AGENDA 2021 – DELIVERING OUTCOMES, BUILDING TRUST

TRANSFORMING INFRASTRUCTURE AND MANAGING RISK

OCTOBER 2020

American Council for Technology–Industry Advisory Council (ACT–IAC)

The American Council for Technology–Industry Advisory Council (ACT–IAC) is a non–profit educational organization established to accelerate government mission outcomes through collaboration, leadership and education. ACT–IAC provides a unique, objective, and trusted forum where government and industry executives are working together to improve public services and agency operations through the use of technology. ACT–IAC contributes to better communication between government and industry, collaborative and innovative problem solving, and a more professional and qualified workforce.

The information, conclusions, and recommendations contained in this publication were produced by volunteers from government and industry who share the ACT–IAC vision of a more effective and innovative government. ACT–IAC volunteers represent a wide diversity of organizations (public and private) and functions. These volunteers use the ACT–IAC collaborative process, refined over forty years of experience, to produce outcomes that are consensus–based.

To maintain the objectivity and integrity of its collaborative process, ACT–IAC welcomes the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of technology. For additional information, visit the ACT–IAC website at www.actiac.org.

This document has been prepared to contribute to a more effective, efficient, and innovative government. The information contained in this report is the result of a collaborative process in which several individuals participated. This document does not – nor is it intended to – endorse or recommend any specific technology, product, or vendor. Moreover, the views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development. Every effort has been made to present accurate and reliable information in this report. However, neither ACT–IAC nor its contributors assume any responsibility for consequences resulting from the use of the information herein.

For further information, contact the American Council for Technology–Industry Advisory Council at (703) 208–4800 or www.actiac.org.

TRANSFORMING INFRASTRUCTURE AND MANAGING RISK

In times of crisis, reliance on the federal government only increases. As the coronavirus pandemic demonstrates, the federal government must play a pivotal role in convening and coordinating a national response, leveraging unique personnel, technology and providing financial resources needed to respond and recover from a crisis. Yet the current crisis and the subsequent long recovery we face as a nation has brought us to an inflection point—a critical moment to re-imagine how our government operates and meets public needs.

This paper, focused on transforming the national infrastructure, expands on ACT-IAC's Agenda 2021 capstone document, "Delivering Outcomes, Building Trust," that includes recommendations on improving government service delivery to the public. Regardless of one's opinion about government's role in our lives, if it doesn't live up to expectations—if it doesn't "work" for the public—faith and trust will continue to decline. As our recent challenges have shown, how the government serves the public, protects the systems and information we rely on and responds and adapts to new opportunities and crises makes a great difference in how people feel about their government. As policymakers and government program leaders chart the course for the future, it's important to recognize that these are not mutually exclusive goals; they are highly interdependent. The government the public expects and deserves is one that delivers services that are accessible and meets personalized needs; provides for efficient resilient infrastructure which protects information and systems and institutions from adverse events; and is agile and adaptable in meeting emerging needs and embracing change.

Crises should be prevented or impact limited to the maximum extent possible. However, history shows that there will always be unpredictable physical disasters, along with successful cybersecurity attacks, and the federal government plays a critical role in how we respond. To deliver fundamentally better outcomes and build trust, the federal government needs to lead and enhance in three areas: 1) conducting better enterprise risk analysis and management to take action to lower the probability of crises occurring; 2) transforming our national infrastructure to better respond to disasters and attacks when they occur; and 3) increasing collaboration at all levels of government, as well as with non-governmental and private sector organizations, to improve data-driven decision-making and response, during a crisis and after. This will result in our country having a substantially improved resilience, being better prepared for and able to respond to crises of all kinds.

The remainder of this paper provides ideas to improve resilience in all types of crises. As part of improving resilience, we describe the need to transform the national infrastructure to support increasing our nation's cyber and physical resilience and the need to adopt enterprise risk management as a discipline. We discuss how the federal government can provide the leadership and means to accomplish the cyber resilience objective, especially regarding protection of federal agencies' data and systems. We also discuss approaches for physical infrastructure resilience. The benefits of such infrastructure transformations are explored, including more efficient government operations and services. We conclude by providing a series of bold, yet practical, recommendations for achieving the objective of substantially improving resilience of our national infrastructure.

ENTERPRISE RISK MANAGEMENT

Through improved management of enterprise risk, our government can better enable our society and our systems to better respond, withstand, and more effectively recover from adverse events—whether natural disasters or deliberate attacks—and whether those events occur in the physical or cyber space. Government agencies, at the federal, state, and local level, carry out risk management—they look at the risks that can lead to incidents and potential crises within the bounds of their agency and how they can effectively respond. Yet such an approach, as the coronavirus pandemic has demonstrated the imperative of looking across the enterprise, whether that be all of government, or even as a nation. Only through proper analysis and management of risks across and at all levels of government, can we improve the resilience of our nation, both to physical as well as cyber risks.

A key to managing risk is having access to accurate, complete, and timely information. Many government agencies can still improve how they analyze data and quickly communicate it to the right stakeholders to enhance decision-making processes and reduce risk across the enterprise. Government executives must lead and advance the practice of enterprise risk management within their agencies and across governments, at the federal, state, and local levels. While risks are unavoidable, especially given agencies missions and operational environments, risk management can effectively reduce the probability and harm through a coordinated effort to limit, mitigate and prioritize risks

TRANSFORMING NATIONAL INFRASTRUCTURE

Improving our enterprise risk management capabilities is imperative, but not sufficient, to ensuring our nation's resilience. Now, more than ever, we need a unified effort to transform the Federal Government's approach to national critical infrastructure—from the electrical grid and smart cities to our digital and cyber infrastructure—to support our ability to not only protect, but also respond to national crises

The Department of Homeland Security highlights the key elements of critical infrastructure using the following definition:

"Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The nation's critical infrastructure provides essential services that underpin American society." [https://www.dhs/gov/topic/critical-infrastructure-security]

Transforming our critical infrastructure, both physical and digital, requires a government-wide strategy that prioritizes investments based on where the greatest risks lie and other factors, including citizen impact, need for greater security, and the need to replace outdated, insecure systems. The foundation for this strategy is in place and government leaders and Congress must commit the necessary time and resources to make meaningful progress. To date, investments for infrastructure have largely been provided to individual agencies via appropriations bills, the process of which does not lend itself to prioritizing the most crucial infrastructure investments for the whole of government or the most important to serve the public interest.

Changing the way we prioritize investments in our critical infrastructure will enable us to respond more effectively to both physical as well as cyber risks and incidents. As an example, such transformation could enable the implementation of a tested, data sharing infrastructure with clear lines of authority and strict data standards that would strengthen communications and credibility of reporting during a crisis. A second benefit of such transformation is that it enables our government to operate more efficiently, including the ability to leverage modern digital capabilities to improve advance warning and preparedness for natural

disasters. For example, such transformation would enable us to better leverage data and the use of data analytics to improve government actions for specific geographic areas at risk.

ADDRESSING OUR DIGITAL INFRASTRUCTURE

Much of our national infrastructure is digital, and its transformation is driven by technical innovation and investment from the private sector, in which the United States is still a leader. Today, U.S.-based telecommunications companies are in a race to deploy 5G capabilities, enabling virtually unlimited bandwidth to homes and businesses, addressing networking limitations and enabling more Americans to enjoy access to high-speed digital offerings. Network, storage and computing infrastructures are in the midst of a major evolution away from dedicated, single function physical assets to virtualized, software-controlled assets. This gives commercial infrastructure providers unprecedented abilities to rapidly develop, deploy and enhance new services that are more adaptive, responsive, resilient and secure. Services such as Software-Defined Wide Area Networking (SD-WAN) allow enterprise network managers to add or reduce bandwidth, implement application-specific routing, monitor traffic patterns for anomalies, and much more, automatically and in near real time. Virtualized storage and computing resources that are increasingly defined, implemented and controlled in the cloud and "at the edge" underpin not only a more effective mobile workforce, but also revolutionary concepts such as smart cities and driverless vehicles. We have come to rely on our digital infrastructure to fuel our economy, create new and exciting new capabilities that positively transform the world around us, connect our families and friends, educate our children, entertain and inform, maintain a strong and capable means of defending our country, and engage in a globally-connected world.

THE CYBER THREAT

This wonderful new digital infrastructure has a significant downside. America's national security and national prosperity is potentially at great risk. Americans need a safe, secure, and trusted digital infrastructure to maintain our way of life and achieve our dreams. Yet the persistent vulnerabilities of our information infrastructure and the political and economic motivations of bad actors put our digital infrastructure at risk. Nation state actors are increasingly aggressive as they conduct cyber operations against the United States. Some, like Russia, employ misinformation to shape and negatively impact geopolitics as an offset to their waning global influence. Others, such as China, leverage cyber operations in their widespread theft of intellectual property to seek dominance in global markets.

Non-state sponsored threats continue to grow as the cost of entry to those seeking malice against the United States and its citizens has shrunk to the cost of a small computer connected to the Internet. Criminal groups have increased their cyber capabilities and activities against our commercial enterprises and our citizens. Motivated by a thirst for financial gain, cyber-criminal groups mount sophisticated campaigns against American citizens and businesses employing increasingly powerful tools to gain access to financial and personal information, intellectual property, or other information that can be sold in today's digital marketplaces. Today's cyber criminals also use ransomware to hold information hostage and extort individual victims, businesses, and government agencies.

Vulnerabilities run rampant throughout today's IT applications and infrastructure and make the threats all the more real and dangerous. Aging, complex and increasingly fragile technology continues to negatively affect America's ability to securely and efficiently operate its digital infrastructure. Despite massive investments in new technology, our IT legacy systems contribute to highly susceptible system misconfigurations that remain atop the greatest cyber vulnerabilities exploited by attackers.

And perhaps one of the greatest vulnerabilities is in the limited attentiveness to cybersecurity by the overall work force. We lack the capabilities to counter cybersecurity threats, the workforce knowledge to defend against social engineering, and the skills to ensure effective security is built into applications and infrastructure. Training for the overall workforce is generally minimal and treated as a compliance exercise. Cybersecurity often has been viewed as an issue for the technology teams rather than a risk worthy of boardroom attention. However, the threat is to the business and customers, and executives need to recognize that IT is just the vehicle used by attackers.

The Value of Information Ensures the Threat Will Grow

Information has tremendous value and is a commodity openly sought and traded. Many pundits say, "Information is the new oil" that fuels businesses across the world. Access to information has become big business, spawning the creation and growth of many of today's largest American brands, such as Amazon, Uber, Google, Apple, Microsoft, and Facebook. These companies have become, within a relatively short time, some of the most valuable companies in the world. Similarly, information is at the heart of competitive advantage for companies such as pharmaceuticals that have recently been reportedly hacked for drugs to counter COVID-19.

The United States government is one of the largest, if not the largest, acquirer and consumer of information on the planet. The information created, collected, aggregated, curated, and stored by the United States government is amongst the most valued information in the world. It includes sensitive personal data of every citizen and resident regarding our health and well-being, travel patterns, wealth, loans, taxes, education, environment, and economy. As such, it is not a surprise that federal, state and local governments are targets for extraction and ransomware.

Building on Past Cyber Successes

The United States government has made many attempts to build Cyber resilience. For example, the 2008 Comprehensive National Cybersecurity Initiative (CNCI) was a bold program designed to protect America's digital infrastructure launched during the Bush administration and embraced by the Obama administration. While some of its initiatives, such as enhancing cyber intelligence capabilities, had substantive improvements, other areas such as improving cyber education, securing supply chains, coordinating research and development efforts, and developing cyber deterrence strategies, have languished.

The United States government has also launched numerous commissions to address cyber threats. The recent Cyber Solarium Commission report features 54 legislative proposals and 60 discrete recommendations, many which are included in the Senate and House versions of the 2021 National Defense Authorization Act. Cybersecurity remains a bi-partisan issue. For over thirty years, each administration has built upon the lessons learned from previous administrations to address cyber risks. Obama administration initiatives to create a Cybersecurity and Infrastructure Security Agency (CISA) became a reality during the Trump administration. Nevertheless, translating aspiration into operational success remains vexing and elusive. The United States government must ensure that it follows through to deliver effective, efficient, and secure cybersecurity results to the American people.

ADDRESSING OUR PHYSICAL INFRASTRUCTURE

The coronavirus pandemic and a range of recent disasters have made visible the need for government to do better at preparing for and responding to physical crises. These events include both natural (e.g. hurricanes, tornadoes, and floods) and man-made events (e.g. forest fires, terrorist bombings, and oil spills), but almost always involve substantial risk to entire communities. The ability of government to operate responsively in the face of marketplace developments, changing citizen

needs and expectations, and the ever-evolving government policies requires a multi-faceted approach. Consider three scenarios of recent disasters where "business as usual" failed to protect lives and property: Camp Fire in Northern California caused by high winds knocking down hot power lines, the deadliest in US history; hurricane Maria; and the COVID-19 pandemic. The current pandemic has made many of these issues even more evident and the need for transformation even more stark.

Furthermore, new technologies are increasing the automation of the nation's critical infrastructure by integrating physical assets with digital control systems. From "Smart Cities" to autonomous vehicles to power transmission to manufacturing, emerging technologies like the Internet-of-Things and artificial intelligence have great potential to create new capabilities, efficiencies, and economic opportunities. But every new technology has not only potential value but also potential risks. Cyber-based disruptions to power plants and ransomware attacks holding hospital IT systems and data hostage illustrate the potential threats and risks. It is essential to identify, assess, and mitigate these kinds of risks as an integral part of all infrastructure modernization efforts and not wait until the damage is done to discover weaknesses.

Many government processes for preventing, minimizing, and responding to crises are based on government regulatory approaches and systems that are proving of limited value for the crises of the 2020s. Achieving both sustainable performance and resilience will require a broad set of changes, from the way government uses regulatory approaches and grants for addressing potential risks to the way government develops it workforce, ensures continuity of operations, and acquires goods and services. Government should embrace dynamic rather than static approaches to infrastructure risk management and that includes better use of data in decisions on investments for preparedness, mitigation, and response.

RECOMMENDATIONS

Improving resilience, security, and efficiency in government operations and coordinating cross-sector actions to improve resilience in the national infrastructure sectors is an ongoing transformational activity. But consistent policies, comprehensive data management and unified action remain elusive. To accelerate this transformation, –the government should focus on 5 actions that, taken together: (a) develop and enhance government and our infrastructure through new technology and techniques; and (b) shift the government and national focus from risk-avoidance to risk awareness and management, all while ensuring that these steps enable greater resilience and ensure mission outcomes. These actions will strengthen both "whole or government" and "whole of nation" enterprise approaches to risk management, decision-making and policy execution. Specific recommendations include:

1. Strengthen and coordinate efforts to leverage technology advancements to increase the performance, resilience and security of government operations.

Ongoing information and communications technology, analytics, security and software innovations offer great promise. Specific examples include network and data center virtualization; augmented intelligence and other applications of artificial intelligence; blockchain-based smart contracts; data analytics using geospatial information systems overlays; and modern application development practices. To take advantage of opportunities, government will need to address technical debt, pockets of obsolescence, outdated operating models and lagging workforce skills. This must start with two specific workforce actions: appointing Highly Qualified Experts (HQEs) and closing gaps in knowledge, skills, and abilities (KSAs) in emerging technologies and practices critical to improving resiliency. In addition, agencies should define and fund pilots and proofs of concept for measurably

improving resilience. Specific examples include: use of drones (potentially at FEMA, DOI, and the Forest Service) advanced automated identity credential and access management (ICAM) and continuous diagnostics and mitigation (CDM) tools (as the civilian government and DOD moves to Zero Trust), and machine learning sensor technology critical to smart highways, rail systems, and aviation management (for use throughout DOT, to include NHTSA, FRA, and FAA). Finally, maximizing use of internal partnerships (e.g. building on the use of Centers of Excellence and Quality Service Management Offices) should improve information sharing and teamwork needed for efficiency, continuity of operations, and ability to respond to future crises.

2. Adopt Zero Trust to secure government infrastructure.

The government will need to replace outdated perimeter-based security to reduce vulnerabilities and counter increasingly sophisticated "bad actors" (state-sponsored, criminal and insider). In addition, security via "check the box" compliance with regulations must be replaced with active security risk management. Non-IT leaders will have to embrace and fund a paradigm shift that requires automation of threat identification, isolation, and mitigation that extends across their organization and focuses on people, data and operations. IT leaders will have to implement clear and unified approaches to network, cloud, system and information security with automated compliance reporting, continuous risk mitigation, and a shift from role-based security to Zero Trust. The good news is that many government entities have elements of Zero Trust already deployed in their infrastructure, to include ICAM solutions along with continuous monitoring. Yet to build knowledge and organization buy-in, leaders in each department or agency should undertake at least one Zero-Trust pilot before the end of FY2021.

3. Establish an Enterprise Risk Officer (ERO) position in the Office of Management and Budget.

To directly address the need for the federal government to lead an effort to improve enterprise risk management for the nation, we recommend the establishment of an Enterprise Risk Officer position. This politically appointed position should be filled by an individual with strong credentials and proven experience in enterprise risk management, specifically with regard to infrastructure transformation, cybersecurity assurance and successful cross-organizational initiatives. The ERO would be responsible for leading the comprehensive, systematic, structured assessment of risks to drive mitigation efforts to improve infrastructure efficiency, resilience and security across government. As part of its responsibilities, the ERO should play a key role in setting executive branch budget priorities and allocations, identifying needed regulatory improvements, and developing guidance and directives to reallocate funds and modify regulations in the face of imminent threats in agency mission areas including public health, environment, public infrastructure, and cybersecurity. This will minimize piecemeal efforts, stove-piped solutions and wasteful overlaps.

4. Empower Agency Chief Risk Officers.

Departments and agencies need to have a deliberate, well-defined and agile process used to identify and manage risk. While agencies, via OMB regulation, have designated a senior official as a Chief Risk Officer (CRO), these positions have been focused on financial management and reporting. Such positions should be empowered to ensure agency processes and procedures are adequate to both meet mission requirements and address agency risk. And with an ERO in place, CROs will work closely with the ERO to ensure there is effective enterprise risk management across the federal government. Further, as part of the CRO's duties, each department and agency

should include risk management scenarios in their training and exercise programs to promote continually assessing and improving their risk management program.

5. Establish use of Outcome Leaders as a best practice across government.

Coordination across government entities is challenging. To facilitate faster, more effective execution of administration infrastructure transformation priorities, Outcome Leaders should be assigned to initiatives involving the need for cooperation across multiple government entities including those at the federal, state, and local levels. As such, Outcome Leaders should be assigned at multiple levels of government, including for each agency or entity participating in any cross-organizational initiative. In the latter case, the agency or entity level Outcome Leader would be responsible not only for ensuring that outcomes are achieved at the agency or entity level, but also for ensuring that those outcomes remain coordinated with the desired outcomes of the cross-organizational initiative.

The need for transparent, proactive risk identification and management has never been more important. The impact of the coronavirus and our government's response to it, while disruptive to normal operations, also offers an opportunity and sense of urgency for change. Given this evolving situation, the federal government should apply an enterprise risk management approach and invest in technology that allows for accurate, complete, and timely information. By eliminating information silos, aligning governing procedures with risk mitigation efforts, and delivering the right information to the right people at the right time using the latest technologies, the federal government can make better decisions based on a more holistic view of risks and their interdependencies that ensures resilience for the long-term.

Transforming Infrastructure and Managing Risk

There are many more specific actions that can be taken. These are addressed in our series:

Agenda 2021
Delivering Outcomes – Building Trust
A Guide for the Future of Government Agenda

ACT-IAC stands ready to help advance these ideas into action. Please contact us at https://www.actiac.org/contact-us or 703-208-4800.

ACT-IAC
Advancing Government