MARCH 2023

Innovation for Resilience

A Focused Study on Workforce, Climate, Supply Chain, and Cyber Resilience

AUTHORS

Hadeil Ali
Naz Subah

Morgan Higman
Joseph Majkut

Emily Harding
Harshana Ghoorhoo

Suzanne Spaulding
Devi Nair
Sophia Barkoff

ADVISERS

Nicole Aandahl
Bob Kolasky
James Andrew Lewis
Jake Harrington

A Report of the CSIS Diversity and Leadership in International Affairs Project, Energy Security and Climate Change Program, International Security Program, and Strategic Technologies Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

MARCH 2023

Innovation for Resilience

A Focused Study on Workforce, Climate, Supply Chain, and Cyber Resilience

AUTHORS

Hadeil Ali
Naz Subah

Morgan Higman
Joseph Majkut

Emily Harding
Harshana Ghoorhoo

Suzanne Spaulding
Devi Nair
Sophia Barkoff

ADVISERS

Nicole Aandahl
Bob Kolasky
James Andrew Lewis
Jake Harrington

A Report of the CSIS Diversity and Leadership in International Affairs Project, Energy Security and Climate Change Program, International Security Program, and Strategic Technologies Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

© 2023 by the Center for Strategic and International Studies. All rights reserved.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Acknowledgments

The authors would like to thank the CSIS iLab and publications team, in particular, Jeeah Lee, Rayna Salam, Lauren Bailey, Katherine Stark, Phil Meylan, and William Taylor, for their tremendous work on this report. The authors would also like to thank Ian Barlow, Lachlan Carey and Jaleah Cullors for their research contributions to this project.

The authors are also extremely grateful for the public and private sector leaders that participated in expert roundtables and private interviews in support of this project. This report is largely a reflection of their insights and concerns about the U.S. government's efforts to grow resilience.

This report was made possible through the generous support of Deloitte Consulting LLP.

Contents

Introduction

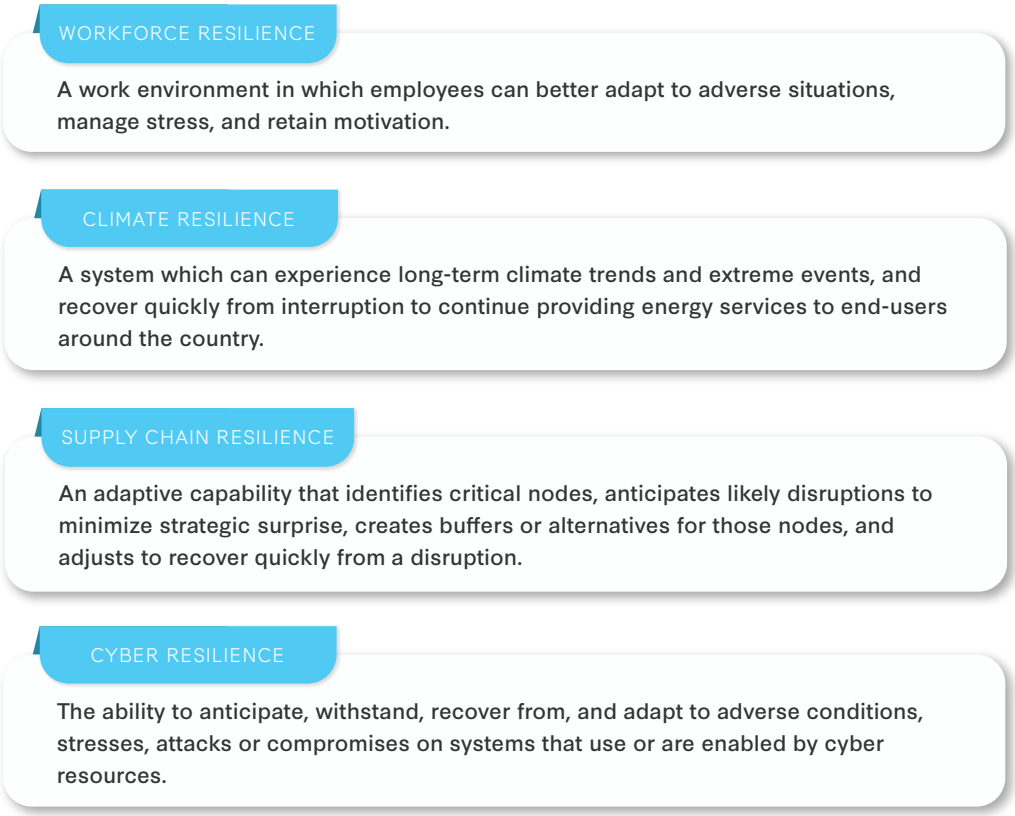
Today's constantly evolving threat landscape underscores the difficulties associated with striving for an elusive end state such as "total security." Instead, the U.S. government should invest in opportunities that can consistently mitigate emerging risks with greater agility. While there is increasing knowledge that resilience is important, its practical applications, associated costs, and needed reforms are not as clearly understood.

Currently, there is little consensus among federal regulators and industry players about how exactly resilience should be defined and measured, and the tangible benefits of resilient systems are realized only in the face of major shocks to a system. However, today's threats necessitate a federal government that can remain resilient and promote overall resilience in systems critical to the functioning of entire sectors before, during, and after an incident.

In the broadest sense, resilience measures how well an individual, institution, or society can prepare for and respond to shocks to the system and endure, perhaps even thrive, under prolonged periods of stress. For the federal government, this definition then raises questions about the essential processes and operations that should be prioritized during a comprehensive recovery and the tools at the government's disposal needed to actively create greater resilience.

For the past year, the Center for Strategic and International Studies (CSIS) studied how the U.S. government can better position itself to promote resilience across four connected focus areas: the workforce, climate security, supply chains, and cybersecurity. Through independent research and a series of roundtables and expert interviews with current and former government officials, academics, think tank practitioners, and industry leaders, the CSIS project team investigated the current capacity for resilience within each focus area, barriers to creating greater resilience, and opportunities for

Figure 1: Definitions of Resilience



Source: Authors' own definition for Workforce Resilience, Climate Resilience, and Supply Chain Resilience; NIST definition for Cyber Resilience available at: https://csrc.nist.gov/glossary/term/cyber_resiliency#:~:text=Definition(s)%3A,are%20enabled%20by%20cyber%20resources.

enhancing overall resilience between the focus areas. This report is a compilation of the four research commentaries produced by each focus area team.

Ultimately, a key theme emerged across the topics: intentional efforts to create diversity, equity, and inclusion (DEI) considerations, by way of enhancing workforce resilience, is foundational to both creating and sustaining long-term resilience. Resilience starts with a robust, dependable, and well-trained workforce that can surge in capacity during a crisis and maintain high levels of performance through the entire recovery process. A resilient workforce is comprised of resilient individuals who are able to adapt to change and manage high-stress situations. Creating a resilient workforce in turn creates resilient communities that are crucial for recovering from society-wide crises, such as a climate-related incident. A diverse workforce is more likely to anticipate a wider range of potential crises, allowing for better planning and preparation. A diversified workforce and vendor base is also important for the sake of reducing the concentration of risk, a key requirement for building reliable supply chains that can withstand major shocks. In an area like cyber that is plagued by a workforce shortage, investing in DEI and workforce resilience is essential to retain talent, mitigate burn out, and inspire the creativity and energy needed to tackle today's challenges. Innovation happens on both sides of resilience: innovation is required to build resilience and enhanced resilience increases capacity

for innovation. A critical piece of that is developing a secure and resilient workforce from which other types of resilience can be cultivated.

This report will begin with an overview of the criticality of workforce resilience and its connection to DEI. The report will then examine innovation and resilience more broadly in the context of climate challenges, supply chain disruptions, and cybersecurity. It will include recommendations from each focus area on how the federal government can more aggressively implement concrete resilience strategies within departments and agencies and in partnership with private industry.

Current systems and government processes were not necessarily designed with resilience in mind, but they can and should adapt to meet today's challenges.

DEI and Workforce Resilience

By Hadeil Ali and Naz Subah

Project Adviser: Nicole Aandahl

This is an updated version of the published commentary "DEI Is Foundational to Workforce Resilience" on June 1, 2022.[1]

In the past decade, events linked to geopolitics, climate change, and technology have created disruptions and unpredictable change. The Covid-19 pandemic exacerbated these trends, leading organizations to think through their capacity for resilience in the face of rapid change. Entities are investing in organizational resilience—the ability to withstand disruptive events and emerge stronger—in order to stay relevant, innovate, and ultimately thrive.[2] Organizations can develop this ability by building financial, operational, and workforce resilience.

Workforce resilience is used to describe a work environment in which employees can better adapt to adverse situations, manage stress, and retain motivation. There are three core indicators of resilience in the workforce:

1. A sense of security at work;
2. A strong sense of belonging with the employer; and
3. A level of adaptability and motivation among employees that facilitates reaching their full potential.

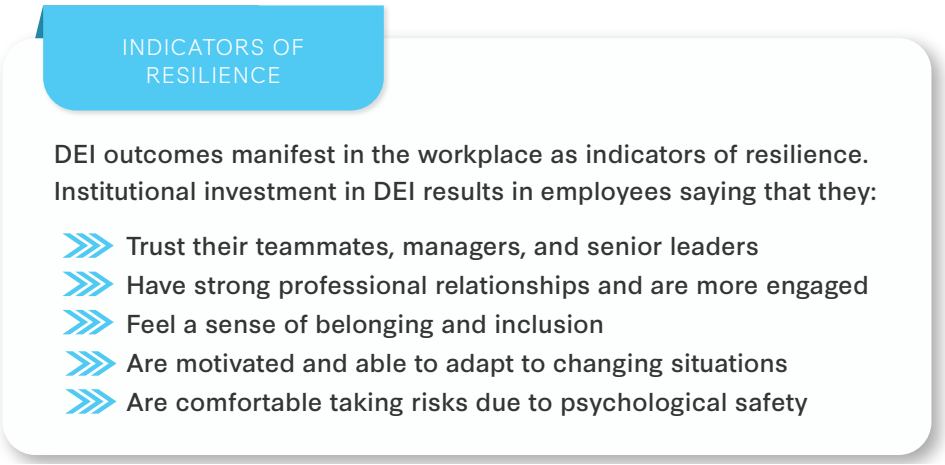
A 2020 ADP survey found that only 19 percent of U.S. workers consider themselves "highly resilient."[3] Resilient individuals can cope with workplace stressors, remain productive and creative under pressure, and maintain a positive outlook toward change. Resilient teams can effectively complete tasks and adjust as necessary despite disruption. A foundation of trust built on resilient teams leads to effective decisionmaking at the executive level despite uncertainty. A resilient workforce is the backbone of a resilient organization.[4] These organizations are prepared for uncertainty, adaptable in

the face of change, and collaborative in how they work; they demonstrate high levels of trust between leaders and employees and act responsibly.

Effective DEI policies and practices strengthen resilience. A diverse team is more innovative, and a diversified workforce is better prepared to mitigate the effects of groupthink. When employees experience equity and inclusion in the workplace, their levels of trust and belonging increase. Inclusive organizational practices, policies, and processes promoted and practiced by leaders provide a sense of security for employees and enable higher levels of engagement. These experiences reinforce individual and collective resilience, enabling organizations to perform their best even during times of crisis.

Resilient organizations foster security, belonging, and adaptability through a culture of inclusion and equitable processes that promote trust.[5] If the federal government wants to grow overall resilience to survive future shocks, it needs to focus efforts on workforce resilience, in part with DEI initiatives. These initiatives will lead to employees feeling a sense of security at work, a strong sense of belonging, and the ability to adapt and stay motivated, especially in times of crisis. The future of the federal government and its ability to perform essential functions is dependent on its ability to build workforce resilience.

Figure 2: DEI as Foundational to Workforce Resilience



Source: Author's research and analysis from various external sources.

Sense of Security

Trust in organizations is integral to employees feeling a sense of security at work. Research shows that employees who do not trust their organizations are more likely to question job security.[6] On the other hand, employees who trust their colleagues, managers, and leaders are 42 times more likely to be highly resilient.[7] Trust also reinforces psychological safety at the individual and team levels. Psychological safety is an environment that encourages, recognizes, and rewards individuals for their contributions and ideas by making individuals feel safe when taking interpersonal risks.[8] Feeling safe allows moderate risk taking, creativity, and innovation, which are all crucial to agile responses in the face of disruption. Studies show that all high-performing teams have one thing in common: psychological safety.[9] Therefore, the federal

government should build trust and psychological safety, not only to engender a sense of belonging in employees but also to reap the benefits of high performance.

Organizational trust is built through fairness, or in DEI terms, equity. Without equity, individuals feel othered and are at risk of disengaging or, even worse, leaving due to feelings of insecurity.[10] Equity in teams acknowledges that every employee brings a unique set of identities, backgrounds, and perspectives and that these are all to be celebrated and valued. Teams and individuals who score high in trust are better suited to build strong relationships with one another.[11] Professional relationships buttress psychological safety and create a solid support system in difficult times. To achieve equity in workforce representation, the federal government should revamp its hiring and recruiting processes. Changing hiring practices requires identifying and eradicating biases and systematic barriers that have historically marginalized certain groups. To achieve equity in workplace experience, the federal government needs to identify where employees are perceiving inequities (e.g., compensation, benefits, and promotions) and address them. However, to achieve true equity, the federal government should overhaul its advancement and succession planning practices as well.

Sense of Belonging

Social belonging is a fundamental human need.[12] Research shows a high sense of belonging is linked to 56 percent higher job performance, 50 percent lower turnover risk, and 75 percent fewer sick days.[13] These are all metrics used to measure employee resilience and, in aggregate, workforce resilience. Diverse representation is a precursor to fostering belonging and inclusion.[14] The first step is to ensure that every element of diversity is represented and valued within the workforce (e.g., background, education, ability, and socioeconomic, caregiver, or veteran status). The federal government has better representation at junior levels, but this declines within senior levels.[15] A truly diverse workforce is one that is representative of the U.S. population. Millennials and Generation Z currently comprise 40 percent of the U.S. workforce and are projected to increase their labor force participation rate in the next decade.[16] The federal government can achieve this diverse workforce by reconstructing its sourcing, recruiting, and hiring practices while also examining representation at every level.

Representation alone, however, is not enough to build belonging; it should also be done by engaging employees in meaningful ways and addressing high-priority needs.[17] Recognizing employees' unique contributions and proactively communicating about changes or opportunities are two ways to boost engagement.[18] Transparent communication can spur belonging, not just between colleagues but also between the senior leadership and the full organization.[19] Open channels of communication require leadership to gather feedback regularly from employees and involve them in decisionmaking.[20] Consistent and intentional involvement gives employees ownership over outcomes and amplifies feelings of inclusion. Employees who feel included and involved are more engaged and less likely to leave. Gallup research shows that organizations with higher retention rates are more likely to be high performing compared to their peers.[21] Retention initiatives, however, require continued investment and long-tailed changes to an organization, making them harder to implement and bear success. Thus, the biggest benefit of employees feeling a sense of belonging is workforce retention. Strong retention rates help the federal government avoid the long and cumbersome process of backfilling roles that require niche expertise and high security clearances.

Adaptability and Motivation

The federal government needs to focus on engaging its employees by offering them a purpose connected to organizational strategy.[22] Investing in purpose is critical to creating a more motivated, adaptable, and agile workforce.

The Covid-19 pandemic has also shifted the focus of the U.S. workforce. Ongoing isolation and lack of connection coupled with the new flexibilities of remote work have allowed certain employees to redefine their purpose and values regarding their organizations.[23] This paradigm shift has spurred the "Great Resignation" as employees quit jobs to pursue passion projects, join organizations that align with their personal values, and attain work-life balance.[24] A larger share of the workforce and especially Millennials and Generation Z prioritize environmental, social, and governance (ESG) principles and DEI when selecting an employer.[25] Research also shows that women and individuals from Generation Z are most likely to want flexible working environments.[26] The organizations best suited to attract and retain top talent are those that can articulate their purpose and synchronize it to their employees and prospective candidates' values.[27] If the federal government does not prioritize communicating its strategies in these arenas, it risks failing to attract and retain top talent. Purpose drives motivation, which in turn drives productivity and engagement.[28]

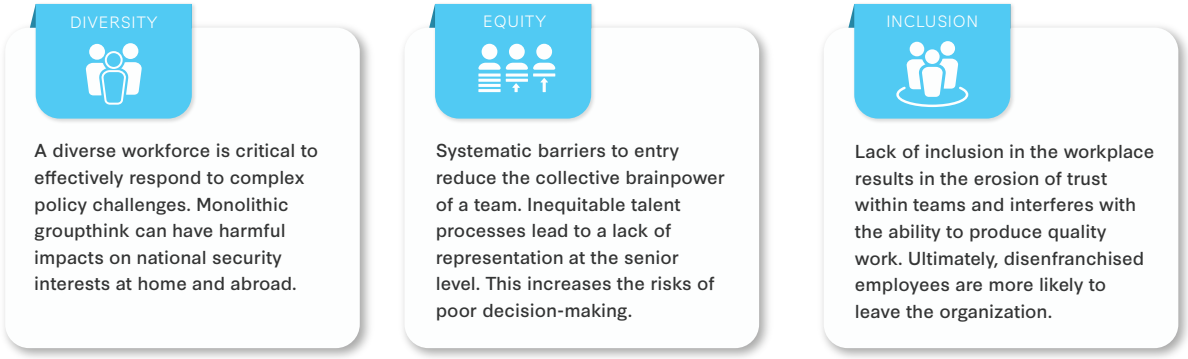
Employers are concurrently facing a burnout crisis brought on by the pandemic—with employees reporting mental health declines, challenges meeting basic needs, and exhaustion.[29] These feelings drive absenteeism in the workplace: around 63 percent of employees are more likely to call in sick if they are feeling burnt out.[30] Companies in the United States lose $300 billion per year as a result of workplace stress. The World Health Organization estimates that lost productivity at work costs the global economy $1 trillion each year.[31] To combat burnout, several organizations have offered additional resources for mental health support (e.g., digital apps), customized financial wellness counseling, and caregiving support. The federal government needs to consider the demands of a shifting workforce that is both burnt out and increasingly eager to work for institutions that deliver on holistic employee well-being.[32] When employees feel healthy and secure (e.g., physically, mentally, and financially), they are more likely to engage at work and be resilient against changes in the workplace. Additionally, when employees feel supported to combat sources of stress, they feel more confident in their ability to weather adversity.[33]

In an increasingly unpredictable world with political, environmental, and socioeconomic challenges, building workforce resilience will be a salve for the federal government. By fortifying its workforce, the federal government is better suited to address risks to national security and provide integrated solutions to complex global problems. Secure, included, and engaged employees will readily tackle future crises in an agile manner. Taking an employee-first, DEI-based approach to building workforce resilience will strengthen institutional resilience and allow the United States to effectively lead on the global stage.

Building toward Workforce Resilience: Recommendations and Next Steps

In June 2021, President Biden signed an executive order on "Advancing Diversity, Equity, Inclusion, and Accessibility in the Federal Government," placing a national spotlight on diversity, equity, inclusion, and

Figure 3: DEI & National Security



Source: Author's research and analysis from various external sources.

accessibility (DEIA).[34] The Biden administration has issued several executive orders prioritizing resilience in supply chains, climate, and cyber that include aspects relevant and critical to strengthening workforce resilience, demonstrating that DEIA and resilience are top of mind for policymakers.

Government bodies such as the Department of State and the U.S. Agency for International Development established DEIA offices and released strategic plans to address how they will embed DEIA into their organizational strategy. The Office of the Director of National Intelligence (ODNI) recently released its 2021 Annual Demographic Report measuring the composition of the intelligence community as well as opportunities to improve the hiring, promotion, and retention of employees of historically underrepresented backgrounds.[35] This report highlights strategic initiatives undertaken by the intelligence community to invest in workforce readiness. The Office of the National Cyber Director, established in 2021, is also prioritizing efforts to increase its current and future workforce resilience by investing in the American people. These are great examples of how the federal government has begun the process of recognizing that a secure nation starts with a secure and resilient workforce.

To make further progress, the government should continue to be intentional about investing in DEI initiatives.

1. The challenge of recruitment is an underlying factor in all diversity, equity, and inclusion efforts. The federal government should identify and eliminate barriers to entry for historically marginalized groups. To do so, the government needs to fully understand where the barriers exist and what feasible options are available to address them. A standardized mechanism to track recruiting practices and outcomes will tackle hiring gaps and unlock the potential for success in other DEI initiatives.

2. The federal government should reevaluate talent processes to eliminate biases in decisionmaking for critical moments like advancement, promotions, and succession planning. Increased transparency and equity in compensation and benefits will address sentiments around inequities in the workplace.

3. The federal government should devise a mechanism to gather employee feedback (e.g., annual survey) regularly and involve employees in decisionmaking. These efforts establish psychological safety and ensure consistent two-way communication for an increased sense of belonging.

4. No initiative can be successful without the active support of senior leaders; therefore, accountability needs to be placed on management for advancing DEI within the workplace. As an institutional priority, DEI progress should be measured and evaluated using key performance indicators and embedded in all senior executive performance plans. Recognizing leaders for creating and maintaining a diverse and inclusive environment reinforces the organizational commitment to promoting DEI.

At its core, resilience is about people and processes. Today's threats not only require a fully staffed federal workforce, but a workforce that is sufficiently prepared to maintain operations during a crisis and provide diverse perspectives about any potential cascading effects from disruptive events. From human-made incidents to natural disasters, intentional attacks to unintentional accidents, continuity of critical government functions cannot be guaranteed without a strongly supported federal workforce.

Figure 4: Workforce as the Foundation for Federal Government Resilience

Workforce resilience underpins the federal government's efforts to advance its climate, cyber, and supply chain resilience.

Source: Authors' creation.

Climate Resilience

By Morgan Higman and Joseph Majkut

This is an updated version of the published commentary "The National Climate Strategy Needs a Resilience Focus" on October 24, 2022.[36]

Over the next three decades, climate change will increase the frequency and severity of certain weather extremes and lead to geographic and ecological challenges in every region of the United States.[37] At the same time, the energy transition is dramatically shifting the energy system toward greater utilization of renewable energy, storage technologies, and higher electricity consumption.[38] These trends create both a challenge and an opportunity for increasing resilience to the hazards associated with climate change.

In the absence of measures to enhance resilience, more frequent and severe weather associated with climate change is anticipated to pose significant risks to the energy system. In addition to billions of dollars in direct costs to the federal government, climate damages could have cascading effects on interdependent critical sectors, such as telecommunications and transportation, and disproportionately impact already vulnerable and disadvantaged groups.[39] For this reason, the energy sector should be at the center of the federal government's efforts to address climate change.

Funding from the Inflation Reduction Act (IRA) and the Infrastructure Investment and Jobs Act (IIJA) have brought forth a new era of climate action in the United States.[40] These federal investments will help put the country on track to meet President Biden's emissions reduction targets and make the energy transition a central political and economic priority.[41] Within this new climate agenda, resilience is increasingly imperative to the plans, programs, and workforce development strategies of the federal government.

Presently, U.S. resilience initiatives are more fragmented than systematic, but there are clear indicators of progress that can and should be built upon. In the near term, executive action and the IRA and IIJA

provide new directives and funding to elevate climate considerations across federal operations and beyond. Making the most of this opportunity, and enhancing resilience in the long term, will require more systematic and accessible data and planning tools, new professional and institutional capacities, and strategic coordination across the federal government, states, communities, and industry.

Building a New "Culture of Resilience"

The challenge of increasing climate and energy resilience begins with creating a culture that recognizes ongoing and future climate change risks as a reality. In 2021, President Biden issued Executive Order 14008 to place "the climate crisis at the forefront of foreign policy and national security planning" by directing federal agencies to develop plans for increasing resilience to the impacts of climate change in their own operations and assets.[42] In response, more than 20 major federal agencies published climate plans.[43] The plans demonstrate some clear themes and opportunities for improvement.

To integrate climate considerations into their organizational missions, federal agencies need systematic, science-based data and tools. These resources should balance rigorous quantitative analysis with techniques or user interfaces that are widely accessible—relatively simple, intuitive, broadly applicable, and shared. The Department of Defense (DOD)'s Climate Assessment Tool (DCAT) provides a first-in-class example.[44] DCAT illustrates the anticipated effects of eight climate hazards in two future scenarios (lower and higher future warming) and two epochs (2035–2064 and 2070–2099) at DOD facilities around the world. Most agencies are still developing resources and strategies to systematically assess climate risks to agency missions and operations.

Sophisticated models are also needed to help the federal government consider interdependencies and the potential for cascading failures across systems and sectors. Considerations of interdependencies are especially important in light of energy transitions and the electrification of critical end uses, such as transportation and heating buildings. Accounting for interdependent vulnerabilities requires the development of a hierarchy of information needs and capabilities across multiple authorities, sectors, and scales. The Department of Energy (DOE)'s Integrated Multisector Multiscale Sector Modeling Project highlights dynamic interactions among climate, energy, water, land, and socioeconomics.[45] It provides insights about the vulnerability and resilience of coupled human and natural systems, from local to continental scales, under scenarios of near-term shocks and long-term stresses. Now is the time for such resources to reach widespread use, with clear connections between model outputs and decisionmaking.

Executive Order 14057 includes new requirements for routine departmental climate literacy and sustainability training programs.[46] Agency trainings are expected to help all staff integrate climate considerations into the normal course of business. In the context of evolving climate science information, technologies, and federal policies, these investments in personnel are critical for promoting science-based decisionmaking and, in some cases, overcoming loss of expertise in recent years.[47] Currently, each agency is developing an individual curriculum. A climate literacy standard across them could provide a foundation of shared principles and training materials while allowing each agency to incorporate its own informational needs.

Climate considerations in agency operations are a first step toward creating a new culture of resilience, but institutionalizing climate readiness across all sectors and communities will require close federal coordination with decisionmakers at different levels.

Enhancing Intergovernmental and Public-Private Collaboration

Federal climate resilience initiatives rely in no small part on state and local governments and the private sector. State and local governments steward much of the country's land and public infrastructure and regulate the private interests which own and operate energy infrastructure. Greater resilience requires the willingness and ability of these counterparts to identify and act upon opportunities to increase resilience.

Climate data tools and resources under development by federal agencies can benefit subnational and private decisionmakers. Platforms for resource sharing can reduce duplicative efforts, enhance efficiency, and facilitate interagency, intergovernmental, and cross-sectoral coordination, creating a common foundation for climate decisionmaking. The Climate Resilience Toolkit is the clearinghouse for U.S. data and climate resources.[48] It centralizes information provided by various agencies, but it is not set up for securely sharing and building on the back end of proven proprietary tools such as the DOD's DCAT.

Semiformal networks can create opportunities for deeper collaboration. At least one institution of this kind is already in place. The Critical Infrastructure Sector Partnerships program under the Department of Homeland Security (DHS) hosts an Energy Sector Council facilitated by the DOE.[49] It provides a venue for federal, state, local, and industry experts to work on energy resilience planning and implementation. The council has not historically focused on climate change, but it provides a valuable foundation for prioritizing resilience, with an emphasis on system interdependencies (e.g., electricity and gas) and sector interdependencies (e.g., energy and water). A private DHS information network allows this council to share trusted but unclassified information among members. Likewise, dedicated networks could facilitate collaboration on climate and energy resilience among federal agencies and between the federal government and state, local, and industry leaders. A new resilience planning and resource hub in the early stages of development under the DOE can and should leverage the benefits of this proven model.[50]

State, local, and industry decisionmakers also play an important role in developing performance goals and monitoring progress on enhancing resilience. The development of standardized, quantifiable resilience indicators has posed a persistent challenge at the distribution level in the electricity sector.[51] Across the country, there is little consensus among state regulators and industry players about how resilience should be defined and measured. Many states simply rely on measures of electricity reliability, which do not adequately reflect differences in criticality, vulnerability, and adaptive capacity across society.[52] Across the United States, there are no metrics to constitute reasonable outages given different natural disaster intensities or standards for reasonable response times to repair disaster-related outages.

With funding from IIJA, federal agencies are well positioned to set up new rules of engagement. Applications to access the recently opened $2.3 billion in DOE formula grants require that states describe their plans for fund distribution and investment, prioritizing "projects with the greatest community economic benefit in reducing the likelihood and consequences of disruptive events."[53] This broad requirement is of mixed value. It does not do much to establish shared core measures of resilience across the country, but it does create needed momentum for subnational resilience initiatives and a template for tracking progress. Federal identification and promotion of innovative, feasible, and replicable state strategies will be important in driving broad, long-term resilience with IIJA and IRA funding. A new resilience planning and resource hub in the early stages of development under the DOE can and should highlight successful strategies for state, local, and private stakeholders seeking to refine resilience goals, metrics, and investments.

Intergovernmental and public-private collaboration can facilitate greater efficiency and help align national resilience priorities with more localized priorities. Ensuring the effectiveness of these collaborations and investments over time will require greater transparency, evaluation, and commitment to accountability.

Revaluating the Cost-Benefit Analysis

Investments in resilience can be expensive, and it can be difficult to calculate the return on such investments because benefits are often realized only intermittently in the face of major threats. As a result, these investments can be difficult to evaluate and justify.[54]

Frameworks for clarifying the value of resilience are under development. The General Services Administration is working to estimate climate vulnerability in life-cycle cost analyses of federal investments in buildings, products, and services.[55] Similarly, the DOE and DOD have developed tools to quantify the costs, benefits, and trade-offs of investments to ensure power availability to on-site, critical energy loads during grid outages. The DOE's benefit-cost approach guides the selection of energy efficiency and renewable energy technologies by type and size.[56] The DOD instead takes a cost-effectiveness approach, which begins with a specific resilience objective—a minimum acceptable level of power disruption—then compares different strategies to achieve that minimum.[57] As with tools to model climate risks, these resources for cost-benefit calculations are not yet widely shared or standardized across agencies or sectors. Common methodologies and resource sharing across authorities could offer important benefits, enabling a more efficient and consistent basis for decisionmaking and evaluation.

More transparent, standardized methods for accounting of resilience costs and benefits can also ensure that environmental justice, equity, diversity, and inclusion are prioritized in resilience investments. This imperative is a cornerstone of the new federal climate agenda. It is especially important because low-income populations and communities of color are more likely to live in the most vulnerable areas, are less able to evacuate, experience greater damages, and have less access to disaster assistance resources from agencies such as the Federal Emergency Management Agency (FEMA).[58] These challenges are perpetuating social inequalities over time.[59]

Integrating equity and inclusion into resilience faces two challenges: defining groups or communities that should benefit and identifying how benefits accrue. The Climate and Economic Justice Screening Tool (CEJST) created by the White House Council on Environmental Quality is expected to help federal agencies incorporate the government-wide Justice40 Initiative requirements.[60] The tool brings together data from established but siloed databases, such as the Environmental Protection Agency's EJSCREEN, the DOE's Low-Income Energy Affordability Data (LEAD) platform, and the FEMA National Risk Index.[61] As a result, the CEJST tool provides foundational insights about how household, community, and regional attributes shape vulnerability.

As particularly vulnerable communities are identified, needed investments among them may vary, from energy efficiency upgrades and storage systems to hardening of homes and community infrastructure and even relocation assistance.[62] Given the wide range of investments that can bolster adaptive capacities, resilience initiatives should be led by inclusive procedures for engaging communities and establishing performance objectives that reflect their needs and priorities. State and federal authorities should also be attentive to the technical and organizational capacity of vulnerable

communities and minimize administrative burdens that can result in missed opportunities and unspent funds.[63] Finally, initiatives that promote climate and energy resilience can and should contribute to economic resilience, and vice versa. Deeper connections between economic and climate vulnerabilities are needed to identify and promote potential co-benefits in these areas, with careful accounting for anticipated and realized benefits.[64]

Supporting resilience and adaptation initiatives abroad is a small but critical part of the current federal resilience agenda. More investment and support are needed to enhance the resilience of developing countries which will be most acutely affected by the intense physical effects of climate change in the coming decades. Enhanced resilience in developing countries is especially important because climate change has the potential to exacerbate instability and conflict, which could create additional demands on U.S. diplomatic, economic, humanitarian, and military resources.[65] For this reason, as the federal government expands its resilience expertise and administrative capacity, the Biden administration is also considering how to efficiently extend U.S. resources to enhance the resilience of vulnerable developing country partners.[66] Like initiatives in the United States, successful resilience strategies in Africa, small island developing states, and elsewhere must begin with broad recognition of anticipated hazards and local perspectives about how to prioritize and protect critical infrastructure and vulnerable communities.[67] This information should inform decisions about where and how to invest in organizational capacity building, workforce development, and new tools and technologies to mitigate anticipated climate hazards are needed to enhance the resilience of developing countries which will be most acutely affected by the intense physical effects of climate change in the coming decades. Enhanced resilience in developing countries is especially important because climate change has the potential to exacerbate instability and conflict, which could create additional demands on U.S. diplomatic, economic, humanitarian, and military resources.[68] For this reason, as the federal government expands its resilience expertise and administrative capacity, the Biden administration is also considering how to efficiently extend U.S. resources to enhance the resilience of vulnerable developing country partners.[69]

Like initiatives in the United States, successful resilience strategies in Africa, small island developing states, and elsewhere must begin with broad recognition of anticipated hazards and local perspectives about how to prioritize and protect critical infrastructure and vulnerable communities.[70] This information should inform decisions about where and how to invest in organizational capacity building, workforce development, and new tools and technologies to mitigate anticipated climate hazards.

Sustaining a robust strategy for resilience requires more than predictions about hazards and identification of vulnerabilities. It also requires decision frameworks for understanding what can and should be made resilient, how resources should be allocated, and the value of investments over time.

Building toward Climate Resilience: Recommendations and Next Steps

Climate change commitments, policies, and programs tend to be concentrated heavily on mitigation, emissions reduction, and the transition to a low-carbon economy. But climate hazards and extreme weather events are increasingly making headlines.[71] An initial round of resilience IIJA funds is set for distribution this fall, and incentives from the IRA can accelerate the resilience benefits of new clean

energy technology innovations and developments.[72] Now is the moment for resilience, recognizing that certain changes are already taking place and that mitigation efforts underway may not be enough to avert more severe climate hazards.

A coordinated federal approach for resilience will reduce climate hazard risks to missions and operations, accelerate cooperation on climate action, drive innovation and economic development, and promote equity, inclusion, and environmental justice. But fractured authority, limited economic incentives, and the novelty of climate risks are significant challenges that should be addressed in order to mainstream resilience and aggressively incorporate climate change considerations into decisionmaking processes.

The federal government of the United States has a key role to play in establishing a national approach. As a large operational enterprise with transparently managed assets, the federal government can demonstrate best practices in planning for climate impacts and designing resilient systems. As a source of funding for state programs and the private sector, the federal government can incorporate both climate and resilience considerations in society-wide planning, where interdependence with the energy sector creates resilience challenges. And as a principal agent in the gathering and dissemination of environmental, economic, and social data, the federal government can be a clearinghouse for information on changing climate risks, societal vulnerabilities, and resilience strategies.

Resilience investments can and should provide clear and direct benefits to local communities, regional economies, and national security. Presently, U.S. resilience initiatives are more fragmented than systematic and more anecdotal than comprehensive. But there are clear indicators of progress in the contents of agency plans, the development of data and tools, and in partnerships with state, local, and industry decisionmakers. Continued coordination, standardization, inclusivity, and evaluation are key levers for a timely, robust U.S. strategy for climate resilience.

The following are key initiatives the federal government should prioritize to enhance climate resilience:

1. The federal government needs to develop resources and strategies to systematically understand (a) climate-related interdependencies across sectors and systems and (b) climate risks to agency missions and operations.

2. The federal government should also increase interagency connectivity of these resources and expand access to these tools at the state and local levels.

3. Federal agencies can help states and industry create concrete, functional definitions for climate resilience and metrics to measure and assess resilience.

4. Federal agencies should create and share frameworks to measure and account for the value of climate resilience when making investments in infrastructure.

5. When making climate resilience-building investments in vulnerable communities, state and federal authorities should consider the technical and organizational capacity of these communities, minimize administrative burdens, and account for economic resilience.

6. The federal government should consider international climate resilience a foreign policy priority and help developing countries create their own means to define and measure climate resilience, enabling smarter investments in infrastructure.

Supply Chain Resilience

By Emily Harding and Harshana Ghoorhoo

Project Adviser: Bob Kolasky

This is an updated version of the published commentary "Building Supply Chain Resilience" on December 15, 2022.[73]

In late 2021, the port of Los Angeles was in the middle of a crisis. Ships were lined up for miles, unable to move products through a bottleneck at the port.[74] The port's executive director said the port had the capability to run 24 hours a day, but a shortage of truck drivers and nighttime warehouse workers prevented a nonstop schedule. He cited the tremendous challenge of getting "this entire orchestra of supply chain players to get on the same calendar."[75]

The Covid-19 pandemic brought the fragility of global supply chains into stark relief. A complex system of producers and suppliers collapsed under the weight of high demand, just-in-time delivery, workforce shortages, and low supply. Labor markets were deeply disrupted as some workers were unable to come to work for health or childcare reasons, and the "Great Resignation" deepened the problem. Producers over-indexed on efficiency in production and did not build enough buffer to anticipate disrupted global trade. Even the defense industrial base was not able to withstand the shocks. The war in Ukraine has further exacerbated the situation, highlighting single-threaded suppliers and foreign control of key elements.

Shocks will never be completely foreseeable or preventable. Instead, government and industry should focus on resilience, or maximizing quick recovery from disruptions. The White House's executive order on supply chain security (EO 14107) highlights that "more resilient supply chains are secure and diverse—facilitating greater domestic production, a range of supply, built-in redundancies, adequate stockpiles, safe and secure digital networks, and a world-class American manufacturing base and workforce."[76] In operational terms, a resilient supply chain identifies critical nodes, anticipates likely disruptions to minimize strategic surprise, creates buffers or alternatives for those nodes, and adjusts to recover quickly from a disruption.

Challenges with Securing Supply Chains

A supply chain crisis is not any one problem; instead, it results from a combination of poor visibility that hampers planning, a narrowing of a pipeline that creates focused risk, and then a shock that throws the system off the rails.

POOR VISIBILITY INTO A DEEP SUPPLY CHAIN

Visibility risk is at the core of supply chain vulnerability. Without complete insight into the spreading web of suppliers, there is always a risk that an unforeseen disruption will derail production. However, modern supply chains have so many layers that constrained time and research resources prevent full visibility.

Prime suppliers often trust that their subcontractors are monitoring their own supply chain, which leads to potential vulnerabilities going unnoticed. Companies may not know when an adversary or competitor acquires a sub-subcontractor, or the chain of custody for a critical widget might be obscured. The DOD suffers from this problem much like any other consumer. The DOD relies on contracts with prime contractors and expects those primes to manage their own supply chains, but too often that trust has proven to be misplaced.

While the DOD once conducted its own supply chain security evaluations, that capability has atrophied over time as Congress has sought to shift the burden onto contractors to verify their own work. As a result, DOD officials are now grappling with how to evaluate layered risk. One interviewee for this project said that there are excellent software tools that can map the many layers of the supply chain, but none of those tools describe the capacity of production within each production line or identify which systems use the same sub-tier suppliers. In other words, if Prime Contractor A understands their supply chain, and Prime Contractor B understands their supply chain, but A and B are unaware they are both drawing on Subcontractor C, the capacity and resilience of the supply chain is actually more fragile than either might assume.

Rules designed to protect proprietary information also contribute to blind spots in the supply chain, according to CSIS's interviews. Each prime should rightfully expect their intellectual property (IP) to be protected, but that protection obscures information relevant for risk assessments and restricts some data from access. For example, to populate supply chain management tools, the DOD needs to get approval from each contractor to access proprietary data. Further, the DOD cannot use contractors to pull together this data because that might open the door to industrial espionage, which means that the DOD cannot supplement its full-time workforce as it usually does.

NARROW PIPELINES CREATING FOCUSED RISK

Focused risk happens when a supply chain narrows to a single source or single location that can be disabled by a shock event. For example, a critical facility or transportation route could be in the path of a tsunami, terrorist violence could imperil a key rail line, political instability could displace a workforce, or a public health emergency could lead to an extended lockdown.

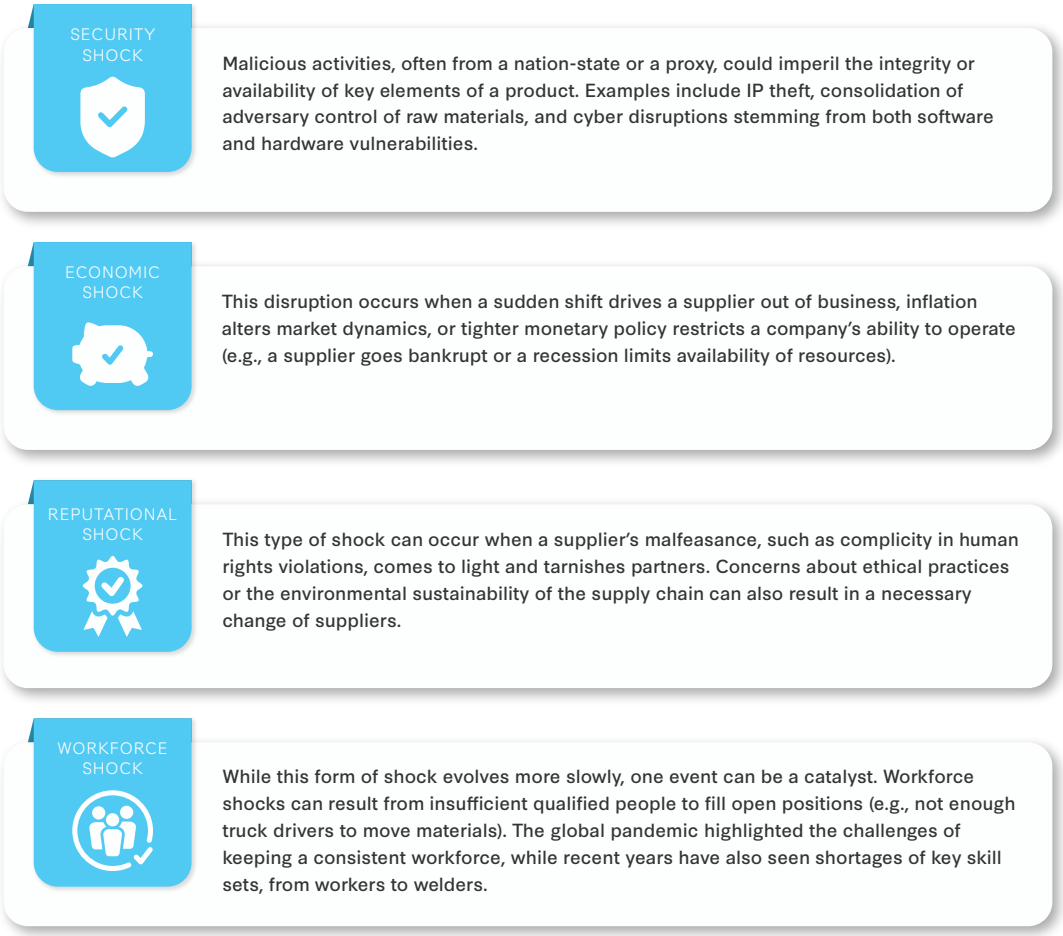
Foreign dependence aggravates focused risk in supply chains, with Taiwan's near-monopoly on the world's most advanced semiconductors being a prime example of concentrated risk. A conflict over Taiwan would cut off global access to about 90 percent of high-end semiconductors.[77] Any conflict in the Pacific would lead to massive disruptions to a range of supplies; China controls 87 percent of

the market for permanent magnets, which are used in the manufacturing of electric vehicle motors, electronics, wind turbines, and defense systems.[78] The United States is still dependent on China for rare-earth and other minerals, critical to goods from consumer electronics to weapons systems.[79]

SHOCKS HAPPEN

The diagram below is far from a comprehensive list of shocks, but it illustrates some of the most common causes for supply chain disruptions.

Figure 5: Types of Supply Chain Shocks



Source: Authors' research and analysis.

Building toward True Supply Chain Resilience: Recommendations and Next Steps

A mindset of resilience means assuming disruptions will occur and planning for a rapid recovery to acceptable functionality.

With regard to supply chains, the federal government should identify opportunities to enhance resilience in three steps:

1. The federal government should improve visibility to minimize blind spots in the supply chain.
2. The federal government should identify potential shocks and evaluate which ones are most likely and most disruptive.
3. The federal government should create contingency plans and buffers for the most critical, vulnerable portions of the supply chain.

IMPROVE VISIBILITY TO MINIMIZE SURPRISE

Maximizing visibility into supply chains should always be the goal. The DOD should step up its staff resources to improve visibility into critical defense supply chains. Further, this staff should build resilience by identifying gaps and working to match those gaps to nontraditional suppliers.

When engaging in evaluation of supply chains, entities should put a premium on constructing a diverse team of analysts. Geographic, socioeconomic, and racial and gender diversity on a team can contribute to fewer blind spots. For example, a person whose family includes truck drivers and Midwesterners might understand transportation during extreme weather better than most. Immigrants and children of immigrants might provide critical insights into seasonal labor concerns and visa challenges. Assembling a team that represents a diverse set of disciplines has repeatedly been shown to result in better outcomes.

Entities should focus on predicting and extending the lifespan of critical components to minimize urgent need. "Digital twins"—or virtual representations of real-world objects that mirror the environment and stresses on the object—are increasingly becoming the go-to industrial approach to accurately predicting the operational lifespan of products to anticipate the demand cycle.[80]

IDENTIFY POTENTIAL SHOCKS

Entities should identify single points of failure or places where the supply chain narrows to criticality. Evaluating each critical piece for threats, such as risk of environmental shock or workforce scarcity, in a rigorous way can then inform scenarios analysis and crisis production plans. Part of that rigor is a diverse team doing the analysis.

The U.S. government has a role to play both anticipating potential security shocks and facilitating information sharing. The Committee on Foreign Investment in the United States needs to keep evolving to identify potential threats early and create a robust support structure for industry. Further, the United States should use existing regulatory authorities and industry groups to encourage critical infrastructure providers to conduct an in-depth, rigorous analysis of potential shocks to their systems and the challenges for recovery.

Creating a diverse workforce and talent pipeline can insulate against labor shifts. The DOD has attempted to create geographic diversity in its pipeline, and industry is working on ways to cultivate both a cleared and uncleared workforce for added diversity. Getting a security clearance can be time consuming and a large hurdle, eliminating some potentially talented candidates who could contribute at the unclassified level. The creation of apprenticeships and embedded trade schools can also facilitate a strong pipeline of certain key skills. Some entities are creating intentional pathways to underserved communities, such as the National-Geospatial Intelligence Agency's initiatives to collaborate with the local community surrounding its new facility in St. Louis.[81]

CREATE BUFFERS AND CONTINGENCIES

The simple act of rigorous evaluation and contingency planning can lay bare a previously unconsidered problem. Advance planning for workforce resilience in particular can pay dividends. Taking the next step to create buffers for key nodes in a supply chain can shift an event from a catastrophic shock into a temporary disruption.

Create a Diversified Workforce Pipeline

The U.S. government should create a national imperative for bolstering industrial skills, such as encouraging trade apprenticeships, while industry could partner with unions, which have proven proficient at retraining and upskilling.[82] In order to sustain their diversified workforce, companies also need to take steps to promote inclusivity. Social inequality presents an underlying challenge both to incorporating a robust pipeline into the defense industry and to growing a diverse array of potential suppliers.[83]

Digital Seed Bank

A database of information, which one participant described as a public-private digital seed bank, could stockpile plans for creating critical components. In a crisis, when current supplies cannot meet sudden and urgent demand, the government can match those plans with companies who might be well suited to shift production lines to meet the dire need. Critically, participating companies would need reassurances about protection of IP or compensation for its use.

Vendor Diversification

A vendor chain that builds in diversity will more effectively create resilience.[84] Vendors that cover several geographic areas are insulated against environmental or security shocks, while vendors that represent a variety of backgrounds and experiences will be better able to identify and anticipate potential disruptions in the market. Entities should place a high value on a diverse supply chain as a hedge against shocks. The DOD is already working to bring in new entrants to the DOD contracting market to improve diversity and innovation, but more can be done.[85] For example, the DOD's strict requirements and complicated contracting processes can be a barrier to entry for smaller businesses, so elements of the department are working with potential contractors to discover the biggest cost drivers and adjust or eliminate them. Since the economic incentives that pushed production of key parts overseas still exist, the DOD is also looking for ways to incentivize onshoring or "friend-shoring" using existing regulatory authority.

Strategic Stockpiling

While big pieces of equipment are impractical to stockpile, the most critical, or most likely to break, components of those pieces could be stored. For example, rather than store an entire generator, utilities can store the elements of their existing generators that are most prone to failure. Additive manufacturing can be a flexible and cost-effective alternative for some parts, providing a bridge capacity for creating those critical parts until regular supply chain mechanisms have recovered.[86]

Nearshoring and Friend-shoring

Companies should carefully evaluate which key parts need to be located within friendly territory, for reasons ranging from counterintelligence concerns to human rights violations to a dependable justice system for resolving disputes. Coordinating with allies and partners for secure manufacturing of precursors is critical. The G7 could be a vehicle for this coordination, given its flexibility, decades

of experience working through economic challenges, including key U.S. allies, and high-level coordination mechanisms. As one workshop participant said, "The challenge in operational resilience is fundamentally an international game."

As the conversation on supply chains builds renewed urgency, EO 14017 has laid a solid foundation for continued steps toward resilience. The 100-day follow-on report to EO 14017 said: "America's approach to resilient supply chains must build on our nation's greatest strengths—our unrivaled innovation ecosystem, our people, our vast ethnic, racial, and regional diversity, our small and medium-sized businesses, and our strong relationships with allies and partners who share our values."[87] Innovation drawing on these strengths is the surest path to true resilience.

Cyber Resilience

By Suzanne Spaulding, Devi Nair, and Sophia Barkoff

Project Advisers: Bob Kolasky, James Andrew Lewis, and Jake Harrington

This is an updated version of the published commentary "Investing in Federal Cyber Resilience" on February 24, 2023.[88]

On December 23, 2015, Russia knocked out power for 250,000 customers in Ukraine. The hackers had taken over the control systems for several electricity plants and remotely shut down the transmission of energy.[89] Power was restored in six hours. Ukrainians found workers who knew where the breakers were physically located along the grid. They got in trucks, drove to those locations, and manually put the breakers back in place. Manual backups to the remote operation, and workers who understood those manual systems, provided resilience that kept this cyberattack from becoming a major disaster.

According one definition from the National Institute of Standards and Technology (NIST), cyber resilience is "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources."[90] The more resilient an agency or department, the greater its ability to bounce back after a cyber incident or maintain mission-essential functions in a degraded environment. The Cyberspace Solarium Commission, which highlighted resilience as one of six foundational pillars in its final report, further emphasized that cyber resilience is about recovering from attacks that "could cause harm or coerce, deter, restrain, or otherwise shape U.S. behavior."[91] Resilience denies an adversary the benefits they seek, potentially altering their cost-benefit analysis. For a municipality or business, resilience in the face of a ransomware attack provides more time and more options in deciding how to respond to the attacker's demand. Systemic resilience across the economy makes the United States more secure. The federal government can contribute to resilience in each of these contexts.

Cyber Resilience and Cyber Risk Management

Like the other challenges discussed in this report, cyber security is an exercise in risk management, not risk elimination. Managing risk depends on assessing (1) the kinds of incidents that would have the greatest impact or consequences (e.g., on key functions, operations, or reputation) and (2) the likelihood of that incident happening. Likelihood is a factor of threat (i.e., who or what is coming at you) and vulnerability (i.e., the conditions that threat might exploit). Much of the conversation around cybersecurity focuses on threat and vulnerability. Focusing on understanding and mitigating the potential consequences of malicious cyber activity is at least as—if not more—important and is the key to building resilience. Cyber threats and vulnerabilities are constantly changing and predicting future threat vectors is nearly impossible. Effective resilience, particularly reducing dependence on networked functions, can mitigate damage regardless of the cause of disruption.

Resilience planning assumes that prevention will sometimes fail, and the threat actors may get in the system. Breaches are going to happen. It asks entities what plans and capabilities have been put in place to reduce the impact of that breach on its systems, key assets, functions, and business requirements.

Organizing toward Resilience: Federal Government Structures

Over the last several administrations, organizational structures have evolved to reflect the need to focus on understanding and building resilience against the impact of cyber incidents as an essential element of managing cyber risk.

To provide White House-level guidance and ensure coherence in approaches across the various agencies and departments with responsibilities for helping to manage cyber risk, the Office of the National Cyber Director (ONCD), an office initially proposed by the congressionally-mandated Cyberspace Solarium Commission, was established in 2021.[92] As part of its stated vision, the ONCD is working to "increas[e] present and future resilience."[93] The former national cyber director Chris Inglis, who stepped down in February 2022, described his role as the coach, while the Cybersecurity and Infrastructure Security Agency (CISA) as the quarterback.[94]

While still too early to grade the ONCD on its efforts, current initiatives, such as its focus on cyber workforce and education issues, signal the ONCD's intent to leverage its role as a coordinator to ensure the federal government is working toward greater resilience.[95] The workforce issue in particular is of critical importance in cyber, given that a number of positions are unfilled and that proposed resilience plans can only be properly staffed by attracting and retaining a cyber workforce (see "Workforce Resilience" on page 4). This has been a long-acknowledged issue for the federal government and private sector alike, so the ONCD's leadership is a welcome opportunity.

The Office of the National Cyber Director also recently released the administration's national cyber security strategy.[96] This comes on the heels of the administration's National Security Strategy, published in October 2022, and the May 2021 executive order on "Improving the Nation's Cybersecurity," which provided an initial blueprint of key themes emphasized in the strategy.[97] The national cyber strategy can be applauded for its focus on resilience as a key pillar of activities. The strength and success of the cyber strategy will turn on its implementation, but the recommendations are moving in the right direction.

For its part, in 2014, the Department of Homeland Security brought together cyber and physical risk analysts to strengthen its understanding of interdependencies and cascading consequences from disruptions in critical infrastructure, including from malicious cyber activity. This led to ongoing work by the National Risk Management Center (NRMC) to identify and map national critical functions (NCFs).[98] CISA has defined these as functions that are so vital that "their disruption, corruption, or dysfunction would have a debilitating effect" on U.S. security.[99] Through the NRMC, public and private entities can coordinate and prioritize different response imperatives around the identified NCFs.

CISA is particularly well suited to conduct this analysis for two key reasons. First, it is responsible for coordinating across all infrastructure sectors, which enables it to assess risks not just within a sector but also to recognize and work to address cross-sector dependencies. Second, CISA leads efforts to assess and address physical and cyber risks, as well as the convergence of these risks. Its work over two decades to model and mitigate physical consequences informs efforts to understand the full impact of cyber disruption.

Another crucial source of insights into consequences is after-action reviews of actual incidents. This is why CISA's Cyber Safety Review Board is such an important part of building resilience. This joint public/private effort to fully understand significant incidents can provide important lessons, assuming their insights are heeded and actions to address identified gaps are forthcoming.

This effort to understand the real-world consequences of incidents also relies on insights from those with deep expertise in the critical functions at issue. It requires understanding the operations that are controlled by or are otherwise dependent on networked systems. It also requires understanding the regulatory and policy environment that may impact options for response. This expertise comes from the infrastructure sectors themselves and from the departments and agencies that have worked with those sectors for many years. This is the thinking behind designating Sector Risk Management Agencies such as the Department of the Treasury and the Department of Energy (DOE) as the leads for their respective sectors..[100] Broader regulatory agencies like the Securities and Exchange Commission and the Federal Trade Commission can also use their authorities to incentivize resilience. Accurate financial accounting depends on data integrity, and consumer protection can include oversight of breaches that impact the public. Even antitrust oversight can potentially play a role in addressing risk concentration.

Finally, there is the NIST, the agency that already oversees current standards in this space for federal and private entities alike, which is being asked to work with outside partners to help measure and develop new standards related to enhancing cyber resilience. The NIST's cybersecurity Risk Management Framework has contributed substantially to efforts to enhance cybersecurity across government, the private sector, and academia.[101] The NIST's ability to leverage diverse talent to develop and inform its standards and best practices makes the agency well postured to expand this work into the area of cyber resiliency, particularly through its ongoing efforts in the areas of zero-trust architecture and software supply chain security.

To ensure long-term resilience, the federal government should continue to strengthen the coordinating capabilities of entities such as CISA, the ONCD, and the NIST and resist calls for a standalone department that attempts to centralize cyber expertise in a single agency.[102] Implementing such a move would be extremely difficult bureaucratically and is likely to undermine efforts at comprehensively addressing cyber risk, including building resilience, by narrowing cybersecurity to a focus on technology rather than enterprise risk management that includes continuity planning based on consequence expertise.

Investing in Resilient Infrastructure

Congress appropriated funds for a Cyber Response and Recovery Fund created by the Infrastructure Investment and Jobs Act (IIJA) but missed the opportunity to require that the broader funding for infrastructure projects include specific resilience measures.[103] **Cyber resiliency experts need an equitable seat at the table to drive informed cyber resiliency decisions in project development and planning, and risk informed trades in project execution.**

Congress also needs to provide consistent funding year after year to support measures that strengthen resilience. Additionally, Congress should be willing to appropriate greater funds to the departments and agencies that are growing their cyber portfolios for preparedness and resilience. CISA has received significant increases in funding in recent years, with a roughly 25 percent budget increase between FY 2020 and FY 2022.[104] The FY 2023 Omnibus spending bill allocates $2.9 billion for CISA—an increase of 12 percent from FY 2022. In addition, Congress appropriated up to $20 million for the Cyber Testing for Resilient Industrial Control Systems program at the DOE.[105] However, essential agencies such as the NIST and the Department of the Treasury have not received funding commensurate with their increased roles. Given that these agencies require a highly specialized workforce, the lack of adequate funding could lead to losses in that workforce in the near future.[106]

Finally, a separate but related part of investing in actual resilient infrastructure is investing in systems and processes that can maintain essential operations during and immediately after an incident and actively investing in the pre-incident planning process. For instance, the Cyberspace Solarium Commission advocated that the federal government should actively map out and invest in Continuity of the Economy (COTE) plans.[107] This theme was indirectly highlighted in ONCD's new cyber strategy as well, where it notes that "in the event of a catastrophic cyber incident, the federal government could be called upon to stabilize the economy and aid recovery." The strategy goes on to say that planning a response in advance of the event (as opposed to during or after) could provide "certainty to markets and make the nation more resilient."[108]

Investing in Process

Per Executive Order on Improving the Nation's Cybersecurity, federal agencies will be required to strengthen cyber postures by transitioning to zero-trust architectures (ZTA)—a security philosophy that adopts the approach of "never trust, always verify." This approach is inherently about resilience, assuming access by a bad actor and limiting the blast radius of an attack, instead of reducing perimeter vulnerabilities.[109] While the very act of pushing for ZTA is demonstrative of a commitment by the federal government to prioritize resilience, the test for departments and agencies will be if their proposed ZTA plans evaluate how certain processes, not just technologies, also can be strengthened to enhance resilience. This will be especially important in the face of implementation time and budget constraints.

As was noted by consulted experts, there is currently a misconception that investing in resilience or other "right-of-boom" mitigation strategies can be expensive and rarely yields near-term benefits.[110] That is not always the case. For instance, there could be an expensive solution for hardening the network, but a cheaper alternative might be to install detection tools or identify ways to disconnect key elements from the network. Similarly, there might be nontechnical, cost-effective solutions that should be identified and supported ahead of time as a part of comprehensive resilience planning, such

as putting in a hand-crank to permit operations to continue, mechanical gauges to provide redundancy for some supervisory control and data acquisition (SCADA) systems, or providing paper ballots to mitigate the prospect that a hack—or alleged hack—could undermine trust in an election.

Motorists wait in line to refuel at a Circle K gas station on May 12, 2021, in Fayetteville, North Carolina. Most stations in the area along I-95 are without fuel following the Colonial Pipeline hack.

Photo by Sean Rayford/Getty Images

Colonial Pipeline

On May 7, 2021, Colonial Pipeline, America's largest fuel pipeline, suffered a ransomware attack on its corporate network. While the attack did not directly impact operations, the loss of capabilities such as billing led to disruptions in operations, including distribution, whose processes depended upon those corporate functions. The failure to anticipate this interdependence weakened Colonial Pipeline's resilience. Moreover, while the disruption did not seriously impact the supply of fuel to gas stations for any significant period of time, the failure of the company to communicate effectively with the public led to panic buying, long lines at gas stations, and some shortages due to the increase in demand. Planning for effective communications is also a key aspect of resilience.

Making trade-offs that prioritize mitigating consequences, in addition to or as an alternative to investing in measures to address vulnerabilities, require the federal government to continuously evaluate what it means to be secure and what it takes to sufficiently recover from a cyber incident. The solutions and recommendations will vary across agencies and missions. For example, the defense and intelligence communities' cybersecurity mission requirements may require different risk management approaches when trying to protect particularly sensitive mission data. This also means the federal government, as is noted in the ONCD's new cyber strategy, needs to "ensure that resilience is not a discretionary element of our new technical capabilities but a commercially viable element of the innovation and deployment process."[111] Investing in processes that enable resilience will require organizations to prioritize consequence mitigation of cyberattacks. This includes being more intentional about efforts to map out interdependencies and cascading effects of incidents; only then can organizations begin to understand how cyber incidents can impact critical functions.

Some systems may be too complex to fully map and predict, which places greater pressure on processes and people agile enough to adapt to unforeseen consequences. It is essential to have a strong, reliable, trained workforce. Employees have to be brought into cyber resilience processes so they are capable of operating in degraded environments and adapting to new risk mitigation approaches. A workforce that is too rigid—or not bought in—can undermine resilience. On the other hand, an agile workforce cannot only sustain essential missions but also potentially innovate for greater resilience going forward.

Enhancing Intergovernmental and Public-Private Partnerships

The federal government should work effectively with the private sector, as well as state and local governments and quasi-governmental entities, in order to build cyber resilience, especially considering that most critical infrastructure is currently owned and operated by the private sector.[112] This requires the government to play a role as a convenor, facilitator, and supporter for the private sector.

INFORMATION SHARING

As noted above, assessing and prioritizing consequences to critical infrastructure require insights from businesses, particularly when trying to understand the full impact of a cyber incident. Yet, the private sector is often reluctant to share information on the impact of cyberattacks due to concerns about optics, potential liability and regulatory action, and implications for their bottom line. There are also lingering concerns about the government's ability to protect their information, despite the government's excellent track record of doing so. Companies view these costs as outweighing the expected benefits. Governments are challenged to provide actionable, real-time information back to companies. It is incumbent on the government to demonstrate the value of robust information sharing.

The recently enacted Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) moves beyond a voluntary information-sharing approach and tasks CISA with developing regulations for cyber incident reporting.[113] By creating an aggregated data set of incidents, the government could better assess the nature, scale, scope, and costs of cyber risks, as well as the return on investment in cyber resilience. **To maintain essential trust with the private sector, and encourage broader sharing on consequences and resilience, CISA—or some other federal entity—should prioritize efforts to use the data collected under CIRCIA to produce timely and actionable products back to the private sector. Congress should provide adequate funding for that analytic work.**

The government can provide statistical analyses that help make the business case for resilience. Where there is ultimately a delta between what a business can be expected to invest in resilience and what the nation needs from that business, government will need to intervene with carrots or sticks or both. This is in line with the ONCD's national cyber strategy, which emphasizes the benefits of finding ways to make the market work more effectively to improve cybersecurity but also recognizes that there are situations in which regulation is required and where financial aid may be necessary. Government should devote analytic resources, working closely with industry, to identify those circumstances and help inform policy decisions about how best to incentivize the level of resilience required for national security and the security and safety of the public.

In general, greater information sharing will be more meaningful if it is in furtherance of operational collaboration. CISA's newly created Joint Cyber Defense Collaborative (JCDC) is another step in the right direction, as are the information-sharing models established between the government and sector-specific Information Sharing and Analysis Centers (ISACs).[114] However, what is still lacking is an interoperable tool to facilitate sharing of not just data but also insights and analysis between industries and the government. **To solve this problem, a Joint Collaborative Environment (JCE) should be established for industry operators to access and analyze operationally relevant data.**[115]

EXERCISE

The importance of analytically driven exercises cannot be emphasized enough. Not only are they critical to establishing relationships ahead of time and growing muscle memory for how to quickly respond during an incident, but they also help participating individuals identify potential cascading effects and assess where there needs to be greater redundancy built into continuity plans. Individual entities should exercise their response plans, but joint public-private exercises are also important for effective resilience. A good example is the Treasury Department's Hamilton Series cyber exercises done in partnership with the Financial Services Information Sharing and Analysis Center (F-ISAC).[116] Similarly, the North American Electric Reliability Corporation's Electricity ISAC (E-ISAC) biennially holds GridEx, the largest grid security and resilience exercise in North America, and CISA hosts Cyber Storm, a biennial exercise that simulates a large cyber incident that impacts multiple sectors.[117] These should be models for other sectors and their sector risk management agencies. **In addition, national-level exercises should be reinvigorated to include the most senior levels of government and include a focus on continuity of the economy.** These exercises should aim to make effective use of data and technology to create realistic scenarios, improve the exercise experience, and employ performance metrics to understand effectiveness within and between exercise events.

Managing the Workforce

In response to Russia's invasion of Ukraine, CISA activated Shields Up, a campaign outlining the ways in which primarily nongovernmental entities should maintain vigilance during heightened geopolitical tensions.[118] CISA continues to report that the threat level remains high, which prompts questions about how long nongovernmental entities will be able to maintain a "crisis" posture. This concern extends to the federal government as well. A key concern is burnout of those accountable for staying vigilant against cyber risk. This highlights a critical piece of enhancing cyber resilience: to continue operations at high levels through a prolonged crisis, it is essential to invest in a resilient federal workforce and, especially in this context, a fully staffed and prepared cyber workforce.

TRAINING THE GENERAL FEDERAL WORKFORCE

At a minimum, all federal employees must be trained to follow basic cyber hygiene protocols. This is important not only to help with prevention, but once an incident occurs, a disciplined workforce can take steps to help contain the situation. The next step is continuity of operations training for the larger workforce, not just IT professionals. Continuity of government training and exercises should always include an element of cyber disruption. These trainings should also prepare workers to manage smaller cyber disruptions beyond those that present as larger cyber incidents (e.g., planning federal law enforcement operations even if the case management system is down).

A well-trained workforce has the potential not only to scramble to keep the lights on but to come up with innovative ways to operate that build even greater resilience in the future.

MANAGING THE FEDERAL CYBER WORKFORCE

As of July 2022, there are roughly 700,000 open cybersecurity positions in the United States, roughly 40,000 of which are within the federal government.[119] Further, the actual cyber workforce skews white and male, leaving women and people of color drastically underrepresented, and largely includes individuals that share similar education and professional experiences.[120] As noted above, this reduces overall resilience.

At every level there is room for the federal government to invest in and remove barriers to hiring and retaining technical and nontechnical cyber talent.[121] From tapping into diverse viewpoints to identify and assess unique cyber risks, to calling up reserve forces that can support an already understaffed and potentially fatigued cyber workforce, the federal government cannot afford to sideline significant parts of the population. Instead, it should work to remove barriers, from accessibility barriers to unnecessary certificate, education, and clearance requirements that can be time intensive or financially difficult to obtain. The DHS Cybersecurity Talent Management System (CTMS), which was launched in 2021, takes a step in the right direction by addressing some of the key issues related to hiring and attracting top cyber talent. It will be important to assess CTMS's successes in the coming years to see where there are still gaps in the talent management process and if there are best practices that can be scaled across industries.

In addition, as the federal government helps build the pipeline for cyber talent by supporting STEM education in K-12 and higher education, the government also should promote the development of civic skills and civic knowledge.[122] Only by instilling a sense of civic responsibility can the United States hope to have a workforce that fully embraces cybersecurity as a shared responsibility.

Building toward True Cyber Resilience: Recommendations and Next Steps

Though there are agency-specific recommendations that the federal government can consider in order to enhance institutional cyber resilience over time, some of which are bolded in earlier sections, there are three key areas where the federal government as a whole should prioritize its efforts:

- The federal government should treat cyber security as an exercise in risk management, not risk elimination, and develop and prioritize response plans accordingly.

- The federal government needs to urgently invest time and energy into developing a fully staffed and more diverse cyber workforce at the federal level and promote initiatives that will also help develop the private sector cyber workforce given the nature of today's cyber incidents.
- The federal government should be prepared to tie planning to consequence analysis and involve non-IT professionals in the planning and exercises.

Conclusion

The ability to adapt is crucial as the nation moves into an uncertain future where extreme weather, increasingly sophisticated cyberattacks, and unexpected crises (such as a global pandemic) threaten to disrupt resources critical to daily functioning. Resilience is key, and the federal government has an essential role in concretely defining and growing resilience domestically and abroad.

As this report outlines, there are steps the federal government can and should take to be more resilient in its processes and promote societal resilience. This requires visibility into potential threats, sufficient planning to address possible disruptions and cascading consequences, consistent investments in people and DEI, and established definitions and metrics to understand resilience and measure progress overtime. Resilience requires up-front investments but will save time, dollars, and lives not if, but when, an unexpected shock occurs.

The federal government has taken promising steps to acknowledge the need for resilience over the myth of "risk elimination" and to more intentionally cultivate resilience. The challenge for the next few years will be to assess how quickly these plans can be implemented, how concretely they can be evaluated, how flexibly they can be adapted, and how consistently they can be prioritized over time.

This report analyzes resilience in four key areas, but the thread that is pulled through these topics is applicable across nearly all the challenges. The ability to assess what is most vital and how best to build in the capacity to bend but not break, to prevent disruptions from becoming catastrophes, to respond and recover with the confidence and strength that provides room for innovation, these are the keys to resilience that can allow an entity, a society, and a nation to—borrowing from William Faulkner—not merely endure but to prevail.

About the Authors and Advisers

WORKFORCE RESILIENCE:

- Hadeil Ali (Author), Director, CSIS Diversity and Leadership in International Affairs Project
- Naz Subah (Author), Program Coordinator, CSIS Diversity and Leadership in International Affairs Project
- Nicole Breland Aandahl (Adviser), Senior Vice President for People and Culture, CSIS

CLIMATE RESILIENCE:

- Morgan Higman (Author), former fellow, CSIS Energy Security and Climate Change Program
- Joseph Majkut (Author), Director, CSIS Energy Security and Climate Change Program
- Ian Barlow (Contributor), Senior Program Manager, CSIS Energy Security and Climate Change Program

SUPPLY CHAIN RESILIENCE:

- Emily Harding (Author), Deputy Director, CSIS International Security Program
- Harshana Ghoorhoo (Author), Research Assistant, CSIS International Security Program
- Bob Kolasky (Adviser), Senior Associate, CSIS International Security Program

CYBER RESILIENCE:

- Suzanne Spaulding (Author), Senior Adviser for Homeland Security, CSIS International Security
- Devi Nair (Author), Associate Director and Associate Fellow, CSIS International Security Program
- Sophia Barkoff (Author), Former Intern, CSIS International Security Program
- Bob Kolasky (Adviser), Senior Associate, CSIS International Security Program
- Jim Lewis (Adviser), Senior Vice President and Director, CSIS Strategic Technologies Program
- Jake Harrington (Adviser), Former Intelligence Fellow, CSIS International Security Program

Endnotes

1 Hadeil Ali and Naz Subah, "DEI Is Foundational to Workforce Resilience," June 1, 2022, https://www.csis.org/analysis/dei-foundational-workforce-resilience.

2 Yuval Shmul, Martin Reeves, and Simon Levin, "Building a Mutually Reinforcing System of Organizational and Personal Resilience," BCG Henderson Institute, March 8, 2022, building-organizational-personal-resilience-reinforcing-system.pdf (mkt-bcg-com-public-pdfs.s3.amazonaws.com).

3 Mary Hayes, Frances Chumney, and Marcus Buckingham, *Workplace Resilience Study: Full Research Report* (ADP Research Institute, September 2020), https://www.adpri.org/wp-content/uploads/2020/09/R0120_0920_v1FINAL_RS_ResearchReport_040621.pdf.

4 Punit Renjen, "Building the resilient organization," Deloitte, January 25, 2021, https://www2.deloitte.com/xe/en/insights/topics/strategy/characteristics-resilient-organizations.html.

5 Fritz Nauck, Luca Pancaldi, Thomas Poppensieker, and Olivia White, "Strengthening institutional resilience has never been more important," McKinsey, May 17, 2021, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-resilience-imperative-succeeding-in-uncertain-times.

6 Amy Edmondson, "Psychological Safety and Learning Behavior in Work Teams," *Administrative Science Quarterly* 4, no. 2 (June 1999), https://www.jstor.org/stable/2666999.

7 Marcus Buckingham, "The Top 10 Findings Resilience and Engagement," MIT Sloan Management Review, March 1, 2021, https://sloanreview.mit.edu/article/the-top-10-findings-on-resilience-and-engagement/.

8 "Psychological Safety," Gartner, n.d., https://www.gartner.com/en/human-resources/glossary/psychological-safety.

9 Laura Delizonna, "High-Performing Teams Need Psychological Safety: Here's How to Create It," Harvard Business Review, August 24, 2017, https://hbr.org/2017/08/high-performing-teams-need-psychological-safety-heres-how-to-create-it.

10 Deloitte, *The Equity Imperative* (London: February 2021), https://www2.deloitte.com/us/en/pages/about-deloitte/articles/the-equity-imperative.html.

11 Delizonna, "High-Performing Teams Need Psychological Safety."

12 Jeff Schwartz, Brad Denny, and David Mallon, "Belonging: From Comfort to Connection to Contribution," Deloitte, May 15, 2020, https://www2.deloitte.com/us/en/insights/focus/human-capital-trends/2020/creating-a-culture-of-belonging.html.

13 Colleen Bordeaux, Betsy Grace, and Naina Sabherwal, "Elevating the Workforce Experience: The Belonging Relationship," Deloitte, November 23, 2021, https://www2.deloitte.com/us/en/blog/human-capital-blog/2021/what-is-belonging-in-the-workplace.html.

14 Curt Harris, "'Diversity of Thought' Hinders Belonging," NALA, n.d., https://nala.org/diversity-of-thought-hinders-belonging/2022.

15 Victoria DiSimone, Deborah Ann McCarthy, and Sandra A. Rivera, *Leveraging Diversity for Global Leadership* (Washington, DC: CSIS, May 2018), https://www.csis.org/analysis/leveraging-diversity-global-leadership.

16 Elka Torpey, "Millennials in the labor force, projected 2019–29," *Career Outlook*, U.S. Bureau of Labor Statistics, November 2020, https://www.bls.gov/careeroutlook/2020/data-on-display/millennials-in-labor-force.htm.

17 Lauren Romansky et al., "How to Measure Inclusion in the Workplace," Harvard Business Review, May 27, 2021, https://hbr.org/2021/05/how-to-measure-inclusion-in-the-workplace.

18 Jackie Wiles and Jordan Turner, "3 Ways to Build a Sense of Belonging in the Workplace," Gartner, April 29, 2022, https://www.gartner.com/smarterwithgartner/build-a-sense-of-belonging-in-the-workplace.

19 Audrey Hametner, "How to Create Belonging in the Workplace without Undermining Diversity," Forbes, November 19, 2021, https://www.forbes.com/sites/ellevate/2021/11/19/how-to-create-belonging-in-the-workplace-without-undermining-diversity/.

20 Cecelia Herbert, "Belonging at Work: The Top Driver of Employee Engagement," Qualtrics, December 9, 2020, https://www.qualtrics.com/blog/belonging-at-work/.

21 Jim Harter, "U.S. Employee Engagement Reverts Back to Pre-COVID-19 Levels," Gallup, October 16, 2020, https://www.gallup.com/workplace/321965/employee-engagement-reverts-back-pre-covid-levels.aspx.

22 Scott Goodson, Ali Demos, and Charles Dhanaraj, "Shift Your Organization from Panic to Purpose," Harvard Business Review, April 27, 2020, https://hbr.org/2020/04/shift-your-organization-from-panic-to-purpose.

23 Ranjay Gulati, "The Great Resignation or the Great Rethink?," Harvard Business Review, March 22, 2022, https://hbr.org/2022/03/the-great-resignation-or-the-great-rethink.

24 Aaron De Smet et al., "'Great Attrition' or Great Attraction'? The Choice Is Yours," McKinsey, September 8, 2021, https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/great-attrition-or-great-attraction-the-choice-is-yours.

25 Deloitte, *A Call for Accountability and Action* (London: Deloitte, 2021), https://www.deloitte.com/content/dam/assets-shared/legacy/docs/insights/2022/2021-deloitte-global-millennial-survey-report.pdf; and Mark S. Bergman, Ariel Deckelbaum, and Brad S. Karp, "Introduction to ESG," Harvard Law School Forum on Corporate Governance, August 1, 2020, https://corpgov.law.harvard.edu/2020/08/01/introduction-to-esg/.

26 Katie Reid, "LinkedIn Data Shows Women and Gen Z Are More Likely to Apply to Remote Jobs," LinkedIn, January 25, 2021, https://www.linkedin.com/business/talent/blog/talent-strategy/women-gen-z-more-likely-to-apply-to-remote-jobs.

27 Frank Breitling et al., "6 Strategies to Boost Retention Through the Great Resignation," Harvard Business Review, November 15, 2021, https://hbr.org/2021/11/6-strategies-to-boost-retention-through-the-great-resignation.

28 Suzanne Spaulding and Devi Nair, "Restore Trust in National Security Institutions," CSIS, *Critical Questions*, January 22, 2021, https://www.csis.org/analysis/restore-trust-national-security-institutions; and Josh Felber, "Using Purpose to Motivate Long-term Productivity," Forbes, November 18, 2021, https://www.forbes.com/sites/forbesbusinesscouncil/2021/11/18/using-purpose-to-motivate-long-term-productivity/.

29 Dave Lievens, "How the Pandemic Exacerbated Burnout," Harvard Business Review, February 10, 2021, https://hbr.org/2021/02/how-the-pandemic-exacerbated-burnout.

30 Ben Wigert and Sangeeta Agrawal, "Employee Burnout, Part 1: The 5 Main Causes," Gallup, July 12, 2018, https://www.gallup.com/workplace/237059/employee-burnout-part-main-causes.aspx.

31 "Who Special Initiative for Mental Health," World Health Organization, n.d., https://www.who.int/initiatives/who-special-initiative-for-mental-health.

32 Ed O'Boyle, "4 Things Gen Z and Millenials Expect From Their Workplace," Gallup, March 30, 2021, https://www.gallup.com/workplace/336275/things-gen-millennials-expect-workplace.aspx.

33 "Employee Wellbeing Is Key for Workplace Productivity," Gallup, n.d., https://www.gallup.com/workplace/215924/well-being.aspx.

34 "Fact Sheet: President Biden Signs Executive Order Advancing Diversity, Equity, Inclusion, and Accessibility in the Federal Government," White House, June 25, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/25/fact-sheet-president-biden-signs-executive-order-advancing-diversity-equity-inclusion-and-accessibility-in-the-federal-government/.

35 Office of the Director of National Intelligence, *Annual Demographic Report* (Washington, DC: 2021), https://www.dni.gov/files/IC-DEI/AnnualReports/FY21_IC_Annual_Demographic_Report.pdf.

36 Morgan Higman, "The National Climate Strategy Needs a Resilience Focus," October 24, 2022, https://www.csis.org/analysis/dei-foundational-workforce-resilience.

37 "Understand Exposure," U.S. Climate Resilience Toolkit, July 28, 2022, https://toolkit.climate.gov/steps-to-resilience/understand-exposure.

38 Stephen Nalley and Angelina LaRose, "Annual Energy Outlook 2022," U.S. Energy Information Administration, March 3, 2022, https://www.eia.gov/outlooks/aeo/pdf/AEO2022_ReleasePresentation.pdf.

39 "U.S. Billion-Dollar Weather and Climate Disasters," NOAA National Centers for Environmental Information, n.d., https://www.ncei.noaa.gov/access/billions/; Craig Zamuda et al., "Energy Supply, Delivery, and Demand," in *Impacts, Risks, and Adaptation in the United States: Fourth National Climate Assessment, Volume II* (Washington, DC: U.S. Global Change Research Program, 2018), https://nca2018.globalchange.gov/downloads/NCA4_Ch04_Energy_Full.pdf; and Environmental Protection Agency, *Climate Change and Social Vulnerability in the United States* (Washington, DC: September 2021), https://www.epa.gov/system/files/documents/2021-09/climate-vulnerability_september-2021_508.pdf.

40 "By the Numbers: The Inflation Reduction Act," The White House, August 15, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/15/by-the-numbers-the-inflation-reduction-act/; and "Fact Sheet: The Bipartisan Infrastructure Deal," The White House, November 6, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/06/fact-sheet-the-bipartisan-infrastructure-deal/.

41 "The Inflation Reduction Act Drives Significant Emissions Reductions and Positions America to Reach our Climate Goals," U.S. Department of Energy, August 2022, https://www.energy.gov/sites/default/

files/2022-08/8.18%20InflationReductionAct_Factsheet_Final.pdf.

42 "EO 14008: Tackling the Climate Crisis at Home and Abroad (2021)," Office of NEPA Policy and Compliance, January 27, 2021, https://www.energy.gov/nepa/articles/eo-14008-tackling-climate-crisis-home-and-abroad-2021.

43 "Climate Resilient Infrastructure and Operations," Office of the Federal Chief Sustainability Officer, n.d., https://www.sustainability.gov/federalsustainabilityplan/resilience.html.

44 "DoD Climate Assessment Tool," U.S. Department of Defense, April 2021, https://media.defense.gov/2021/Apr/05/2002614579/-1/-1/0/DOD-CLIMATE-ASSESSMENT-TOOL.PDF.

45 "Discovering Our Future," IM3, n.d., https://im3.pnnl.gov/.

46 "Executive Order on Catalyzing Clean Energy Industries and Jobs Through Federal Sustainability," The White House, December 08, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/08/executive-order-on-catalyzing-clean-energy-industries-and-jobs-through-federal-sustainability/.

47 The White House, *Federal Sustainability Plan* (Washington, DC: White House, December 2021), https://www.sustainability.gov/pdfs/federal-sustainability-plan.pdf; and U.S. Office of Personnel Management, *Climate Action Plan* (Washington, DC: OPM, September 2021), https://www.sustainability.gov/pdfs/opm-2021-cap.pdf.

48 "Meet the Challenges of a Changing Climate," U.S. Climate Resilience Toolkit, n.d., https://toolkit.climate.gov/.

49 "Critical Infrastructure Sector Partnerships," CISA, n.d., https://www.cisa.gov/critical-infrastructure-sector-partnerships; and "Energy Sector: Council Charters and Membership," CISA, n.d., https://www.cisa.gov/energy-sector-council-charters-and-membership.

50 "Grid Resilience Planning and Resource Hub," Grid Deployment Office, 2022, https://www.energy.gov/gdo/grid-resilience-planning-and-resource-hub.

51 Morgan Higman, *Making Energy Resilient* (Washington, DC: CSIS, May 2022), https://www.csis.org/analysis/making-energy-resilient.

52 "Electric Reliability Historic Data," U.S. Energy Information Administration, November 29, 2017, https://www.eia.gov/electricity/data/eia411/eia411_history.php.

53 "Biden Administration Launches $2.3 Billion Program to Strengthen and Modernize America's Power Grid," Department of Energy, April 27, 2022, https://www.energy.gov/articles/biden-administration-launches-23-billion-program-strengthen-and-modernize-americas-power; and "Notice of Request for Information on Formula Grants to States and Indian Tribes for Preventing Outages and Enhancing the Resilience of the Electric Grid," *Federal Registrar* 87, no. 26191, 26191–26192, May 3, 2022, https://www.federalregister.gov/documents/2022/05/03/2022-09445/notice-of-request-for-information-on-formula-grants-to-states-and-indian-tribes-for-preventing.

54 U.S. Government Accountability Office, *Electricity Grid Resilience* (Washington, DC: March 2021), https://www.gao.gov/assets/gao-21-346.pdf.

55 U.S. General Services Administration, *Climate Change Risk Management Plan* (Washington, DC: September 2021), https://www.sustainability.gov/pdfs/gsa-2021-cap.pdf.

56 "REopt: Renewable Energy Integration & Optimization," National Renewable Energy Laboratory, n.d., https://reopt.nrel.gov/.

57 Ariel Castillo and Annie Weathers, "Energy Resilience Program and Assessment Tool," Energy Exchange, August 11, 2020, https://www.acq.osd.mil/eie/Downloads/IE/Defense%20Energy%20Resilience%20

Program%20and%20Assessment%20Tool_20200811.pdf.

58 Shalanda Young, Brenda Mallory, and Gina McCarthy, "The Path to Achieving Justice40," The White House, July 20, 2021, https://www.whitehouse.gov/omb/briefing-room/2021/07/20/the-path-to-achieving-justice40/; Anthony Leiserowitz and Karen Akerlof, "Race, Ethnicity, and Public Responses to Climate Change," Yale F&ES Project on Climate Change and George Mason University Center for Climate Change Communication, 2010, https://climatecommunication.yale.edu/wp-content/uploads/2016/02/2010_04_Race-Ethnicity-and-Public-Responses-to-Climate-Change.pdf; Boyeong Hong, Bartosz Bonczak, Arpit Gupta, and Constantine Kontokosta, "Measuring inequality in community resilience to natural disasters using large-scale mobility data," *Nature Communications* 12 (March 2021), https://www.nature.com/articles/s41467-021-22160-w; and James Elliott, "As Disaster Costs Rise, So Does Inequality," *Socius: Sociological Research for a Dynamic World*, December 4, 2018, doi:10.1177/2378023118816795.

59 Junia Howell and James R. Elliott, "Damages Done: The Longitudinal Impacts of Natural Hazards on Wealth Inequality in the United States," *Social Problems* 66, no. 3 (August 2018): 448–67, doi:10.1093/socpro/spy016.

60 "Explore the Map," Climate and Economic Justice Screening Tool, n.d., https://screeningtool.geoplatform.gov/en/#3.47/28.02/-89.3; and "Justice40," The White House, n.d., https://www.whitehouse.gov/environmentaljustice/justice40/.

61 "EJScreen: Environmental Justice Screening and Mapping Tool," U.S. Environmental Protection Agency, April 1, 2022, https://www.epa.gov/ejscreen; "Low-Income Energy Affordability Data Tool," U.S. Office of Energy Efficiency & Renewable Energy, n.d., https://www.energy.gov/eere/slsc/maps/lead-tool; and "The National Risk Index," FEMA, n.d., https://hazards.fema.gov/nri/.

62 "Low-Income Community Energy Solutions," U.S. Office of Energy Efficiency & Renewable Energy, n.d., https://www.energy.gov/eere/slsc/low-income-community-energy-solutions.

63 Natasha Prudent Malmin, "The Weight of Administrative Burden: The Distributive Consequences of Federal Disaster Assistance on Recovery after Hurricane Harvey," (PhD dissertation, Georgia State University and Georgia Institute of Technology, May 2021), https://smartech.gatech.edu/bitstream/handle/1853/66431/MALMIN-DISSERTATION-2021.pdf?sequence=1.

64 Changsoon Choi, Pam Berry, and Alison Smith, "The Climate Benefits, Co-Benefits, and Trade-offs of Green Infrastructure: A Systemic Literature Review," *Journal of Environmental Management* 291, no. 1 (August 2021), doi:10.1016/j.jenvman.2021.112583.

65 National Intelligence Council, *Climate Change and International Responses Increasing Challenges to US National Security Through 2040* (Washington, DC: Office of the Director of National Intelligence, October 2021), https://www.dni.gov/files/ODNI/documents/assessments/NIE_Climate_Change_and_National_Security.pdf.

66 "Fact Sheet: President Biden Announces New Initiatives at COP27 to Strengthen U.S. Leadership in Tackling Climate Change," White House, November 11, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/11/fact-sheet-president-biden-announces-new-initiatives-at-cop27-to-strengthen-u-s-leadership-in-tackling-climate-change/.

67 National Intelligence Council, *Climate Change and International Responses Increasing Challenges to US National Security Through 2040.*

68 Ibid.

69 "Fact Sheet: President Biden Announces New Initiatives at COP27 to Strengthen U.S. Leadership in Tackling Climate Change," White House.

70 Ibid.

71 Eric Roston and Brian Sullivan, "How Science Links Global Warming to Extreme Weather," *Washington Post*, July 19, 2022, https://www.washingtonpost.com/business/energy/how-science-links-global-warming-to-extreme-weather/2022/07/18/80b19e1a-06ca-11ed-80b6-43f2bfcc6662_story.html.

72 "Notice of Request for Information on Formula Grants to States and Indian Tribes for Preventing Outages and Enhancing the Resilience of the Electric Grid," *Federal Register*; and Jim Monke et al., "Inflation Reduction Act: Agriculture Conservation and Credit, Renewable Energy, and Forestry," Congressional Research Service, August 10, 2022, https://crsreports.congress.gov/product/pdf/IN/IN11978.

73 Emily Harding and Harshana Ghoorhoo, "Building Supply Chain Resilience," CSIS, *Commentary*, December 15, 2022, https://www.csis.org/analysis/building-supply-chain-resilience.

74 Michael R. Blood, "Biden plan to run LA port 24/7 to break backlog falls short," AP News, November 16, 2021, https://apnews.com/article/joe-biden-business-los-angeles-pete-buttigieg-a46b44e9efcd03f498ce0b4350 1b6637.

75 Ibid.

76 "Executive Order on America's Supply Chains," The White House, February 24, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/.

77 Yimou Lee, Norihiko Shirouzu, and David Lague, "T-Day: The Battle of Taiwan," Reuters Investigates, December 27, 2021, https://www.reuters.com/investigates/special-report/taiwan-china-chips/.

78 "Fact Sheet: Securing a Made in America Supply Chain for Critical Minerals," The White House, February 22, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/02/22/fact-sheet-securing-a-made-in-america-supply-chain-for-critical-minerals/.

79 Sabri Ben-Achour, "The U.S. is trying to reclaim its rare-earth mantle," Marketplace, April 30, 2021, https://www.marketplace.org/2021/04/30/the-u-s-is-trying-to-reclaim-its-rare-earth-mantle/.

80 Aaron Parrott, Brian Umbenhauer, and Lane Warshaw, "Digital Twins," Deloitte, January 25, 2020, https://www2.deloitte.com/us/en/insights/focus/tech-trends/2020/digital-twin-applications-bridging-the-physical-and-digital.html.

81 "Residents m=Map North St. Louis, Learn about Geospatial Intelligence at Community Mapathons," National Geospatial-Intelligence Agency, September 8, 2022, https://www.nga.mil/news/Residents_Map_North_St_Louis_Learn_About_Geospatia.html.

82 William Reinsch and Jack Caporal, *Preparing the Workforce for 2030* (Washington, DC: CSIS, October 2020), https://www.csis.org/analysis/preparing-workforce-2030-pillar-trade-leadership.

83 Kimberley Botwright and Felipe Bezamat, "Predictions 2022: Here's how supply chains might change according to business leaders," World Economic Forum, January 13, 2022, https://www.weforum.org/agenda/2022/01/supply-chains-2022-business-leaders-davos-agenda/.

84 Alexis Bateman, Ashley Barrington, and Katie Date, "Why You Need a Supplier-Diversity Program," Harvard Business Review, August 17, 2020, https://hbr.org/2020/08/why-you-need-a-supplier-diversity-program.

85 "EXIM Signs Memorandum of Understanding with Lithuania's Ministry of Economy and Innovation," Export-Import Bank of the United States, Press release, November 24, 2021, https://www.exim.gov/news/exim-signs-

memorandum-understanding-lithuanias-ministry-economy-and-innovation.

86 ManMohan S. Sodhi and Thomas Y. Choi, "In-Time Supply Chain, Revamp It," Harvard Business Review, October 20, 2022, https://hbr.org/2022/10/dont-abandon-your-just-in-time-supply-chain-revamp-it.

87 The White House, *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth* (Washington, DC: White House, June 2021), https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.

88 Suzanne Spaulding, Devi Nair, and Sophia Barkoff, "Investing in Federal Cyber Resilience," February 24, 2023, https://www.csis.org/analysis/investing-federal-cyber-resilience.

89 "Compromise of a Power Grid in Eastern Ukraine," Council on Foreign Relations, December 2015, https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine.

90 "Cyber resiliency," NIST, n.d., https://csrc.nist.gov/glossary/term/cyber_resiliency#:~:text=Definition(s)%3A,are%20enabled%20by%20cyber%20resources.

91 Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report* (Washington, DC: March 2020), https://www.solarium.gov/report.

92 Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report*, 37.

93 "Office of the National Cyber Director," The White House, n.d., https://www.whitehouse.gov/oncd/.

94 "Strengthening America's Cyber Resiliency: A Conversation with the National Cyber Director," Foundation for Defense of Democracies, June 10, 2022, https://www.fdd.org/events/2022/06/02/strengthening-americas-cyber-resiliency-a-conversation-with-the-national-cyber-director/#downloads.

95 Camille Stewart, "Office of the National Cyber Director Requests Your Insight and Expertise on Cyber Workforce, Training, and Education," The White House, October 3, 2022, https://www.whitehouse.gov/oncd/briefing-room/2022/10/03/office-of-the-national-cyber-director-requests-your-insight-and-expertise-on-cyber-workforce-training-and-education/; and U.S. Government Accountability Office, *Kick-Starting the Office of the National Cyber Director* (Washington, DC: 2022), https://www.gao.gov/assets/gao-22-105502.pdf.

96 "National Cybersecurity Strategy," White House, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

97 The White House, *National Security Strategy* (Washington, DC: October 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf; "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; and Suzanne Smalley, "White House Cyber Director Defends 'tough' national cybersecurity strategy ahead of release," Cyberscoop, October 17, 2022, https://www.cyberscoop.com/inglis-previews-national-cyber-strategy/.

98 "National Critical Functions," Cybersecurity & Infrastructure Security Agency, n.d., https://www.cisa.gov/national-critical-functions.

99 Ibid.

100 "Sector Risk Management Agencies," Cybersecurity & Infrastructure Security Agency, n.d., https://www.cisa.gov/sector-risk-management-agencies.

101 "NIST Risk Management Framework," NIST, n.d., https://csrc.nist.gov/Projects/risk-management/about-rmf.

102 Suzanne Spaulding and Mieke Eoyang, "Bad Idea: Creating a U.S. Department of Cybersecurity," Defense360,

CSIS, December 13, 2018, https://defense360.csis.org/bad-idea-creating-a-u-s-department-of-cybersecurity/.

103 U.S. Congress, House, *Consolidated Appropriations Act 2022*, H.R. 2471, 117th Cong., 2nd sess., Enrolled Bill March 12, 2022, https://www.govinfo.gov/app/details/BILLS-117hr2471enr.

104 U.S. Congress, House, *Department of Homeland Security Appropriations Act 2022*, H.R. 4431, 117th Cong., 1st sess., Reported in House July 15, 2021, https://www.govinfo.gov/app/details/BILLS-117hr4431rh.

105 "Division D—Energy and Water Development and Related Agencies Appropriations Act, 2022," U.S. House of Representatives Document Repository, https://docs.house.gov/billsthisweek/20220307/BILLS-117RCP35-JES-DIVISION-D.pdf#page=97.

106 Mark Montgomery, "Congress Invests in National Cyber Resilience but Misses Important Opportunities in the Consolidated Appropriations Act," Lawfare, April 1, 2022, https://www.lawfareblog.com/congress-invests-national-cyber-resilience-misses-important-opportunities-consolidated.

107 Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report*, 59.

108 "National Cybersecurity Strategy," White House.

109 Emily Harding et al., "Never Trust, Always Verify": Federal Migration to ZTA and Endpoint Security," CSIS, *CSIS Briefs*, June 16, 2022, https://www.csis.org/analysis/never-trust-always-verify-federal-migration-zta-and-endpoint-security; and "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

110 "Boom" is at best an imperfect metaphor for the impact of malicious cyber activity. Consulted experts noted the need to broaden our conception of "boom" in this context, and perhaps lower the threshold for what constitutes a "boom."

111 "National Cybersecurity Strategy," White House.

112 "Critical Infrastructure Sector Partners," Cybersecurity and Infrastructure Security Agency, n.d., https://www.cisa.gov/critical-infrastructure-sector-partnerships.

113 U.S. Congress, House, *Consolidated Appropriations Act 2022*, H.R. 2471, 117th Cong., 2nd sess., Enrolled Bill March 12, 2022, https://www.govinfo.gov/app/details/BILLS-117hr2471enr.

114 "Joint Cyber Defense Collaborative," Cybersecurity & Infrastructure Security Agency, n.d., https://www.cisa.gov/jcdc.

115 Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report*, 101.

116 "Exercises," FS-ISAC, n.d., https://www.fsisac.com/hubfs/Resources/FS-ISAC_ExercisesOverview.pdf.

117 "GridEx," North American Electric Reliability Corporation, n.d., https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx; and "Cyber Storm: Security Cyber Space," Cybersecurity & Infrastructure Security Agency, n.d., https://www.cisa.gov/cyber-storm-securing-cyber-space.

118 "Shields Up," Cybersecurity & Infrastructure Security Agency, n.d., https://www.cisa.gov/shields-up.

119 "Announcement of White House National Cyber Workforce and Education Summit," The White House, July 18, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/18/announcement-of-white-house-national-cyber-workforce-and-education-summit; and Federal Cyber Workforce Management and Coordinating Working Group, *State of the Federal Cyber Workforce* (Washington, DC: Cybersecurity & Infrastructure Security Agency, 2022), 6, https://www.cisa.gov/sites/default/files/publications/State_of_the_Federal_Cyber_Workforce_Report_09.14.2022.pdf.

120 The Aspen Institute, *Diversity, Equity, and Inclusion in Cybersecurity* (Washington, DC: Aspen Institute, September 2021), 5, https://www.aspeninstitute.org/wp-content/uploads/2021/09/Diversity-Equity-and-Inclusion-in-Cybersecurity_9.921.pdf.

121 Lindsey Sheppard, Morgan Dwyer, Melissa Dalton, and Angelina Hidalgo, "To Compete, Invest in People: Retaining the U.S. Defense Enterprise's Technical Workforce," CSIS, *CSIS Briefs*, November 23, 2020, https://www.csis.org/analysis/compete-invest-people-retaining-us-defense-enterprises-technical-workforce.

122 "Civics," The Center for Strategic and International Studies, https://www.csis.org/programs/international-security-program/defending-democratic-institutions/civics.

COVER PHOTO GERARDO MORA/GETTY IMAGES

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**