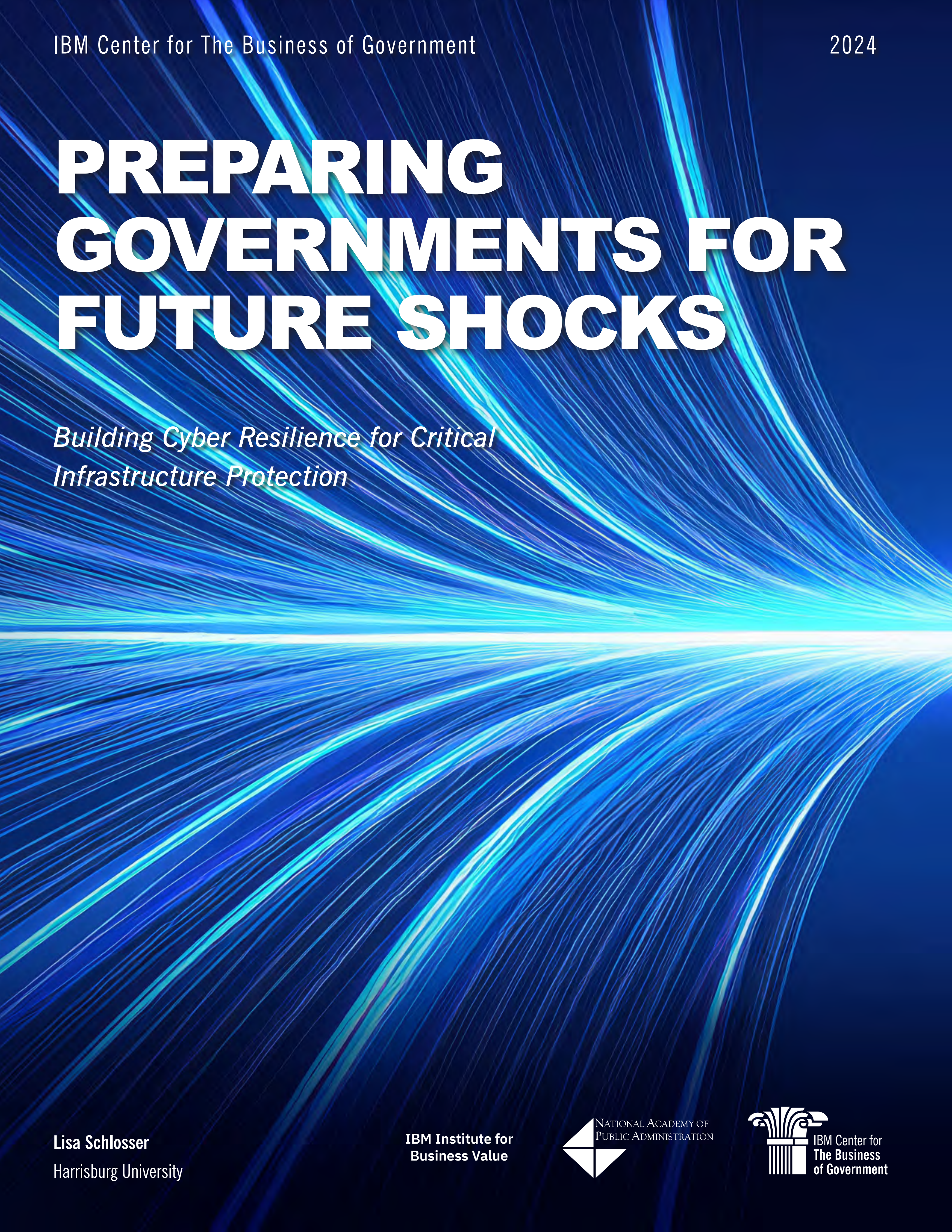


IBM Center for The Business of Government

2024

PREPARING GOVERNMENTS FOR FUTURE SHOCKS

Building Cyber Resilience for Critical Infrastructure Protection

Lisa Schlosser
Harrisburg University

IBM Institute for Business Value

National Academy of Public Administration

IBM Center for
The Business of Government

Preparing Governments for Future Shocks:
Building Cyber Resilience for Critical Infrastructure Protection

Lisa Schlosser

Harrisburg University

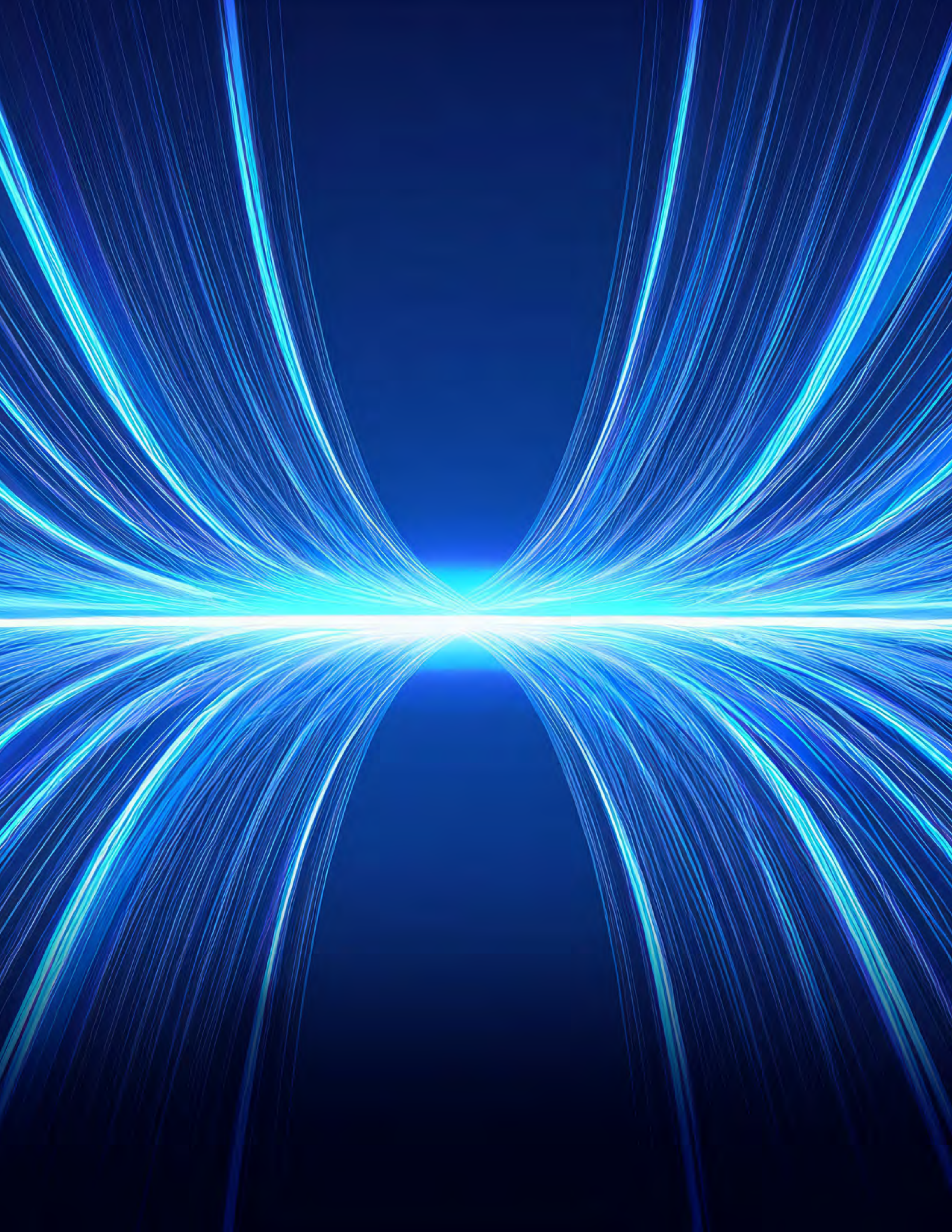
OCTOBER 2024

IBM Institute for Business Value

National Academy of Public Administration

IBM Center for The Business of Government

Table of Contents



Foreword

The Future Shocks Initiative

Government leaders increasingly indicate that what were previously viewed as Black Swan events are now becoming more frequent—and more destabilizing—shocks. The past several years saw acceleration toward a connected world where physical goods and digital services are increasingly interdependent. The vulnerability of social and economic well-being has increased due to reliance on connectivity and distributed value chains subject to disruption on multiple fronts.

Risks have grown due to complex variables such as geopolitical conflicts, multiple public health emergencies, energy crises, climate-related natural disasters (e.g., wildfires, hurricanes, drought), the breakdown of longstanding trade relationships, economic displacement, and economic inequality. The combination of these factors renders prior planning models obsolete.

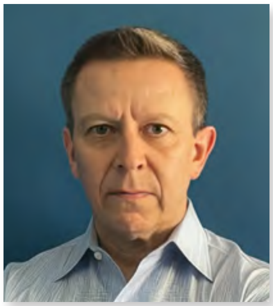
Citizens, nongovernmental organizations, and commercial enterprises continue to rely on governments to help manage uncertainties. Traditional incident response frameworks may no longer be sufficient, as events occur across multiple domains, jurisdictions, and decision-making authorities. Rather, collaborative action to address anticipated threats requires focus and cooperation across a broad ecosystem of partners and stakeholders. Governments must prepare for "future shocks" by supporting stakeholders with insights, resources, innovation, and adaptation that characterizes successful response to any high-impact event.

The IBM Center for The Business of Government, the IBM Institute for Business Value, and the National Academy of Public Administration (the Academy) continue to lead an initiative to help government identify core capabilities critical to building such resilience, and make progress toward addressing major national and international priorities including the Grand Challenges in Public Administration put forth by the Academy.

We have convened a series of international roundtable discussions with global leaders from across the public, private, academic, and nonprofit sectors to capture lessons across six key domain areas: Emergency Preparedness and Response, Cybersecurity, Supply Chain, Sustainability, Workforce, and International Cooperation. In each domain, we harvest insights from the roundtables to identify strategies and solutions for governments to act.

Previous roundtables brought together leaders in emergency management, cybersecurity, supply chains, and sustainability for insightful discussions of actionable and practical steps to build resilience to future shocks. For more information about this initiative, see the report *Preparing Governments for Future Shocks*, listen to the *podcast* with Michael J. Keegan, the IBM Center for The Business of Government, or review the *Future Shocks resource* page on the Center's website.

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



David Zaharchuk
Research Director
IBM Institute for Business Value
David.zaharchuk@us.ibm.com

Teresa W. Gerton
President and CEO
National Academy of Public Administration
tgerton@napawash.org

Cristina Caballe
Vice President, Global Public Sector, IBM Consulting
Cristina.Caballe@es.ibm.com

Introduction

As demonstrated by the findings from the *initial cybersecurity roundtable* done through the Future Shocks initiative, cyber resilience is crucial for protecting critical infrastructure, which includes essential services from the energy grid to clean water distribution. These systems are increasingly targeted by cyberattacks. Cyber resilience involves not only robust cybersecurity measures to prevent attacks but also the ability to quickly detect, respond to, and recover from incidents. This ensures continuity of operations and minimizes the impact of cyber threats. By enhancing cyber resilience, governments can safeguard critical systems, support the reliable functioning of vital services even in the face of crises, and help build and maintain public trust.

To discuss the above imperatives, the Center and IBV joined with NAPA to convene a roundtable that identified opportunities and practical actions government can take to address these challenges. The roundtable included executives from the government, nonprofit, academic, and commercial sectors, for a highly interactive, roundtable discussion entitled *"Preparing Governments for Future Shocks: Building Cyber Resilience for Critical Infrastructure Protection."* This session addressed three areas essential to the cybersecurity and resilience of critical systems: Emergency Preparedness and Response, Supply Chain Resilience, and Workforce Resilience.

This report summarizes the discussions in this roundtable by presenting the challenges, observations and best practices, and opportunities within each of these areas. Roundtable participants identified multiple recommendations for government action, discussed in the report and summarized in table 1.

Table 1—Recommendations For Government Action

Emergency Preparedness and Response Recommendations
• Implement National Resilience Plan NSM 22 and the Cyber Response and Recovery Funding (CRRF) Act to align aspirations and resources
• Continue to look at ways to optimize/streamline/create economies of scale, and created tiered governance structures for ISACs
• Develop and communicate incentives and resources to help SMBs prioritize cybersecurity
• Establish response and resilience frameworks that address the physical/cyber nexus and test plans
• Consider the inclusion of space systems as a critical infrastructure domain
Supply Chain Resilience Recommendations
• Establish center of excellence for procuring IT hardware in U.S.
• Create formal partnerships to share supply chain information across domains
• Shift to best value vs low-cost procurement models
• Use AI to drive real-time tracking
• Require attestations by third-party
Workforce Resilience Recommendations
• Use AI to improve the hiring process
• Enhance coordination between the public and private sectors by using proven models
• Improve cybersecurity classification codes and hiring processes
• Focus on employee engagement to support retention
• Create national database of cybersecurity professionals
• Create role-based cyber education models for disciplines within the organization beyond technical practitioner roles

Emergency Preparedness and Response

> *“The time to exchange business cards is not when a crisis happens; it is before a crisis occurs.”*

Governments across the globe face multiple crises, all of which transcend national borders, including a global pandemic, economic upheaval, civil unrest and environmental instability. As the public sector increasingly relies on technology to address major events, the cybersecurity challenge cuts across all critical infrastructure domains. Cyber challenges are becoming more complex as they impact disruptors evolving in frequency and impact, such as war, instability, and weather.

Promising new technologies—such as artificial intelligence (AI) and quantum computing—can provide governments with the ability to continuously improve resilience, especially in times of crises. Artificial intelligence, for example, offers opportunities but introduces challenges. As AI continues to advance and become more pervasive, so do its risks—from mass disinformation campaigns and deepfakes to fully autonomous weapon systems. Quantum computing is also adding a new dimension of opportunity and risks. For example, quantum capabilities can help solve large-scale problems much faster such as analyzing compounds to create new drugs and optimizing global supply chains.[1] However, with new capabilities come new risks. Nation-states will have a more powerful tool to attack critical infrastructure at scale. Also, given the power of quantum computing, current encryption solutions may be less difficult to crack.[2]

[1] Stackpole, Beth. “Quantum Computing: What Leaders Need to Know Now.” MIT Sloan, January 11, 2024. https://mitsloan.mit.edu/ideas-made-to-matter/quantum-computing-what-leaders-need-to-know-now.

[2] “13 Risks That Come with the Growing Power of Quantum Computing.” Forbes, August 13, 2024. https://www.forbes.com/councils/forbestechcouncil/2022/11/08/13-risks-that-come-with-the-growing-power-of-quantum-computing/.

The National Cybersecurity Strategy outlines a fundamental shift in the approach to emergency preparedness and response planning for the critical infrastructure:

1. Rebalance the Responsibility to Defend Cyberspace Away from End Users and to the most capable and best positioned actors in the public and private sector
2. Align Cybersecurity Aspirations and Resources

Three recent incidents underscore the need to understand and address these and other risks and impacts, by enhancing preparedness, response, and resilience to sustain critical infrastructure operations.

- First, the actions taken by the People's Republic of China (PRC) state-sponsored cyber group known as Volt Typhoon[3] have shown how nation-state actors can infiltrate various critical infrastructure domains to gain a foothold for future attacks.
- Second, the Colonial Pipeline ransomware attack caused a critical infrastructure provider to shut down its pipeline system.[4]
- Third, and more recently, a widespread outage, due to a faulty software update from CrowdStrike, led to substantial disruptions across numerous critical infrastructure domains, including airlines, hospitals, banks, and millions of other businesses.[5]

These incidents highlighted many risks to our critical infrastructure. For example, the CrowdStrike incident reiterated the need to evaluate software more effectively. The incidents also underscored the need to have a coordinated, national response plan in place that addresses the physical/cyber nexus and associated "single point of failure" risks within the critical infrastructures. This highlighted the need to proactively identify potential impacts to critical infrastructure domains in the event of a major cybersecurity event.

In addition, these incidents have shown that the approach for updating emergency preparedness and response, along with other critical infrastructure-related policies, needs greater agility to keep up with the current threat environment, as well as an injection of modern technology. Indeed, one roundtable participant noted that the policies and regulations in this domain need to be as agile as the technology that they govern. Some existing policies and regulatory requirements, for example, are 40 years old. Additionally, these incidents resulted in a potential need to identify a single point of contact in the government to rapidly coordinate

[3] "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure: CISA." Cybersecurity and Infrastructure Security Agency CISA, September 5, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[4] Easterly, Jen. "The Attack on Colonial Pipeline: What We've Learned & What We've Done over the Past Two Years: CISA." Cybersecurity and Infrastructure Security Agency CISA, May 7, 2024. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

[5] "Widespread It Outage Due to Crowdstrike Update: CISA." Cybersecurity and Infrastructure Security Agency CISA, July 26, 2024. https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update.

incident response for the critical infrastructure, and to ensure the appropriate coordinating entity is adequately staffed and resourced to respond—highlighting the need for better planning and federal and private-sector emergency preparedness and response.[6]

In addition to these incidents, continuing analysis of the approach to protecting critical infrastructure has identified other needs. For example, roundtable participants highlighted the necessity to understand and address the needs of states, tribes, and the small and medium business (SMB) community. SMBs are often at the forefront of cybersecurity attacks, yet lack the resources to rapidly respond to these incidents.

The Information Sharing and Analysis Centers[7] provide another resource that has shown significant value. Shifting the primary focus of ISACs from information sharing to bidirectional, analyst-to-analyst exchange can provide necessary context for cyberthreats.

There is also a need to continuously review and improve the ISAC governance structure. Roundtable participants noted that a modern governance structure should involve federal, state, local, and tribal leaders, each of which would have a different role but be part of an emergency response coalition. Participants also discussed a need for frameworks, standards setting, and integration across ISACs, as they currently vary widely with regard to needed input, impact, and efficiency.

Most incidents of any scale impact multiple critical infrastructure sectors simultaneously—information sharing would therefore benefit from standards and protocols. Other significant initiatives, including the National Resilience Plan and Cyber Response and Recovery Act, have been adopted over the years to confront these threats and continuously improve emergency and response actions, but public and private sector leaders recognize that novel approaches must be taken. The National Cybersecurity Strategy (NCS) has called for two fundamental shifts in allocating roles, responsibilities, and resources in cyberspace:[8]

- Rebalance the responsibility to defend cyberspace away from end users and to the most capable and best positioned actors in the public and private sectors
- Realign incentives to favor long term investments in cybersecurity resilience

[6] GAO. (May 2021). Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness. Washington, DC. https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic.

[7] "Information Sharing: A Vital Resource: CISA." Cybersecurity and Infrastructure Security Agency CISA, February 15, 2015. https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/information-sharing-vital-resource.

[8] National cybersecurity strategy implementation plan, May 2024. https://www.whitehouse.gov/wp-content/uploads/2024/05/NCSIP-Version-2-FINAL-May-2024.pdf.

This shift recognizes that cybersecurity requirements need to be harmonized to reduce complexity and costs. For example, the NCS has reduced the number of initiatives from 69 in July 2023 to 31 in April 2024. Reciprocity represents another opportunity to streamline cyber operations, enabling an entity regulated by multiple bodies to satisfy the requirements of multiple regulating bodies.

Participants in the roundtable identified the following emergency preparedness and response recommendations to support the NCS strategy and to best ensure readiness to address future shocks.

Table 2—Emergency Preparedness And Response Recommendations

• Implement, National Security Memorandum on Critical Infrastructure Security and Resilience (NSM 22), and the Cyber Response and Recovery Funding (CRRF) Act to align aspirations and resources
• Continue to look at ways to optimize/streamline/create economies of scale, and created tiered governance structures for ISACs
• Develop and communicate incentives and resources to help SMBs prioritize cybersecurity
• Establish response and resilience frameworks that address the physical/cyber nexus and test
• Consider the inclusion of space systems as a critical infrastructure domain

Supply Chain Resilience

> *"We have to think about speed and how to move at secure speed to innovate while protecting the U.S. supply chain."*

Shocks to supply chains over the past few years continue to reverberate.[9] Whether a supply chain focuses on efficiency and resiliency or on data-led insights and innovations for the future, addressing supply chain challenges involves balancing priorities and navigating the complex ecosystem of modern, global supply chains.

Governments face unique supply chain challenges. They enable commercial supply chains by providing critical infrastructure and security, and oversee massive public sector networks. However, these escalating supply chain challenges require increased digital transformation and innovation. Both the public and private sectors, nationally and internationally, have encountered challenges in building actionable resilience solutions into supply chains.

> The need to acquire innovative technology must be balanced with ensuring the security over, and resilience of, the supply chain. Many solutions are being identified, and one of the most promising is the launch of the Supply Chain Resilience Center (SCRC), announced by the Biden-Harris administration on November 27, 2023. The SCRC was created to protect the U.S. Supply Chain from evolving threats.

[9] "Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library, CVE-2024-3094: CISA." Cybersecurity and Infrastructure Security Agency CISA, March 29, 2024. https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094.

One of the primary areas of supply chain risk is in chip development. U.S. Department of Defense (DoD) has implemented a promising model to address this issue. DoD is the largest procurer of chips, and has set up a trusted supplier program. The Defense Microelectronics Activity (DMEA) division of the DoD, the Trusted Foundry (also referred to as Trusted Supplier Program) "covers a broad range of technologies and is intended to support both new and legacy applications, both classified and unclassified."[10]

While the program has certified approximately 83 suppliers, a major challenge remains involving utilization of incentives for the use of the program. Another challenge involves pre-selection and risk-rating of suppliers, which may disqualify competition (particularly for small businesses)—a foundational aspect of the U.S. government procurement system. Another consideration is information sharing and the publication of software ownership, often tied to vendor responsibility to attest to product security including sourcing origins and alternate sourcing opportunities. The Biden administration's 2021 Executive Order on Cybersecurity[11] called on agencies to address this issue by working with contractors to note sourcing as part of their Software Bill of Materials (SBOM). At the same time, governments must be cautious about intentionally or unintentionally sanctioning companies based on software and hardware ownership or risk.

Additionally, numerous federal entities rely on authorities to operate (ATOs) to secure systems, networks, and applications, which are often comprised of hundreds to thousands of individual cyber and system controls. However, an ATO only reflects security status on the day the ATO review is done. Third-party attestation provides an option to establish a continuous risk assessment process, by taking the burden off entities that often do not have the expertise to maintain sufficient security. More broadly, the risk assessment process could be made more effective by maintaining a matrix of key risks, updated through the use of AI and other modern technologies.

[10] McGregor, J. (2024, March 18). Globalfoundries' trusted foundry status helped secure Chips Act Investment. *Forbes*. https://www.forbes.com/sites/tiriasresearch/2024/03/18/globalfoundries-trusted-foundry-status-helped-secure-chips-act-investment/.

[11] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity.

The federal government is addressing supply chain in many other ways. The Biden administration announced, on November 27, 2023, the launch of the Supply Chain Resilience Center (SCRC) at the Department of Homeland Security, created to protect the supply chain from evolving threats. The SCRC examines security of U.S. port infrastructure, and provides recommendations to private sector stakeholders. The SCRC will also analyze vulnerabilities and conduct scenario planning with private sector stakeholders to help mitigate supply chain disruptions, ensure reliable and efficient deliveries of goods and services, and lower costs for the American people.[12] The SCRC may begin to resolve the issue that, historically, no single entity has owned supply chain resiliency and data visibility. A Center of Excellence (COE) to focus on the actual governance and procurement of trusted supplies may provide another practical next step.

The participants in the roundtable identified the following supply chain resilience recommendations to ensure readiness to address future shocks.

Table 3—Supply Chain Resilience Recommendations

• Establish center of excellence for procuring prioritized commodities including technology, electronics and microchips
• Create formal partnerships and collaboration tools to share, track and visualize supply chain Information and risk management across domains such as an SCM control tower
• Shift to best value vs low-cost procurement models to improve supply chain readiness
• Use AI to drive real-time tracking, suggested solution and resource maximization
• Drive policy to delegate the required ATO risk attestations to third-party support

[12] Biden-Harris Administration Announces Supply Chain Resilience Center to protect U.S. supply chain from evolving threats: Homeland security. U.S. Department of Homeland Security. (2023, November 27). https://www.dhs.gov/news/2023/11/27/biden-harris-administration-announces-supply-chain-resilience-center-protect-us.

Workforce Resilience

“AI will not replace you; but the people who use AI will.”

Amidst rapid technological changes and unprecedented industry disruptions, there is a growing disparity between the skills required in the workforce and the professionals who have obtained those skills. Public agencies will need to be able to recruit, retain, and develop a professional workforce who can successfully address emerging critical infrastructure issues now and into the future.

Consequently, cybersecurity workforce resilience has evolved as an ongoing challenge, one that requires continuous improvements to address increasing threats to the critical infrastructure. Government faces several workforce resilience challenges

First, a huge pay gap exists between the public and private sectors. The long lead time to hire qualified cybersecurity professionals in government compounds this problem, as does the difficulty of matching needs with openings on a nationwide scale—due to the lack of a national database, or a system to identify cybersecurity professionals across geographical boundaries.

Effective workforce resilience is dependent upon public and private sector coordination, cross-training, and the implementation of programs and practices that facilitate this collaboration.

Another identified issue involves the lack of consistency in academic programs, where many institutions do not expose graduates to real-world, hands-on cybersecurity education. The cybersecurity workforce needs practical expertise in applying modern technological tools and processes, particularly as governments and companies increasingly utilize emerging technology, such as AI, to improve cybersecurity detection, prevention, and response.

Many cybersecurity positions require a college degree. However, countless jobs in cybersecurity do not require a college degree, which removes a great barrier to obtaining top talent. In addition, while technical skills are critical in many cybersecurity roles, studies show how a "new skills paradigm, that soft skills like time management and the ability to work in team environments, is often more important in some roles than hard skills in Science, Technology, Engineering, and Math (STEM).[13]

Additionally, employees often feel disenfranchised. Workers have concerns that jobs are modernizing, meaning AI will replace certain roles. In particular, while white-collar jobs such as consultancy and cybersecurity should continue as AI scales, more manual roles may see significant reductions. Additionally, employees can become disenfranchised when they face changes in their jobs to remain engaged or promoted.

Governments could address such concerns through AI literacy programs, which can support cyber practitioners as well as other employees according to roles and responsibilities—from front line workers to executives. For example, an executive needs to know what AI can do for the mission and risks associated with its use, in order to make decisions about adoption and protection of AI technology. Conversely, practitioners need technical training on how to design, implement, operate and protect systems that use AI. A lawyer or a procurement officer would need to know how to frame contracts that cover risk, responsibility, and liability. These different disciplines often work in a collaborative fashion, but each looks at technology through their own lens. Education should be tailored accordingly, both within agencies and in academic programs. This could relieve concerns across the workforce, and provide a pathway for employees to refresh skills in addressing tech advances.

[13] Solino, K. (2023, June 30). IBM targets teaching soft skills in its most popular SkillsBuild courses. Fortune Education. https://fortune.com/education/articles/ibm-targets-teaching-soft-skills-in-its-most-popular-skillsbuild-courses/.

Finally, while remote work became increasingly more common due to COVID, employers have found that remote work often diminished coherence and collaboration; consequently, many organizations have moved to reduce remote work, or have adopted a hybrid approach that offers flexibility but hinders the ability for those not in the room to collaborate and feel like part of the team.

Numerous initiatives in both the public and private sector can enhance workforce resilience capabilities. While AI developments have presented a cybersecurity challenge, this technology can also help to identify and acquire cybersecurity talent by eliminating bias, improving the quality of hiring, decreasing time to hire, and improving communication, among other benefits.[14]

A consistent theme highlighted in the roundtable is that the government should capitalize on proven models of coordination between the public and private sectors. For example, the use of the Intergovernmental Personnel Act (IPA) program has shown promise in allowing public sector employees to serve in State, local, and tribal governments, institutions of higher education, and other eligible organizations to conduct research and enhance their skills.[15] Continued improvements in securing the critical infrastructure depend on exposing the cybersecurity workforce to the most current technological trends and technology, and to a deeper understanding of government systems and operations.

In 2022, the Department of Veterans Affairs (VA) announced a collaboration to connect veterans to training and networking programs that lead to gainful employment in technology fields.[16] This program trains veterans either without experience or in another industry to gain the skills to work in public sector cybersecurity.

The Scholarship for Service (SFS) Program provides another model. SFS recruits and trains information technology professionals to meet the cybersecurity workforce needs of federal, state, local, and tribal governments. This program provides scholarships from the National Science Foundation for up to three years of support for cybersecurity undergraduate and graduate (MS or PhD) education. Recipients must agree to work after graduation for the U.S. Government, in a position related to cybersecurity, for a period equal to the length of the scholarship.[17]

Other institutions have implemented successful workforce models. Government entities such as the National Security Agency have established effective programs for preparing its workforce by collaborating with academia. In the UK, businesses are required to set aside .05 percent of their payroll for apprenticeships to train subject matter experts.[18] Some companies require newly hired cybersecurity professionals to pass cybersecurity training courses and programs.

[14] Harver. (2024). How Heineken decreased Time to Hire by 42% and assessed 13.5k candidates in 8 days. https://harver.com/wp-content/uploads/2019/01/harver_Time-to-Hire_Heineken.pdf.

[15] NARA. (2024). Temporary Assignments Under the Intergovernmental Personnel Act (IPA). Retrieved from Code of Federal Regulations: https://www.ecfr.gov/current/title-5/chapter-I/subchapter-B/part-334.

[16] Frueh, M. (2022, May 22). VA and IBM collaboration to build pathways for veteran success. https://news.va.gov/103777/va-ibm-collaboration-to-build-pathways-for-veteran-success/.

[17] U.S. Office of Personnel Management. (2024). CyberCorps: Scholarship For Service. https://sfs.opm.gov/.

[18] Michael Price Associates Ltd. (2022, February 10). All about…the Apprenticeship Levy. https://www.mpa.co.uk/news-insights/knowledge-hub/all-aboutthe-apprenticeship-levy/.

Roundtable participants also noted that the Office of Personnel Management (OPM) and other agencies need to update cybersecurity classification codes. The updates would define which positions require a college degree and which do not. Additionally, updated classification codes would help to address cybersecurity jobs needed in the future, even in light of the emergence of AI. For example, humans will need to provide oversight, quality assurance, and operation of AI solutions. Human roles will also be required to review complicated logs and provide analysis of, and context for, the impacts of findings about AI systems. OPM and agencies should also continue to focus on developing processes and programs that decrease hiring time.

Continued emphasis on employee engagement is also critical for retention of cybersecurity professionals. Employees need to be engaged as organizations determine the appropriate role of AI. Enhancing the diversity of the workforce at decision-making and operational tables should be a key consideration, to include opportunities for neurodiversity workers. Visibility into a career path and promotions should be a priority for employers. Employers must also continue to optimize opportunities for remote work and work-life balance. Roundtable participants also discussed the opportunity to develop a national database of cybersecurity professionals to help to identify and hire qualified individuals more rapidly.

The participants in the roundtable identified the following workforce resilience recommendations to ensure readiness to address future shocks.

Table 4—Workforce Resilience Recommendations

• Use AI to improve the hiring process
• Enhance coordination between the public and private sectors by using proven models
• Improve cybersecurity classification codes and hiring processes
• Focus on employee engagement to support retention
• Create national database of cybersecurity professionals
• Create role-based cyber education models for disciplines within the organization beyond technical practitioner roles

Summary

In summary, executives from the government, nonprofit, academic, and commercial sectors convened, to discuss "Preparing Governments for Future Shocks: Building Cyber Resilience for Critical Infrastructure Protection." The roundtable resulted in a robust discussion regarding the topics of emergency preparedness and response, supply chain resilience, and workforce resilience. Attendees identified current challenges to protecting the critical infrastructure from the cybersecurity threat. Participants also identified best practices from both the public and private sectors, nationally and internationally. Finally, the group identified actionable recommendations to address the risks to the critical infrastructure, as summarized below.

Emergency Preparedness and Response Recommendations

- Implement National Resilience Plan NSM 22 and the Cyber Response and Recovery Funding (CRRF) Act to align aspirations and resources
- Continue to look at ways to optimize/streamline/create economies of scale, and created tiered governance structures for ISACs
- Develop and communicate incentives and resources to help SMBs prioritize cybersecurity
- Establish response and resilience frameworks that address the physical/cyber nexus and test plans
- Consider the inclusion of space systems as a critical infrastructure domain

Supply Chain Resilience Recommendations

- Establish center of excellence for procuring IT hardware in U.S.
- Create formal partnerships to share supply chain information across domains
- Shift to best value vs low-cost procurement models
- Use AI to drive real-time tracking
- Require attestations by third-party

Workforce Resilience Recommendations

- Use AI to improve the hiring process
- Enhance coordination between the public and private sectors by using proven models
- Improve cybersecurity classification codes and hiring processes
- Focus on employee engagement to support retention
- Create national database of cybersecurity professionals
- Create role-based cyber education models for disciplines within the organization beyond technical practitioner roles

About the Author

Lisa Schlosser
Cyber Security Advisor
Harrisburg University

Email: lschlosser@harrisburgu.edu

Ms. Lisa Schlosser currently resides in Delaware and volunteers: on the Board of Directors for Clear Space Theatre and Humane Animal Partners, and recently completed a term as an elected official for the City of Rehoboth Beach, Deleware. She also serves as a Cyber Security Advisor to Harrisburg University; as a therapy dog handler for Pets for People; and as an instructor at University of Maryland-Global Campus.

In her full-time career, Lisa was the Federal Deputy Chief Information Officer/Deputy Associate Administrator, Office of Management and Budget (OMB), under the President Obama Administration as a career SES. In this role, Lisa helped to oversee policy and budgeting related to the government's $86B information technology portfolio. During this time, Lisa was also an Adjunct Professor at Georgetown University, Washington, DC.

She previously served in the Environmental Protection Agency (EPA), as the Chief Information Officer (CIO), U.S. Department of Housing and Urban Development (US HUD), and the Associate Chief Information Officer/Chief Information Security Officer, US Department of Transportation (US DOT).

Prior to joining the Federal Government, Lisa worked in the private sector as a Senior Manager for Ernst & Young LLP, helping to establish the international Cyber Security Practice; and as a Vice-President for Global Integrity. Before entering the commercial sector, Lisa served in the US Army, and recently retired as a Lieutenant Colonel from the US Army Reserves.

Lisa holds a B.A. degree in Political Science from Indiana University of Pennsylvania, and an M.S. degree in Administration from Central Michigan University.

Recent Reports from the IBM Center for The Business of Government

Preparing governments for future shocks: An action plan to build cyber resilience in a world of uncertainty

by Tony Scott

Building On Regulatory Foundations
and Bridging to the Future
REGULATION

Building On Regulatory Foundations and Bridging to the Future

by Dan Chenok and
Susan Dudley

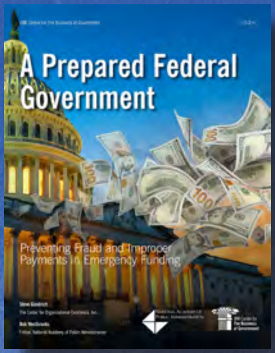
Helping Governments Prepare for Future Crises:
Using Metrics to Address Transformational Events

Helping Governments Prepare for Future Crises

by Karen Kunz and
Scott Pattison

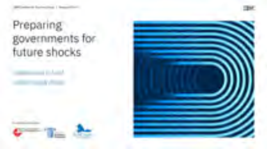
Preparing governments for future shocks: A roadmap to resilience

by Chris Mihm


A Prepared Federal Government
Preventing Fraud and Improper Payments in Emergency Funding

A Prepared Federal Government: Preventing Fraud and Improper Payments in Emergency Funding

by Steve Goodrich and
Bob Westbrooks



Preparing governments for future shocks: Collaborating to build resilient supply chains

by Robert Handfield Ph.D.

Partnering for Resilience

by Chris Mihm

Preparing Governments for Future Shocks: Building Climate Resilience

by Chris Mihm

Building future ready governments
Transformational lessons learned from a global shock

Building future ready governments - Transformational lessons learned from a global shock

by Cristina Caballe Fuguet, Kee Won Song and David Zaharchuk

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

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:.

IBM Center for
The Business of Government