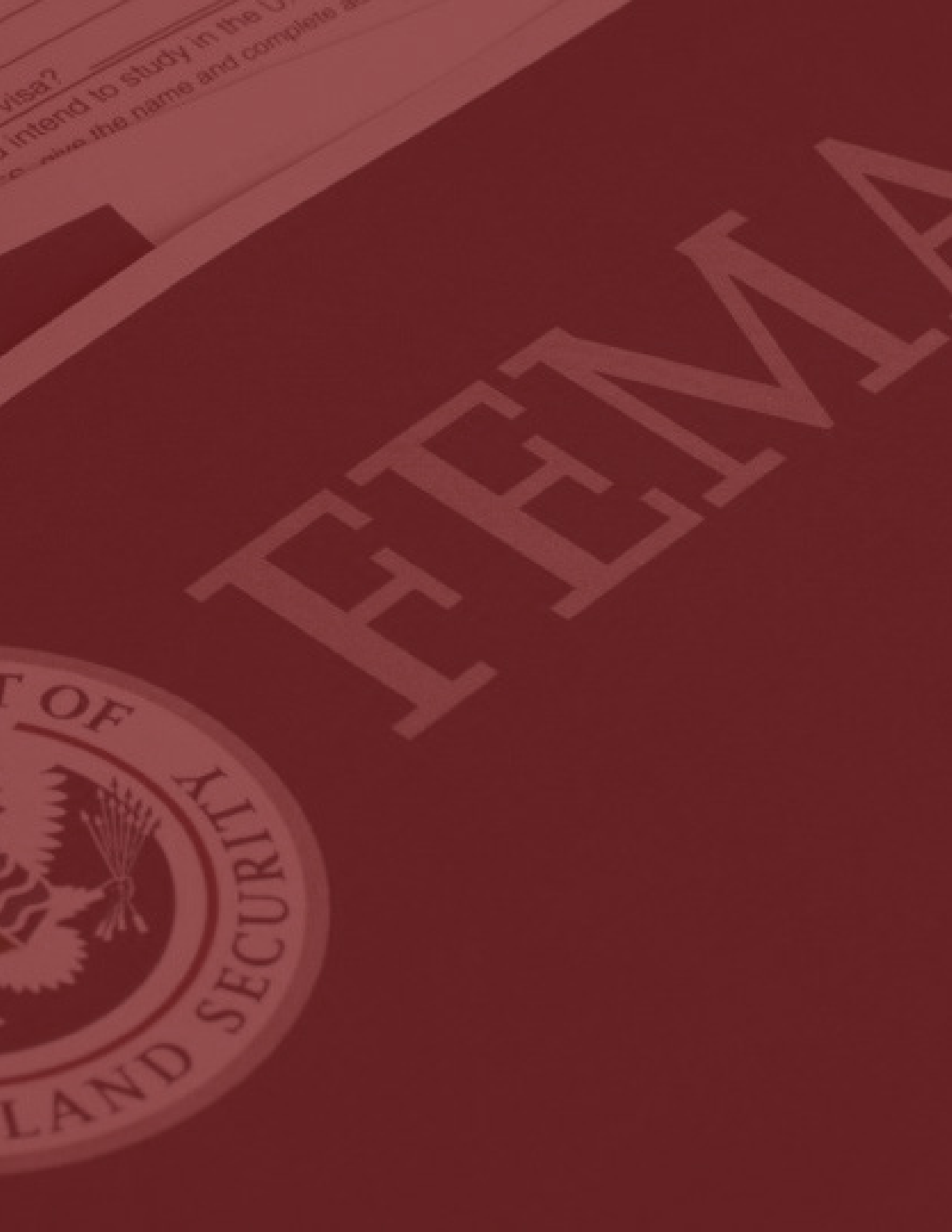
Findings and Recommendations of the BENS

Commission on the National Response Enterprise:

A CALL TO ACTION


visa?
intend to study in the U
the name and complete a
FEMA
OF
SECURITY
LAND

INTRODUCTION

This report presents a **"Call to Action"** for the 117th Congress and the Executive Branch to strengthen U.S. emergency response for sustained, widespread events such as the COVID-19 pandemic, which, as of this writing, has afflicted almost 11.6 million people in the United States and claimed more than 250,000 lives. Immediate, bold steps are urgently required to build trust and confidence with state and local governments and private and civil sector partners and create an effective, unified approach that meets the American people's needs.

Business Executives for National Security (BENS) established the Commission on the National Response Enterprise in July 2020. Our goal was to strengthen the country's resiliency through enhanced coordination, cooperation, and communication between all levels of government, business, and civil society. Thirty-three Commissioners and 58 executives from across these sectors researched and analyzed the many facets of an effective national response, arriving at three significant findings and 11 specific recommendations.

While the components of an integrated national response capability are largely in place, execution challenges remain, particularly when a crisis impacts numerous states simultaneously and extends over a prolonged period, as has been the case with COVID-19. Now is the time to reimagine and enhance components of the National Response Framework to address the challenges and embrace the opportunities of the 21st Century and to truly achieve the "Whole Community" approach to emergency response that it envisions.

First, explicit coordination and communication channels must exist and be well-known to all stakeholders. Second, a transparent and shared operating picture must be developed for the right resources to get to the right place at the right time. And third, we must maximize the use of existing and emerging technologies -- including by connecting every American to broadband – to power an effective emergency response.

These fundamentals are necessary, but alone will not be sufficient. More consistent and extensive exercising of all components of the National Response Framework and incident-specific response plans are indispensable, too. Not only will testing enable quick action and smooth operations when crises strike, but it will also foster relationships and trust among stakeholders across all sectors, which is foundational to working together successfully.

In the coming weeks and months, the Commission looks forward to working through BENS to engage Congressional and Executive Branch partners in determining the best ways to implement these recommendations for the American people.

COMMISSIONERS

Mark J. Gerencser
Commission Co-Chair
Author and Former Managing Partner
Booz Allen Hamilton

Alex Gorsky
Commission Co-Chair
Chairman & CEO
Johnson & Johnson

The Honorable Jeh C. Johnson
Commission Co-Chair
Former Secretary
Department of Homeland Security

ADM Thad Allen, USCG (ret.)
Former Commandant
US Coast Guard

Barbara Bennett
Former President & COO,
Vulcan, Inc.

Edward D. Breen
Executive Chairman & CEO, DuPont, Inc.

Calvin G. Butler
CEO, Exelon Utilities

Teresa Carlson
Vice President, Worldwide Public Sector,
Amazon Web Services

Senator William M. Cassidy, MD (R-LA)

Thomas J. Donohue
Chief Executive Officer, US Chamber of Commerce

Richard D. Fairbank
Founder, Chairman & CEO,
Capital One Financial Corp.

William J. Flynn
President & CEO, Amtrak

The Honorable Craig Fugate
Former Administrator,
Federal Emergency Management Agency

Joanna Geraghty
President & COO,
JetBlue Airways

General Frank J. Grass, USA (ret.)
Former Chief, National Guard Bureau

Senator Margaret Hassan (D-NH)

Rod Hochman, MD
President and CEO, Providence St. Joseph Health, Chair-Elect, American Hospital Association

Governor Larry Hogan (R-MD)
Immediate Past Chairman,
National Governors Association

General Charles H. Jacoby, Jr., USA (ret.)
Former Commander, US Northern Command

Ambassador Stuart E. Jones
President, Regions & Corporate Relations,
Bechtel Corp.

Juliette Kayyem
Faculty Chair, Homeland Security Program, Harvard Kennedy School of Government; former Assistant Secretary for Intergovernmental Affairs,
US Department of Homeland Security

VADM Joseph Maguire, USN (ret.)
Former Director, National Counterterrorism Center; Former Acting Director of National Intelligence

GEN Stanley A. McChrystal, USA (ret.)
Co-Founder, McChrystal Group LLC

Brian T. Moynihan
Chairman & CEO, Bank of America

RADM Joseph L. Nimmich, USCG (ret.)
Former Commander, First Coast Guard District
Former Deputy Administrator, FEMA

The Honorable David Paulison
Former Director, Federal Emergency Management Agency

Charles H. Robbins
Chairman and CEO, Cisco

William R. Roberts
Regional President (Ret.), Verizon

Kristi M. Rogers
Managing Partner, Principal to Principal LLC

Dr. Paul M. Romer
Nobel Laureate - Economics, 2018
Professor, New York University Stern School of Business

Virginia M. Rometty
Former Executive Chairman, IBM

Frances F. Townsend
Former Assistant to the President for Homeland Security and Counterterrorism

General Joseph L. Votel, USA (ret.)
President & CEO,
Business Executives for National Security
Ex Officio

TABLE OF CONTENTS

EXECUTIVE SUMMARY

A Call to Action for Creating a Coordinated National Response to All Crises

When the President of the United States takes the oath of office on January 20, 2021, Americans will mark one year to the day since the first confirmed diagnosis of COVID-19 inside U.S. borders.

The country's collective experience since the pandemic began underscores the indispensability of superior crisis-response capabilities to our national and economic security. The effort to manage COVID-19 has also demonstrated the complex nature of U.S. emergency response, from the interwoven responsibilities of federal, state, and local governments to the critical role of individual citizens in its success. Even as the battle continues to defeat this deadly virus and recover from its devastating impacts, national leaders are already shifting to rebounding and adapting response capabilities before the next natural- or human-made threat strikes.

The prolonged duration of the COVID-19 pandemic, combined with its damaging effects on every facet of life nationwide, continue to pressure-test the U.S. National Response Framework (NRF) in ways not experienced since the Framework's 2008 implementation. There are countless examples of how the NRF effectively enabled integrated response capabilities and the delivery of medical care, financial resources, food and water, and other assistance to those in need. But there are also numerous reports of challenges and gaps in systems and operations that impeded surge and supply chains for critical goods and services and prevented the "Whole Community" involvement envisioned in both the NRF and the National Preparedness Goal: "A secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."

Business Executives for National Security (BENS) initiated the Commission on the National Response Enterprise (the Commission) in July 2020 to determine where opportunities exist to strengthen and adapt U.S. plans, processes, and structures to respond

to future crises. Over 90 days, the Commissioners and 58 additional business leaders interviewed 165 government, private sector, and civil society stakeholders and researched five critical components of emergency response: Roles, Surge, Supplies, People, and Infrastructure & Economy.

The Commission concluded that the components of an integrated national response capability are essentially in place. However, significant execution challenges remain, particularly when a crisis impacts numerous states simultaneously, with limited time to acquire and pre-position needed supplies and other resources. To truly achieve a "Whole Community" approach to emergency preparedness and response, we must reimagine and redesign our capabilities to reflect and embrace 21st Century realities.

The Federal government must lead in defining and establishing clear lines of communication and coordination during crises; creating state-of-the-art command centers for national emergency response and surge and supply efforts; and better leveraging technology, data and analytics to power response. As appropriate, it should encourage replication of these recommendations, as well as other best practices, at the state and local levels.

These actions, combined with continuous exercising of all components of the NRF and incident-specific response plans, will facilitate decision-making and unity of effort across government, business, and civil sectors, based on real-time information and a clear common operating picture. Consistent, pervasive testing and exercising across the emergency response enterprise is essential not only to enable quick action and smooth operations when crises strike, but also to foster relationships and trust among stakeholders in all sectors.

Trust is a less tangible but foundational element of a fully functional emergency response enterprise. Citizens need to trust that their neighbors, communities, and governments will come to their aid when disaster strikes. Businesses need to trust that they can generously provide goods and services to the Nation without falling victim to frivolous lawsuits. States need to trust the Federal government's coordinating capabilities without fear of infringement on their rights and responsibilities. And everyone must have confidence in the safety of personal information, shared data, and the accuracy of real-time situational awareness, which drives decision-making across the enterprise.

The Federal government must lead the way to better define and establish clear lines of communication and coordination during crises.

While trust cannot be legislated or mandated, it emerges naturally from regular interaction, shared experiences, and personal relationship-building. Emergency response leaders and their teams should make every effort to continually build and deepen trusting relationships among all stakeholders within and across sectors and to establish confidence in plans, systems, and providers through continual testing and exercising.

COVID-19 has cost our country dearly, in lives lost and livelihoods shattered. We cannot change what has already occurred -- but, going forward, we can commit to do better. The upcoming inauguration of America's 46th President and convening of the 117th Congress present a meaningful opportunity for transformational thinking about emergency response strategy, policies, and processes. It is with that goal and imperative in mind that the BENS Commission on the National Response Enterprise offers the following three findings and 11 action-oriented recommendations. We hope this Call to Action can serve as a blueprint for policymakers, legislators, and other thought leaders as we strive, together, to elevate the United States' ability to prepare for and respond to future crises.

FINDINGS AND RECOMMENDATIONS

FINDING #1: Facilitating Communication and Coordination

Successful emergency response depends on a defined strategy; clear, tested roles and responsibilities; and shared visibility and strong relationships among all stakeholders.

Recommendation #1: Create transparent emergency response roles, strategy, and spending

Over time, the well-intentioned desire to prepare for every possible type of crisis has led to the creation of numerous national plans to respond to specific threats. This proliferation of plans, combined with their infrequent use and testing, can create confusion when new crises occur. The Commission recommends four actions to strengthen overall emergency management planning and clarify leadership and coordination of effort during disasters:

- **Amend the Stafford Act.** Congress should expand the Robert T. Stafford Disaster Relief and Emergency Assistance Act to include pandemics, cyber events, and other emergencies of extended duration or with possible nationwide impacts.
- **Eliminate confusion caused by the proliferation of existing response plans.** The President and other national leaders should reinforce the National Response Framework as the guiding document for all crises impacting the United States, with clear guidance that all incident-specific response plans must be drafted to be embedded within it.
- **Require biennial delivery of a National Emergency Response Strategy.** Every two years, the Secretary of Homeland Security should be required to submit a comprehensive national strategy for emergency management to the House Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs.
- **Establish expense-reporting authority for all emergency-related response spending by the federal government.** Congress should provide FEMA with the necessary powers to collect from other Federal entities the financial information needed to develop an aggregate spending total. FEMA should then be statutorily required to provide that accounting to Congress annually.

Recommendation #2: Strengthen Responder Relationships

Frequent interactions and trust between emergency response leaders at all government levels are essential components of a fully functioning national emergency response system. Strong relationships do exist today, but they are not ubiquitous. Steps to strengthen responder relationships include sharing best practices, creating a searchable, online inventory of nationwide crisis response roles (including current contact information for each position), and establishing a common lexicon. Congress should also require the creation of a standing mechanism to facilitate information exchange, coordination, and the delegation of responsibilities before, during, and after crises.

Recommendation #3: Link Responder Networks to Create a Common Operating Picture

The National Response Coordination Center (NRCC) within FEMA headquarters offers significant potential to develop a robust, resilient, interoperable data and communications network between all federal, state, and local emergency operations centers. Redesign of the NRCC should include, at a minimum, round-the-clock operations, 365 days a year. The aim should be to maximize unity of action between the government, business, and civil sectors when crises strike, and to enable access to real-time data and metrics for all stakeholders.

Recommendation #4: Expand Inclusion of Non-Traditional Partners

Trusted partnerships between the business sector, civil society organizations, and all government levels

are valuable force-multipliers for U.S. disaster resiliency and response. In recent years, both DHS and FEMA have meaningfully expanded outreach to the business community and non-profit organizations, but more must be done to develop these relationships, especially with companies and organizations not traditionally involved in emergency response. FEMA should strive to familiarize the private sector with its National Business Emergency Operations Center (NBEOC), Voluntary Agency Liaisons (VALs), and other resources, and raise awareness about their roles in emergency response so that non-traditional partners know how to engage. FEMA should also designate specific individuals or teams within the redesigned NRCC for businesses and civic organizations to contact with offers of assistance during crises; and should include the Chair of the National Council of ISACs (Information Sharing and Analysis Centers) in NRCC briefings and operations.

Recommendation #5: Prioritize the Exercising and Testing of Plans

The complexity of U.S. emergency response demands rigorous, ongoing testing to ensure that effective plans and core abilities will be available to respond to catastrophic events when they occur. Regular exercises of these capabilities have occurred in various forms since 2000, but COVID-19 highlighted weaknesses in FEMA's existing National Exercise Program. These include but are not limited to the exercises' low frequency, limited participant knowledge of the NRF and supporting crisis-specific response plans, and reported delegation of responsibility for exercise participation from senior leaders to subordinates. The Commission recommends creating or redesignating a leadership position within the Department of Homeland Security to oversee the development and operation of a comprehensive National Crisis Response Exercise Framework (NCREF) to more effectively coordinate testing and exercising of plans across the emergency response enterprise.

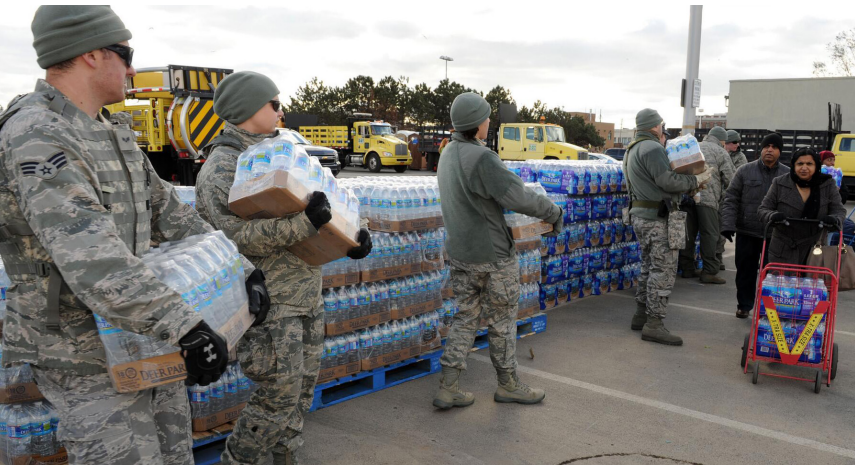
FINDING #2: Delivering Supplies and Volunteer Resources

Effective response efforts prioritize getting the right resources to the right place at the right time.

Recommendation #6: Maximize Surge and Supply Capabilities

Effective emergency response includes the ability to quickly surge critical goods, expertise, and personnel to a crisis zone while sustaining essential supply chains nationwide. The large number of states simultaneously impacted by COVID-19 put enormous pressure on these national capabilities, especially during the pandemic's early months. Several actions would significantly improve system-wide visibility of assets, facilitate coordination and planning, and ensure continuity of surge and supply operations:

- **Create a Surge Center within FEMA** that uses emerging technologies and telecommunications capabilities to deliver the situational awareness, secure the two-way information exchange, and share the data analytics needed across all sectors to drive accurate, real-time decision-making on surge response and industrial base resilience.
- **Develop a secure national disaster app** that offers voluntary access to features such as a map displaying current disaster and response activities, and AI-enabled predictive analytics showing future threat areas and actions needed.
- **Expand the use of flexible contracting options** for companies with emergency and non-emergency supplies at scale to create improved performance in surge and supply response operations. The expanded use of pre-defined and IDIQ (Indefinite Delivery/Indefinite Quantity) contracts are among the tools that merit consideration.
- **Enhance industrial base and stockpile resilience** through investment in cutting-edge data visualization tools and technologies like AI, machine learning, and blockchain to enable information sharing in real-time and inform rapid



decision-making. In combination with other tools such as shelf-life optimization, these technologies can assist in tracking surge and supply pipelines, support effective schedule replenishment, and promote first-in, first-out inventory management of the Strategic National Stockpile.

Recommendation #7: Harness All Available Skills and Support

Americans want to help their communities and country recover from crises, but numerous hurdles currently prevent willing and qualified volunteers from contributing to response efforts. Two forward-leaning actions would provide more appealing avenues of entry and address critical shortfalls in needed skills and expertise:

- **Build, launch, and train Civilian Expertise Reserves (CER)** modeled after the National Guard to recruit a highly trained, rapid-response force of professionals with targeted skill sets that could be activated for service in both state and federal crises. CERs would have State-based operations and a leadership hierarchy in each state, and national leadership based in Washington, D.C., that would assume command upon federalization.
- **Adapt and expand an existing online volunteer aggregator** and make it available to all emergency response stakeholders, to help them recruit and build a roster of ready volunteers. The federal government should not run this program. Instead, a non-profit or civil society organization currently operating a successful volunteer database or aggregator should be incentivized to adapt software, hardware, and existing tools to develop their capability for emergency response.

FINDING #3: Leveraging Technology

Integrated national response capabilities leverage new technologies and empower every American to take part.

Recommendation #8: Improve Abilities to Access, Use and Share Information

During crises, data in all forms, whether gathered and held by the government, private sector, or civil society, has the potential to help identify problems, prioritize resources, and develop plans for mitigation and resiliency. The COVID-19 pandemic revealed critical data challenges in the context of U.S. emergency response. For the Nation to be prepared and resilient, the federal government should move quickly to:

- **Develop a strategy, framework, secure capabilities, and computational resources** necessary to guide the sharing of timely and accurate data before and during times of national crisis.
- **Prioritize the acquisition and use of new technologies capable of engendering trust in the handling of personal data.** Possible options include secure watermarking, fingerprinting to assess revision history via open standards, and data lakes, among others.
- **Congress should explore creating targeted protections for organizations and businesses asked to share information and data with governments** during times of crisis as a possible way to build trust and address liability and regulatory concerns.

- **Pursue data standardization.** Data standardization is necessary for stakeholders to achieve the increased visibility and common operating picture envisioned in the redesign of the National Response Coordination Center and stand-up of a new FEMA Surge Center.
- **Promote trust in the mathematical models used in emergency response** (along with their supporting data). Congress should consider establishing non-partisan, public-private review boards to catalog, assess, and evaluate existing and developing models in preparation for use during future crises. Investment may be required to incentivize continual curation and analysis of such models and to ensure they are tamper resistant.

Recommendation #9: Connect Every American

The National Response Framework stipulates that every U.S. citizen is responsible for planning and responding to disasters, to the maximum extent possible, before other assistance will be made available. Yet more than 19 million Americans lack access to quality, high-speed internet at home, which undermines their ability to carry out this responsibility, putting them and others at risk. Investing in high-quality, national digital infrastructure capable of extending service to every household in the country is an economic, national security, and civic imperative. Every American must have guaranteed access to broadband.

Recommendation #10: Expand Access to the Benefits of Emerging Technologies

Artificial intelligence (AI), the Internet of Things (IoT), 5G, and blockchain technology are among the advanced technological tools already demonstrating value to emergency management in terms of enhanced capabilities, connectivity, and trust-building among stakeholders. Best practices should be shared throughout emergency response networks nationwide to expand awareness of the importance of investing in and deploying these technologies.

Recommendation #11: Keep Pace with Security and Technology Advances

COVID-19 placed unprecedented demand on state-level IT infrastructure and exposed its dangerous antiquation at all government levels. To bolster the resiliency and security of these systems and the Nation:

- **Congress should drive and incentivize efforts to migrate state and local legacy systems to new, secure platforms** capable of integration with other organizations across the NRF and in line with the IT modernization strategies offered by the Cybersecurity and Infrastructure Security Agency.
- **Congress should also vigorously drive and fund IT modernization by the federal agencies and departments that are part of the National Response Framework.** Congress should encourage and incentivize every NRF organization to pursue an individual modernization strategy that improves the efficiency, security, and resiliency of their own IT capabilities, while also requiring that those systems be capable of integrating with the systems of other emergency response entities. Achieving that goal will involve each organization taking advantage of cloud-based solutions to the maximum extent possible, other than in situations where mission-based needs may necessitate continued use of on-premises capabilities or legacy systems and architectures.
- **Government, private sector, and civil society entities should work toward employing a "Zero Trust" model for employees and their devices that require access to emergency response systems and data.** While advancing toward that goal, organizations should leverage the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which scales cyber risk management for ICT (Information and Communication Technology) products, services, and processes within five core function areas (identify, protect, detect, respond, and recover)

to improve their ability to prevent, detect, and respond to cyber attacks.

- **The Administration should develop and issue an updated National Cyber Strategy** that incorporates layered cyber deterrence, resilience, supply chain risk management for internet-connected devices, "Defend Forward" operations, and industry and international collaboration as critical pillars.
- **Governments at every level should seek to establish partnerships with companies that possess deep technology and cybersecurity expertise** to expand information sharing regarding new technologies, threats, and opportunities. NIST's National Cybersecurity Center of Excellence and DHS/CISA's Information and Communications Technology Supply Chain Risk Management Task Force illustrate the mutual value this type of cooperation affords. Adapting these models may make sense for interested states or regions as well.

The BENS Commission on the National Response Enterprise offers this blueprint for change to policymakers, legislators, and other thought leaders searching for substantive ways, in the wake of COVID-19, to elevate the Nation's ability to prepare for and respond to future crises in the United States. The following pages provide supporting explanations for each of our findings and action-oriented recommendations. Our goal is implementation, and through BENS, we will work to unify and engage all public sector, business, and civil society stakeholders in its pursuit.

SUPPORTING EXPLANATIONS

FINDING #1: Facilitating Communication and Coordination

Successful emergency response depends on a defined strategy; clear, tested roles and responsibilities; plus, shared visibility and strong relationships among all stakeholders.

Stakeholders across the national emergency response enterprise agree that the most effective approach to disaster response is locally executed, state managed, and federally supported. The federalist construct of the United States government aligns well with this approach, as it presents significant barriers to the central organization of a tightly coordinated, controlled response to major crises. Having communities take the lead, rather than play a support role, enables timely information sharing about conditions on the ground, facilitates prioritization, and leverages local knowledge to coordinate support from state and federal agencies.

Catastrophic disasters and crises impacting large numbers of states, potentially for extended periods, require enhanced federal government coordination to keep local and state governments from becoming overwhelmed. Such was the case with COVID-19. The pandemic brought to the fore numerous impediments to effective communication and coordination between local, state, and federal authorities, within critical departments and agencies of the federal government, and with the business community, non-profit organizations, and civil society.

These hurdles hindered surge and supply operations, compromised the speed necessary to control the virus's spread, and hampered the provision of essential medical assistance, with tragic life and death, health, and economic consequences for millions of Americans. The Commission recommends several actions to help avoid these dangerous obstacles in the future:

RECOMMENDATION #1: Create Transparent Emergency Response Roles, Strategy, and Spending

Established in March 2008, the National Response Framework (NRF) outlines how the United States should respond to all types of disasters and crises, ranging from significant local emergencies to catastrophic natural disasters impacting multiple states. It details the coordinating structures for delivering core capabilities required to respond to an incident, including various stakeholder roles and responsibilities, and provides a guide for executing a "Whole Community" approach to emergency planning and response.

"existing statutory authorities tasking HHS to lead the Federal government's response in a pandemic are insufficient and often in conflict with one another"

The NRF comprises a base document and 15 Emergency Support Function (ESF) annexes. ESFs are federal coordinating structures that group resources and capabilities into functional areas needed during a national response, such as transporation, communications, firefighting, and so on. One or more Federal Coordinating Officer(s) is specified for each of those support functions, with management oversight for that particular ESF and ongoing responsibilities throughout the preparedness, response, and recovery phases of incident management. There are currently 12 different federal departments or agencies designated as Coordinators or Co-Coordinators within the 15 categories.

The first confirmed case of COVID-19 in the United States was reported to the Centers for Disease Control on January 20, 2020; yet uncertainty among federal government agencies regarding jurisdiction, mobilization, authorities, and resources resulted in nearly 60 days of indecision and delay in federal response efforts. On March 13, 2020, President Donald Trump issued an emergency declaration establishing FEMA's lead role in coordinating federal support during the pandemic. The Department of Health and Human Services, the designated Coordinating Officer for ESF #8 (Public Health and Medical Services), moved into a support function.

This confusion had been foreseen. From January to August 2019, a joint exercise called the Crimson Contagion Functional Exercise tested the abilities of the federal government, 12 states, and several local governments, plus other public and private sector agencies, to respond to a severe influenza pandemic originating from China. The after-action report (AAR) released by the Office of the Assistant Secretary for Preparedness and Response (ASPR) of the Department of Health and Human Services concluded that "existing statutory authorities tasking HHS to lead the federal government's response in a pandemic are insufficient and often in conflict with one another." It further reported "confusion between HHS, FEMA, and the Department of Homeland Security on which federal agency would take the lead in the crisis," noting that "participants lacked clarity on federal interagency partners' roles and responsibilities during an influenza pandemic response."

The absence of pandemic-specific language within the Robert T. Stafford Disaster Relief and Emergency Assistance Act posed another obstacle. When state and local response capabilities are overwhelmed by a declared major disaster or emergency, the Stafford Act authorizes the federal government to provide aid in the form of technical, financial, logistical, and other assistance. Experts generally agree that a pandemic could trigger eligibility for the more limited emergency assistance available under the Act, but lack consensus around whether pandemics qualify for major disaster assistance.

To eliminate these critical weaknesses in the U.S. emergency response enterprise, the Commission recommends the following:

Amend the Stafford Act. Congress should amend the Robert T. Stafford Disaster Relief and Emergency Assistance Act to include pandemics, cyber events, and other emergencies of extended duration or with possible national impacts. These changes would enable effective and rapid deployment of assets and expertise in any national crisis, regardless of the event's nature or timeframe.

Eliminate confusion caused by the proliferation of existing response plans. The President and other national leaders should clearly and continuously reinforce that the National Response Framework is the guiding document for all crises impacting the United States. The NRF is the only construct with the capacity to bring together all stakeholders, and to create and sustain the unity of effort needed to respond to and recover from any crisis that impacts more than one state or a contained region, regardless of its nature.

That said, the NRF is a framework, not a plan. Specific incident response plans (like those for pandemics, oil spills, and tornados, for example) must be drafted to be embedded within the NRF, with triggers identifying necessary actions and those responsible for execution, including FEMA as overall coordinator. Of note, the Crimson Contagion AAR reported that HHS representatives in FEMA's National Response Coordination Center played a critical role in providing subject matter expertise and coordination support to meet the public health and medical mission, which serves as encouraging proof that this construct can work.

Require biennial delivery of a National Emergency Response Strategy. Every two years, the Secretary of Homeland Security should submit to the House Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs a comprehensive national strategy for emergency management. Required by statute and modeled loosely after the National Defense Strategy, this report would outline an approach consistent with any provisions of the President's most recent National Security Strategy relating to emergency preparedness,

response, and recovery. It would also address any relevant policy guidance, or any strategic homeland security guidance issued by the President or the Secretary of the Department of Homeland Security.

Establish expense reporting authority for all emergency-related response spending by the federal government. Currently, no federal department or agency can provide an accurate total of the dollars spent on emergency response in any given year. Without enterprise-wide visibility into that spending, Congress and the Administration cannot make informed decisions related to emergency management priorities or plans. Congress should provide FEMA with the necessary authorities to collect from other federal entities the necessary financial information to develop that aggregate spending total. FEMA should then be statutorily required to provide the accounting to Congress each year.

RECOMMENDATION #2: Strengthen Responder Relationships

Emergency response systems across the Nation's 50 states and four territories are anything but standardized, reflecting the varied anticipated needs of their own citizens and communities during a crisis. A well-functioning national emergency response system must proactively facilitate communication, develop relationships, and build trust among stakeholders. The Commission recommends two actions to drive ongoing collaboration:

FEMA should create a nationwide inventory of crisis response roles and responsibilities, providing visibility into state and federal emergency response organizations -- a level of awareness that does not currently exist. This inventory should include a searchable, state-by-state mapping of counterparts, with up-to-date, online availability of contact information for each position. Alongside this effort, the agency should create a common emergency-response lexicon. Such a lexicon would help overcome a challenge faced by federal, state, and local emergency responders during COVID-19, when varied terminology associated with the stockpiles caused significant inter-governmental confusion.

Congress should establish an Emergency Readiness, Action, and Communication System (ERACS) to manage the coordination, exchange, and delegation of responsibilities related to anticipated crises impacting the United States. Like the Department of Homeland Security's National Terrorism Advisory System, or the U.S. military's defense readiness condition (DEFCON), ERACS should create a voluntary but incentivized baseline of understanding regarding emergency response across all sectors. ERACS would detail categories and triggers for escalation from normal conditions to a crisis, and outline each sector's responsibilities and expected actions within each phase. Though operating at the federal level, the system would provide flexibility for other government levels, industry, and civil society to adjust readiness and act independently. As envisioned, ERACS could communicate needed information and expand situational awareness of stakeholder actions taken or those that need to be taken. It would operate uniformly across all sectors to instill trust and confidence in emergency response by all stakeholders in government, business and civil society.

RECOMMENDATION #3: Link Responder Networks to Create a Common Operating Picture

Shared awareness of fast-developing crisis metrics is indispensable to an informed, effective national response. Yet, stakeholders described struggling to gain a common operating picture during the COVID-19 response. Reported obstacles included minimal data sharing and the lack of an established method to submit requests for resources and track responses in real-time.

Compounding this problem, the national emergency response enterprise is characterized by a patchwork of antiquated, non-standard, and non-interoperable IT systems, further inhibiting coordination. Of note, the after-action report on the Crimson Contagion joint exercise expressly noted that HHS' and DHS/FEMA's use of disparate information management systems "hampered their ability to establish and maintain a national common operating picture." Developing interoperable systems, technologies, and capabilities to facilitate robust, resilient communication and data sharing between all federal, state, and local emergency operations centers will be critical to achieving this goal.

The Commission urges FEMA to reimagine and redesign its National Response Coordination Center to create and display this common operating picture, enable unity of action across sectors, and support round-the-clock operations every day of the year.

As a first step, joint federal and state working groups should convene and work together to identify critical crisis response data, data collection strategies, and an appropriate open architecture capable of facilitating information sharing and data collection, storage, integrity, access, and display. Data standardization will be necessary to enable these actions.

Once established, federal, state, and local fusion cells/centers and key private and civil society actors will need regular and reliable access to this platform

(in an appropriately permissioned way). They could then push and pull data as appropriate and connect and align actions, policies, and directives, while maintaining visibility into a dynamic environment. *(The upcoming section entitled "Leveraging Technology" discusses both topics in greater detail.)*

RECOMMENDATION #4: Expand Inclusion of Non-Traditional Partners

The National Response Framework explicitly identifies the private sector and nongovernmental and voluntary organizations as "essential partners" in responding to incidents. Embracing business and civic organizations as trusted partners rather than merely as vendors or providers of goods and services is essential to fully realize FEMA's "Whole Community" approach.

Over the past decade, both FEMA and the Department of Homeland Security have taken significant steps toward that goal and expanded outreach to business and non-profit organizations. For example, both now have Private Sector Offices, which act to ensure effective coordination and integration with key business and industry components and not-for-profit organizations engaged in emergency response and recovery. Through its Loaned Executive Program, DHS and its component agencies host corporate representatives and industry experts for 3- to 12-month rotations.

More recently, FEMA also launched the National Business Emergency Operation Center (NBEOC), a virtual organization that facilitates two-way information sharing between public and private sector stakeholders in preparing for, responding to, and recovering from disasters. Active partnerships between DHS, CISA, FEMA, and the U.S. Chamber of Commerce have also expanded outreach to and information exchange with the business community. These are all positive steps.

For obvious reasons, however, outreach efforts have been heavily focused in several sectors, including retail (especially big box and food and beverage), logistics, and critical infrastructure. Business leaders in other sectors have expressed interest in contributing resources for emergency response efforts but report uncertainty about whom to call with offers of supplies or services and how to find opportunities to assist.

Trusted partnerships between the business comunity sector, civil society organizations, and all government levels can be valuable force-multipliers for U.S. disaster resiliency and response. Continued and expanded investment in developing these relationships, especially with companies and organizations not traditionally involved in emergency response, is crucial. The Commission recommends several actions to continue the progress already made:

FEMA should designate specific individuals or teams within either the redesigned NRCC or proposed FEMA Surge Center that businesses and civic organizations can contact with offers of assistance during crises. This information would then be available in real-time for incorporation into response planning.

DHS and FEMA should expand relationships with civic organizations and businesses in sectors less familiar with emergency response (especially during periods between crises). These relationship development efforts should educate new partners about how they might be able to assist in future disaster planning and response; familiarize them with the NBEOC, FEMA Voluntary Agency Liaisons (VALs), and other resources; and provide contact information for the individuals within these offices and the redesigned NRCC or proposed FEMA Surge Center who can accept and coordinate offers of assistance.

FEMA should include the Chair of the National Council of ISACs (NCI) in briefings and operations in the National Response Coordination Center during emergencies and disasters. The National Council of Information Sharing and Analysis Centers reaches owners and operators of critical infrastructure across 26 key industry sectors. These sectors have designated NCI as their information sharing and operational arms regarding cyber and physical security threats and other hazards. Involving

the Council Chair would improve the two-way flow of timely, accurate information between emergency response leaders and hundreds of ISAC member companies, including those in the civil sector through the ISAC for Nongovernmental Organizations.

Federal departments and agencies should proactively share best practices in private sector engagement with state and local emergency response organizations, and vice versa, so they might be replicated or adapted at other levels. Whereas federal emergency response efforts benefit most from relationships with companies with a national footprint, state and local efforts can significantly benefit from relationship development efforts with regional and local suppliers.

There is no substitute for frequent, regular engagement in developing trusted public-private partnerships. Time and effort invested by federal, state, and local governments in developing these relationships with private and civil sector organizations and with one another will pay benefits in the ability to quickly and efficiently surge resources, collective experience, and capabilities to meet demand during any national crisis. Ongoing contact during the periods between crises is the only way to develop and sustain the foundation of trust needed to propel unity of action when disaster strikes.

RECOMMENDATION #5: Prioritize the Exercising and Testing of Plans

Comprehensive regional and national testing and exercising across all parts of the national response enterprise is essential to maximize operational effectiveness and adequately prepare the United States to respond to future crises. Regular exercises of these capabilities have occurred in various forms dating back to 2000, but COVID-19 highlighted weaknesses in FEMA's existing National Exercise Program. These include but are not limited to the exercises' low frequency, limited participant knowledge of the NRF and supporting crisis-specific response plans, and reported delegation of responsibility for exercise participation from senior leaders to subordinates.

The Commission recommends creating or redesignating a leadership position within the Department of Homeland Security to oversee the development and operation of a National Crisis Response Exercise Framework (NCREF). This leader would maintain constant visibility into tests and exercises occurring across the federal emergency response enterprise and make recommendations to the Secretary of Homeland Security regarding gaps or potential overlaps that require attention. The NCREF's design should ensure that high-risk regional and national threats are being tested against, along with coordination responsibilities and response activities across a broad range of agencies, private sector, and civil society stakeholders.

The leader would also seek to ensure that each test or exercise includes activities to build trusting relationships among participants. He or she should consider including media experts to help educate news producers about the emergency response enterprise, and to bolster relationships with outlets that can assist with communications during crises. The leader would also conduct an annual review of past lessons learned to avoid duplication of effort, analyze progress in addressing previously-identified weaknesses, and ensure that the national response enterprise is functioning optimally.

The Commission recommends that the NCREF include a robust modeling capability to stress-test the Nation's power and digital infrastructure against "Black Sky" hazards, catastrophic events that severely disrupt U.S. critical infrastructures' normal functioning in multiple regions over long durations. This capability would supplement the crisis-response-capabilities exercises that currently take place through DHS/CISA's national Cyber TTX series, including GridX (for the electric grid), Hamilton Series (for financial services), Cyber Storm (DHS) and Guard (NSA/USCYBERCOM). It would serve as a "digital twin" of modern industrial

society, replicating complex interdependencies and providing insight into the second- and third-order effects of threat events and response efforts. Whereas traditional planning paradigms identify potential risks, formulate scenarios, and generate static reports, a computer model would have the ability to dynamically test scenarios by identifying critical gaps and vulnerabilities and developing local, state, and federal responses. It would be continuously run, updated regularly, and extensively used for crisis planning and decision-making.

FINDING #2: Delivering Supplies and Volunteer Resources

Effective response efforts prioritize getting the right resources to the right place at the right time.

The large number of states simultaneously impacted by COVID-19 severely tested the United States' ability to surge and supply numerous critical goods and services, especially during the pandemic's early months. The crisis also raised numerous related questions about the resilience of the U.S. industrial base, the health of the Strategic National Stockpile, and whether or not the Nation could find and activate the massive number of doctors, nurses, and other health professionals needed to care for the sick and dying.

The Commission recommends multiple actions designed to improve total asset visibility; facilitate coordination, planning and, communication; and build trust across the emergency response enterprise's supply chain operations. We also propose mechanisms for identifying and recruiting willing volunteers from across the country, including those with the specialized skill sets and qualifications desperately needed during times of national crisis.

RECOMMENDATION #6: Maximize Surge and Supply Capabilities

Surge and supply operations share many requirements for success during national crises, including total asset visibility, effective planning, a common operating picture, well-defined communications channels, a well-exercised coordination mechanism, maximum continuity of operations across the enterprise, and best-in-class technical integration.

Recent crises, including the COVID-19 pandemic, have surfaced hurdles to successfully delivering each of these requirements. Reported challenges have included (but are not limited to) gaps in trust among disaster stakeholders, periodic shortfalls in DHS and FEMA staffing and funding, insufficient engagement of the business community in disaster surge and supply planning and operations, and a lack of incentives for stakeholder participation in testing, exercising and other resilience activities. Stakeholders also report that surge response is constrained by the absence of a surge-specific command and control center to drive decision-making and cross-sector activities.

The complexity of the surge and supply systems within the U.S. emergency response enterprise provides many possible entry points to improve their operations, efficiency, and effectiveness. The Commission has identified six for priority action:

Establish a FEMA Surge Center. Command and control for surge should reside within FEMA, coordinating with the Departments of Homeland Security, Defense, Treasury, Energy, Transportation, Health & Human Services, and others, as appropriate. IT capabilities within

each agency and department must be capable of integration to enable real-time communication; and need cloud-capabilities to facilitate data sharing, analytics, and guidelines. Creating a FEMA surge hub would maximize the efficiency of planning, communicating, and executing surge response and fortify industrial base resilience writ large.

Improved visibility into real-time data analytics will drive more effective response. Other technologies such as AI can also provide better situational awareness of supply and demand to drive decision-making in real-time. As the federal government invests in new IT capabilities and retires legacy systems, the ability to quickly communicate with private and civil sector stakeholders will improve significantly. With improved information sharing, relevant data will be visible across sectors, most notably around roles and responsibilities and current gaps and capabilities.

Develop a national disaster app. Building off of FEMA's supply chain control tower, a secure national disaster support application would offer access to features such as a comprehensive pre-contracted-stockpiles filtering capability, a current map showing disaster and response activities in play, schedules and sign-up capability for joint exercises, AI-enabled predictive analytics showing future threat areas, and access to pre-negotiated contracts and critical points of contact. Participation in this program would be entirely voluntary; however, willing stakeholders could only gain access by displaying their inventories, supply chain, and times to replenish. They would also agree to participate in regular and ongoing supplies-focused testing and exercise plans. Protecting the confidentiality of data (and privacy of any third-party owner of the information) shared by businesses who choose to participate will necessarily be of utmost priority. Existing examples of successful information sharing between the private and public sectors should be investigated and potentially replicated.

Enable more flexible contracting options for companies. The availability of pre-defined and IDIQ (Indefinite Delivery/Indefinite Quantity) federal contracts for companies with emergency and non-emergency supplies at scale would increase efficiencies and improve performance in surge and supply operations.

The Department of Defense has various existing pre-defined contracting mechanisms to rapidly surge people, supplies, and resources that could serve as models for FEMA's use. The Defense Logistics Agency, in particular, has a wide range of these contracts, which proved valuable during Hurricane Sandy response.

The expanded use of IDIQ contracts by emergency response agencies would deliver similar advantages. Rather than include any exchange of goods and services, these contracts denote an overall mission and definition of what materiel can surge quickly.

To encourage technological innovation, increase deployment speed and improve cost efficiency, the U.S. Army Corps of Engineers and FEMA should also create a database of best-in-class contractors, manufacturers, and service providers that can adapt to various crises. The response to COVID-19 revealed that to achieve this goal, a substantial investment of time and effort is needed across a wide range of services, with a specific need identified with regard to firms that specialize in private sector temporary facility installation, like field hospitals.

The speed and efficiency of contracting for surge operations would additionally benefit from developing stronger relationships between federal entities, local public health officials, and construction, disaster management, and sanitization companies, among others, as well as with universities, convention centers, and real estate managers, in advance of future crises. The Commission also recommends developing a list of guidelines and construction specifications, including post-completion maintenance requirements and mechanisms for storing and recycling portable structures and mechanical equipment.

Enhance industrial base and stockpile resilience. Private sector emphasis on just-in-time production and efficient market mechanisms constrains the ability to surge supplies during a crisis. While lean operations can be good for the bottom line, they can also result in bottlenecks and production/distribution delays in times of rapidly surging demand. A reluctance to invest in idle capacity or store excess inventory due to costs and shelf-life considerations has cascading, adverse effects on the U.S. industrial base, national stockpiles, and overall emergency response.

Weaknesses in supply- and demand-signaling on the local, state, and federal levels hamper private industry's ability to direct or re-tool production to fulfill demand, and also distorts civil society organizations' data on the ground, potentialy impacting the priority a community or region receives as the response unfolds. Without an integrated technical framework, alerts around the potential for surge and the mechanisms to trigger a surge response are delayed or delivered piecemeal.

Investing in and implementing technologies such as dashboards, AI, and blockchain can enable immediate information sharing to inform rapid decision-making, with room for critical adjustments as additional data is gathered. This allows governments to gain total asset visibility to inform the allocation of resources and help the private and civil society sectors prioritize production mechanisms and distribution before, during, and after a crisis. Continued development of DoD's and DHS predictive analytics programs, and improvements in the Strategic National Stockpile through investments in blockchain technology and shelf-life optimization, can help track surge and supply pipelines, supporting effective schedule replenishment and promoting first-in, first-out inventory management. Additional data collection and analysis around the Stockpile will also improve understanding of geographical reference points relative to regional capacity and delivery status, identify where needs are the greatest, and improve partnership with commercial markets.

RECOMMENDATION #7: Harness All Available Skills and Support

The dramatic increase in FEMA disaster declarations -- 93 in the first nine months of 2020, compared with full-year totals of 81 in 2010 and 45 in 2000 -- underscores the Nation's imperative to engage more Americans and a broader range of their critical skill sets in disaster recovery and emergency response.

As has been noted by The National Commission on Military, National, and Public Service and other organizations, substantial evidence exists that "...the desire of Americans to serve far exceeds their opportunity to do so. Among Americans there is a great demand for more opportunities to serve, more knowledge about existing opportunities, and fewer barriers to service." Reported barriers to service include lack of awareness of available positions, perceived burdensome time commitments required by existing formal volunteer models, as well as lack of job security and health benefits. Meeting the demand for talent and opportunity will require bold action to overcome these hurdles. The Commission offers two forward-leaning

Weaknesses in supply- and demand-signaling on the local, state, and federal levels hamper private industry's ability to direct or re-tool production to fulfill demand.

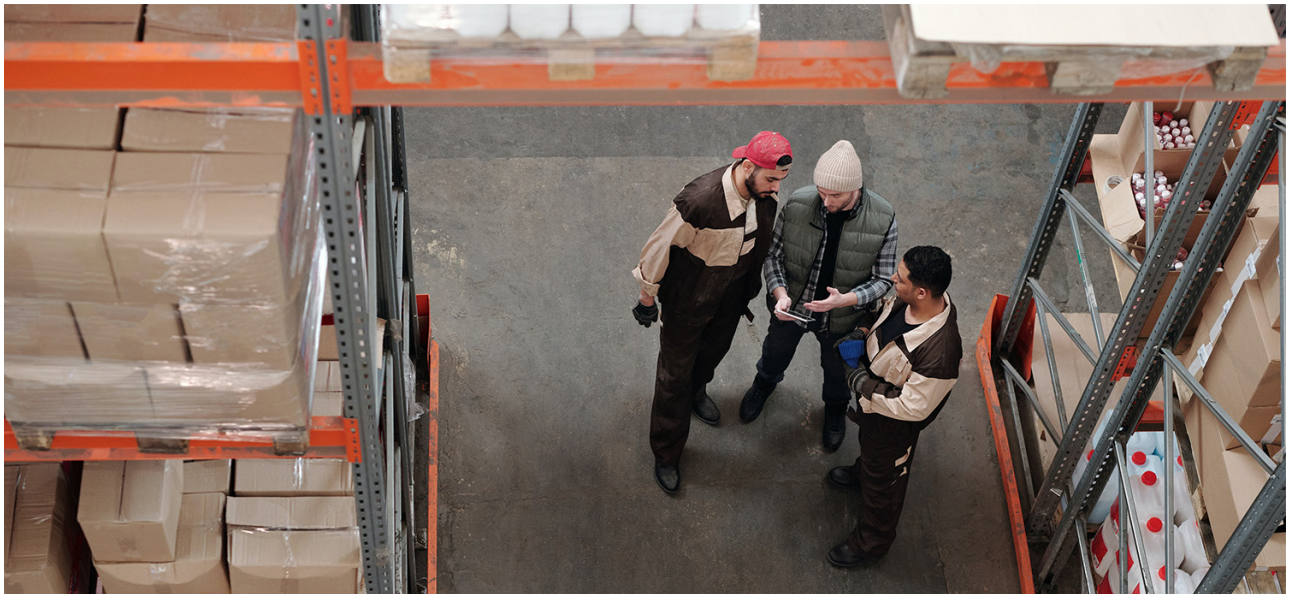
recommendations that, in combination, address shortfalls in skills and expertise and provide further avenues of entry for willing volunteers.

Build, launch, and train Civilian Expertise Reserves. The Commission believes that Civilian Expertise Reserves (CERs) provide the best way to recruit civilians with targeted skill sets to participate in standing organizations that can deploy when required. CERs would provide emergency managers with a highly trained, rapid-response force of professionals who can augment or supplement existing resources.

The National Guard provides a useful model for forming a CER and its operating authorities. As envisioned, the individual CERs could activate for service in both state and federal crises. Guard best practices for recruiting (such as tuition assistance and stipends), and employment protections (covered by the Uniformed Services Employment and Reemployment Rights Act) could apply to CERs as well. Similarly, aspects of FEMA's Disaster Reservist, Surge Capacity Force and Community Emergency Response Team (CERT) programs may offer useful insights on how to streamline time commitment requirements, recognizing that CERs will need to take into account training and skills already resident within certain professions. The National Guard's command and control structure may also present a model for designing the CER management and leadership systems. CERs would have state-based operations and a leadership hierarchy in each state, with national leadership based in Washington, D.C., which would assume command upon federalization.

Contemporary emergency response demands new kinds of skill and expertise, including advanced data analytics, cybersecurity, and information technology, which join more traditional specialized skill sets such as medicine, electrical engineering, and construction. The Commission recommends piloting two CER programs, directed at recruiting medical personnel and cybersecurity professionals. Insights, lessons learned, and best practices would inform the launch of additional CERs.

Adapt and expand an online volunteer aggregator. While CERs build capacity for special technical skills, an online marketplace aggregator could help identify and recruit other interested individuals and build a robust database of ready volunteers, potentially catalogued by specific credentials such as DHS CERT qualifications and prior diversity-and-inclusion training. The aggregator could also be used to share information about training and credentialing opportunities, guidance, policies, and regulations at the local, state, and federal levels. All emergency response stakeholders, from local mayors and small



businesses to federal agencies, would be able to call upon the aggregator for volunteer assistance.

The Commission opposes either creating a new entity to carry out the aggregator mission or assigning its management to a government organization or department. Several existing non-profit and civil society organizations already operate volunteer databases and aggregators, including the Red Cross, Network for Good, Volunteer Match, Americorps, SeniorCorps, Service Year Alliance. The wisest course of action would be to work with one or more of these organizations to see if existing software, hardware, and tools could be adapted to this end.

While the Civilian Expertise Reserves and volunteer aggregator are distinct proposals, similar funding and management models could apply. Both should include direct federal and state government support to the aggregator's host organization. The non-profit or civil society organization selected to host the aggregator would also be authorized to solicit financial contributions to cover overhead and personnel costs from individuals, businesses, foundations, and other sources, in the same ways they conduct fundraising for their other programs.

FINDING #3: Leveraging Technology

Integrated national response capabilities leverage new technologies and empower every American to take part.

Technology, data, and analytics hold the power to transform U.S. crisis response, as we are already beginning to see. Secure communications systems enable first responders to coordinate rescue missions. Relief agencies can crowdsource and share critical information in real time. At every level, governments are using data analytics to improve awareness of needs and delivery of services. There is boundless potential for new and emerging technologies to make U.S. emergency management systems, planning, and operations even smarter, more effective, and more secure -- and that potential remains largely untapped.

Meanwhile, the Federal Communications Commission reports that at least 19 million Americans lack access to quality, high-speed internet. Large gaps in broadband coverage persist, primarily in rural areas and tribal lands. Beyond the unequal access to opportunity this digital divide creates, lack of broadband coverage profoundly hinders response capabilities in the United States, and the resilience of national, state, and local economies and education systems during emergencies and natural disasters.

The Commission urges aggressive investment in and leveraging of technology, data, and analytics to maximize the effectiveness of U.S. emergency response systems, with four specific actions recommended:

RECOMMENDATION #8: Improve the Ability to Access, Use and Share Information and Data

Data in all forms, whether held by the government, private sector, or civil society, has the potential during crises to help identify problems, prioritize resources, and develop plans for mitigation and resiliency. The COVID-19 pandemic revealed critical data challenges in the context of emergency response. For the Nation to be prepared and resilient, the Federal government should move quickly to:

Prioritize the acquisition and use of technologies capable of engendering trust in the handling of personal data. Transparency and trust in the handling of personal data are foundational to driving

the advances described above. The government, private sector, and civil society organizations should prioritize the investigation and acquisition of strong technologies to that end, such as secure watermarking, fingerprinting to assess revision history via open standards, and data lakes.

Explore whether to create targeted protections for organizations and businesses asked to share information and data with governments during times of crisis as a possible way to build trust and address liability and regulatory concerns.

Pursue data standardization. Data standardization efforts are already underway in the federal government, and will be indispensable for FEMA to redesign its National Response Coordination Center and to stand up a new Surge Center. Congress should consider expanding or applying the DATA Act (Digital Accountability and Transparency Act of 2014) to include data relevant to disasters, mitigation, recovery, and resilience.

Now is the time for Congress to drive and invest in the modernization of federal, state, and local information technology systems and cybersecurity capabilities.

Promote trust in the mathematical models used in emergency response. Even as the response to COVID-19 has relied heavily on mathematical modeling and science, it has also demonstrated how, when groups of Americans distrust or disregard scientific experts, they can act in ways which put themselves and other citizens at risk, with potentially fatal consequences. To encourage citizens to accept and comply with emergency response leaders' directives during future crises, the federal health authorities will need to rebuild trust in and understanding of these models and the data which supports them.

Models are routinely used in risk management and response approaches to the broad range of natural and human-made hazards that could potentially impact the United States -- for example, to forecast the rates of transmission of infectious disease, anticipated wind speeds and water level elevation during hurricanes, or the expected dispersion spread of oil spills at sea. Advances in scientific research and mathematical formulations regarding various hazards can help improve the accuracy of related predictive models, which in turn will enable more effective emergency preparation and response planning.

A catalog of existing hazard and disaster-related scientific and mathematical models, including an evaluation of their accuracy, strengths, and weaknesses, would provide a baseline upon which to build public trust. The ability to track a model's evolution from generation to final point of use, and to demonstrate its tamper-resistance, will be critical as well. The federal government should consider establishing nonpartisan, public-private review boards to examine current models and those under development with the goal of creating such a catalog. Financial investment may be required to incentivize the constant curation and analysis of these models in the public and private sectors.

RECOMMENDATION #9: Connect Every American

Within the National Response Framework, every U.S. citizen is responsible for planning for and responding to disasters, to the maximum extent possible, before other assistance will be made available. Yet, for the 19 million Americans who lack quality, high-speed internet access in their homes, executing this mission is challenging if not impossible. The COVID-19 crisis put a spotlight on a sharp digital divide between rural and urban communities, low- and high-income families, small and big business, and government and private sectors. These divisions have hampered recovery and sustainment efforts throughout the country.

A resilient economy and an inclusive economy are two sides of the same coin. High-speed, low-latency broadband is no longer optional: Every American

must have guaranteed access to broadband. Investing in high-quality, national digital infrastructure capable of extending service to every household in the country is an economic, national security, and civic imperative.

RECOMMENDATION #10: Expand Access to the Benefits of Emerging Technologies

Artificial intelligence (AI), the Internet of Things (IoT), 5G technology, and blockchain are already demonstrating their ability to add enormous value to emergency management. Select examples include improved decision-making and planning through advanced data collection, transmission, and analysis; shortened response times through improved modeling and simulation capabilities; and more efficient resource distribution to areas impacted by a crisis, enabled by enhanced transparency and interoperability.

An equally critical, though less recognized, benefit of these technologies is their ability to create transparency and build trust among stakeholders throughout the response framework. For example, it's now possible to provide a permanent record that demonstrates what resources were committed to an area impacted by a crisis and by whom. All participants can access this record and submit entries, helping not only to eliminate inefficiencies and decrease opportunities for resource diversion and corruption, but also to build trust among stakeholders.

At a more macro level, increased reliance on technology to strengthen U.S. safety and security requires real trust in its value and capabilities on the part of emergency response professionals, policymakers, and citizens. Education will be vital to earn their trust and, even more importantly, to ensure that the Nation has a trained workforce capable of enabling and operating these technologies.

Examples of success and best practices in employing these technologies should be shared throughout emergency response networks nationwide to expand awareness about, investment in, and deployment of these capabilities.

RECOMMENDATION #11: Keep Pace with Security and Technology Advances

The cyberspace landscape continues to evolve and grow more complex; yet government at every level has drastically underinvested in critical needs for state-of-the-art security and infrastructure resilience -- as the rapid, forced shift of government, business, education, and healthcare services to virtual, remote operations during the COVID-19 crisis revealed.

For example, most states encountered significant challenges in their distribution of federal Pandemic Unemployment Compensation. Why? Because their unemployment systems relied on aging software run on COBOL, a legacy programming language outdated for decades.

At the same time, cyber threats have hit historic highs in the months since the pandemic began -- taking the form of a record-setting number Denial of Service (DOS) attacks, large-scale cyberattacks reported by twelve Governors on their states, a five-fold increase in phishing, and a sharp rise in ransomware attacks, often directed at the most vulnerable targets like municipalities and critical infrastructure.

Now is the time for Congress to drive and invest in the modernization of federal, state, and local information technology systems and cybersecurity capabilities. Both are integral to emergency response, economic recovery, and Americans' ability to work, attend school, and access government services through intense, prolonged national crises. The Commission makes two recommendations related to technology upgrades:

Congress should drive efforts to migrate state and local legacy systems to new, secure platforms capable of integration with the systems of other NRF organizations and in line with the IT modernization strategies offered by the Cybersecurity and Infrastructure Security Agency.

Congress should also vigorously drive and fund IT modernization by the federal agencies and departments that are part of the National Response Framework. The private sector now offers a differentiated set of IT capabilities at different system layers, making possible nearly any combination of components, whether managed by a vendor, the government entity, or both. Industries leading in technological innovation have also demonstrated that hybrid, multi-cloud environments are viable and often preferred options for managing government workloads as decentralized systems. Congress should encourage and incentivize every NRF organization to pursue an individual modernization strategy that improves the efficiency, security, and resiliency of their own IT capabilities, while also requiring that those systems be capable of integration with the systems of other emergency response organizations.

Achieving that goal will involve each organization taking advantage of cloud-based solutions to the maximum extent possible, other than in situations where mission-based needs may necessitate continued use of on-premises capabilities or legacy systems and architectures. Similarly, while the resiliency provided by the use of more than one commercial cloud vendor is optimal, flexibility should be maintained for agencies and departments to determine how many and which commercial cloud providers can best enable each to meet their own mission-specific requirements.

While upgrading government IT systems is necessary, it will be insufficient to advance national resilience and preparedness without an accompanying strengthening of cybersecurity systems, processes, and practices. This same holds true for the emerging technologies that are increasingly being used across the national security enterprise, as described in the preceding sections.

Expanded access to 5G networks will drive a massive increase in IoT devices -- currently projected to number more than 25 billion globally by 2021, and to grow to some 1,000,000 per square kilometer over the next decade. Internet-connected sensors, cameras, security monitors, and controllers modernize and increase systems' efficiency within power grids, public water supplies, transportation infrastructure, and emergency response systems. However, they also expose these systems to potential attacks by adversaries. As the use of these technologies increases, so will the Nation's network vulnerabilities.

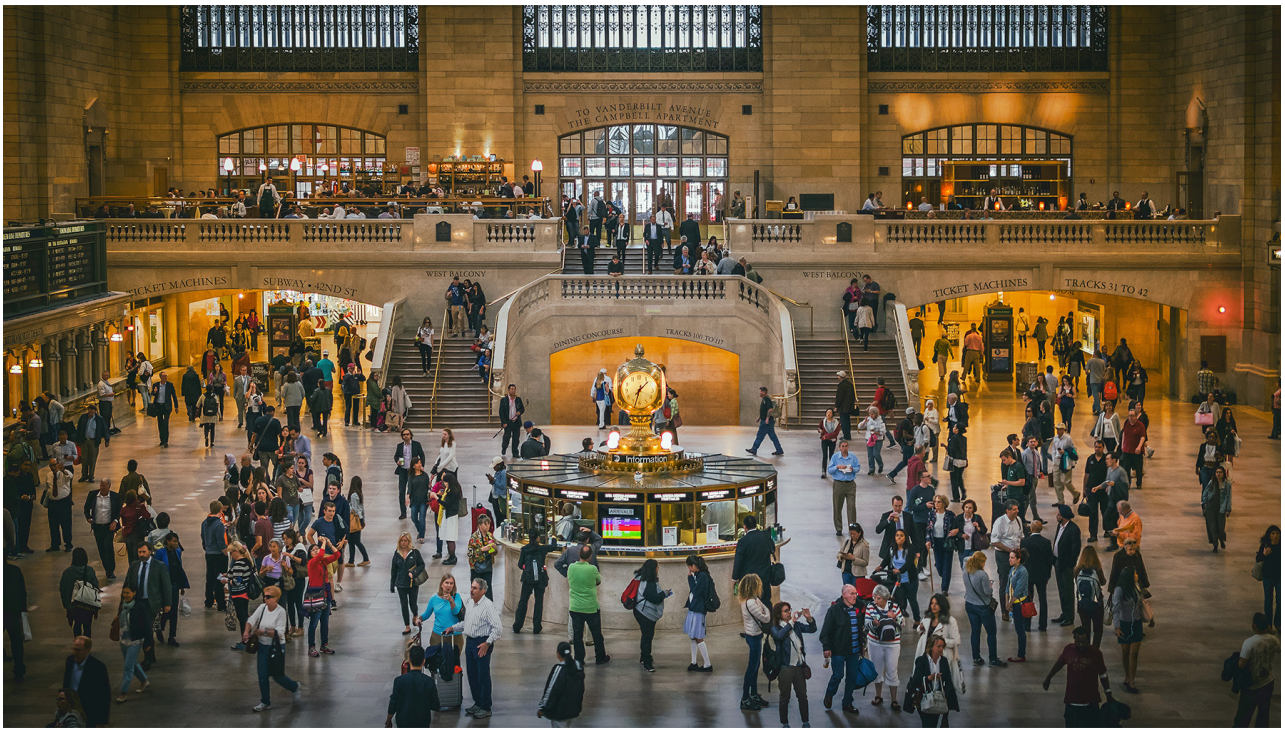
The Administration should develop and issue an updated National Cyber Strategy that incorporates layered cyber deterrence, risk management, resilience, and "Defend Forward" operations, as well as industry and international collaboration. Securing the IoT device supply chain will also be critical to protect against the exploitation of vulnerabilities inherent in all internet-connected devices. More than 30 supply chain studies are reportedly underway in the second half of 2020, under the auspices of organizations such as MITRE and the DHS Information and Communications Technology Supply Chain Risk Management Task Force. A great deal of analysis on this subject will become available to the incoming Administration and Congress, which can be used to inform this aspect of the Strategy's development.

Government, private sector, and civil society entities should work toward employing a "Zero Trust" model for employees and their devices that require access to emergency response systems and data. Zero Trust strives to protect modern digital environments and prevent successful data breaches by leveraging network segmentation, preventing lateral movement, and simplifying user-access control. Rooted in the principle of "never trust, always verify," it aims to eliminate the concept of trust from an organization's network architecture. While advancing toward this goal, organizations should leverage the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which scales cyber risk management for ICT (Information and Communication Technology) products, services, and processes within five core function areas -- identify, protect, detect, respond, and recover -- to improve organizational abilities to prevent, detect, and respond to cyber attacks.

Governments at every level should seek to establish partnerships with companies that possess deep technology and cybersecurity expertise to expand information sharing regarding new technologies, threats, security, and opportunities. The U.S. business community has extensive knowledge and expertise related to the constantly escalating pace of technological change and the associated increase in security vulnerabilities. Trusted partnerships between business and government at all levels will help the Nation stay abreast of relevant developments in technology and digital infrastructure modernization. The U.S. Department of Energy Cybersecurity Risk Information Sharing Program, NIST's National Cybersecurity Center of Excellence, and DHS/CISA's Information and Communications Technology Supply Chain Risk Management Task Force are examples of the mutual benefit that this type of cooperation affords. Adapting these models may make sense for other federal organizations and interested states or regions as well.

These findings and recommendations will help drive the unity of effort needed for rapid response to and successful recovery from the damaging impacts on our Nation of future hazards, both natural and human-made. With the release of this *Call to Action*, BENS enters a second, critical phase of work in achieving the Commission's goal to ensure that the United States has superior capabilities to respond to such crises.

During this second phase, we will pursue the specific policy, legislative, regulatory, and administrative changes necessary to implement the Commission's 11 recommendations and will leverage the power of public sector, business, and civil society stakeholders to ensure mission success. We look forward to engaging Congressional, Executive Branch, and state partners in building a safer and more secure America.



ACKNOWLEDGEMENTS

This report was developed and written through the knowledge and hard work of our Commissioners and their staffs, 165 interviewees, more than 80 BENS members, and BENS staff brought together under the auspices of the Commission on the National Response Enterprise. BENS expresses its deepest gratitude to all who contributed and offers special thanks to Congresswoman Elissa Slotkin for insights and perspectives shared throughout the process.

WORKING GROUP 1: SURGE

Pete Dordal
President, GardaWorld Federal Services – Co-Chair

John Huntz
Managing Partner, Huntz & Co. – Co-Chair

Mandy Cavanaugh
Owner, Team Housing Solutions

Jim Evans
President, Sevan Multi Site Solutions

Max Kelly
Co-Founder & CEO, [redacted]

Doug Kitani
CEO & Director, Erickson

Suzet McKinney
CEO & Executive Director, Illinois Medical District

Sean Murphy
Managing Director, BDO USA

Roy Shaposhnik
Owner, RS Logistical Solutions

Jeff Stone
Chairman, Indigo BioAutomation

Glenn Vogel
CEO, Espire Services

Rory Yanchek
Vice President, 3M Company

WORKING GROUP 2: SUPPLIES

Stan Walz
President & CEO, Vector CSP – Co-Chair

Major General Jim Hodge (ret.)
President, Institute for Defense and Business – Co-Chair

Bill Banta
General Manager, Enterprise Solutions

Len Botkin
Global Corporate Services Executive, Bank of America

Jeff Campbell
Vice President, the Americas, Global Government Affairs, Cisco

Catherine H. Crawford, PhD
IBM Fellow, Research, IBM Corp.

Roosevelt Giles
President & CEO, Endpoint Consulting LLC

VADM. Mark Heinrich (ret.)
Founder & Managing Director, Oakleaf Partners

Andrew Hersh
Head of Critical Infrastructure Resiliency, Lockton Companies

Ellen Houlihan
Lecturer on Effective Leadership, Catalyzer

Beth Jones
Managing Director, Center for Accelerating Operational Efficiency, DHS Center of Excellence

Carrie Kinsler
Chief Executive Officer, TXR Logistics

Jeff Lucas
Office of Senator Bill Cassidy (R-LA)

David O'Brien
Senior Vice President & Chief Supply Officer, Exelon

Fred Roberts
Director, Comman, Control, and Interoperability Center for Advanced Data Analysis, DHS Center of Excellence

Maria Sierra
Office of Senator Bill Cassidy (R-LA)

Ben Trowbridge
Managing Partner, Acelros

WORKING GROUP 3: PEOPLE

Roger Shedlin, MD, JD
President, CEO & Chairman, OrthoNet – Co-Chair

Chris Smith
Principal, Business Consulting, Grant Thornton LLP – Co-Chair

Stephen Baum
President, The Point Group Network LLC

Jim Brown
Founder & General Partner, Arena Growth Partners

John Carder
Vice President, Information and Technology, & Chief Information Officer, Messer Construction Co.

Catherine H. Crawford, PhD
IBM Fellow, Research, IBM Corp.

Scott Drach
Vice President, Human Resources, Boeing Defense, Space & Security

John Driscoll
CEO, Carecentrix

Matthew Lawlor
Executive Chair, Ceca Foundations

Brendan Marshall
Founder, Flow

Steve Mathias
Vice President, Global Military Sales and Strategy, Bell

John McCartney
Chairman, Huron Consulting

Chip Whitaker
Executive Vice President, Metis Solutions

WORKING GROUP 4: INFRASTRUCTURE & ECONOMY

Sam Cole
Principal, Stonecutter Ventures – Co-Chair

Chris Marlin
President, Lennar International – Co-Chair

Steve Cannon
CEO, AMB Group

Mike Capps
CEO, Diveplane

Paul Cheng
President, Famecast Media

David Christian
Executive Vice President (ret.), Dominion Energy

Catherine H. Crawford, PhD
IBM Fellow, Research, IBM Corp.

Dan Hesse
Former CEO, Sprint

Dan Holland
Managing Director, Goldman Sachs

Frank LaPrade
Chief Enterprise Service, Officer Capital One

James Smith
Senior Managing Director, Ankura Consulting

Chris Vincze
CEO, TRC Companies

Samuel Visner
Director, National Cybersecurity FFRDC, MITRE

Mark Wassersug
Chief Operating Officer, Intercontinental Exchange

WORKING GROUP 5: ROLES

Thurbert Baker
Former Attorney General, State of Georgia – Co-Chair

Chris Musselman
Head of US Commercial Business, Palantir Technologies – Co-Chair

Lauren Bedula
Senior Vice President, Beacon Global Strategies

Alfred Berkeley
Chairman, Princeton Capital Management

David Bonfili
CEO, ACME General Corp.

Edward Davis
Founder, Edward Davis Company

Christopher Frech
Senior Vice President, Global Government Affairs, Emergent BioSolutions

Lori Hennon-Bell
Vice President, CSO, Prudential Financial

Murang Pak
President & CEO, Global Risk Advisers

Riaz Siddiqi
Chairman, Clovis Point Capital

Anthony Vinci
Managing Director, Cerberus Capital Management

Shaun Modi
Co-Founder & Managing Partner, TM

COMMISSIONER ADVISORS

Lawrence Di Rita
Greater Washington, D.C. Market President
Bank of America

Mark Patterson
SVP, Chief of Staff to the Chairman & CEO
Cisco

ADVISORY GROUP

Mary M. Boies
Counsel, Boies, Schiller & Flexner, LLP

Raphael Benaroya
Managing Director, Biltmore Capital Management, LLC

Denis A. Bovin
Senior Advisor, Evercore Partners, Inc.

Norman "Norm" C. Chambers
Former Chairman, NCI Building Systems

Steven E. Darnell
President & CEO, SPG International, LLC

John K. Hurley
Managing Partner & CIO, Cavalry Asset Management

Ramon P. Marks
Sr. Partner (Ret.), Arnold & Porter, LLP

Bruce E. Mosler
Chairman, Global Brokerage, Cushman & Wakefield, Inc.

William "Bill" F. Murdy
Chairman, Thayer Leader Development Group

BENS STAFF

Sean Berman
Senior Associate, Policy/Projects

Peter Crail
Director, Policy/Projects

Sally Hayes
Research Associate

Courtney Joline
Director, Policy/Projects

Samantha Kirsch
Policy Associate, Policy/Projects

Clinton Long
Senior Director, Publications/ Communications

Debbie McCarthy
Senior Vice President, Engagement & Strategy

Nicole McCloskey
Research Associate

Patrick Sweeney
Vice President, Member Engagement

Caroline Preston
Senior Policy Associate, Policy/ Projects

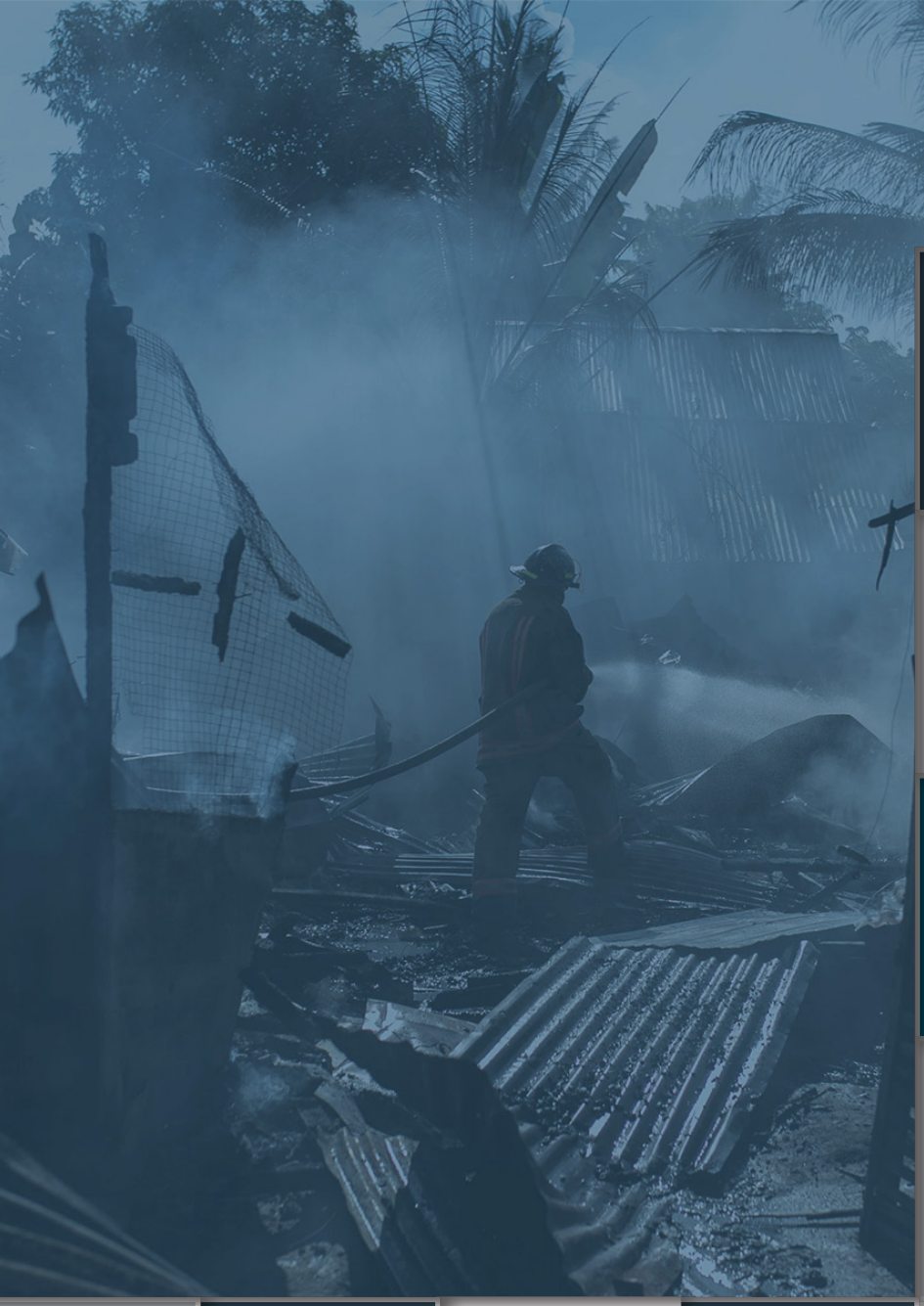
Noah Riley
Research Associate

David Smith
Research Associate

James Whitaker
Vice President, Emerging Challenges

Sean Withington
Research Director, Emerging Challenges

Aaron Woolf
Vice President, Policy/Projects



Business Executives for National Security

1030 15th St. NW • Suite 200 East
Washington, DC 20005

www.BENS.org | 202.296.2125
Twitter: @BENS_org