

**PREPARING FOR FUTURE CRISES: EXAMINING THE  
NATIONAL RESPONSE ENTERPRISE**

---

---

**HEARING**

BEFORE THE

SUBCOMMITTEE ON  
EMERGING THREATS AND SPENDING  
OVERSIGHT

OF THE

COMMITTEE ON  
HOMELAND SECURITY AND  
GOVERNMENTAL AFFAIRS  
UNITED STATES SENATE  
ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

MARCH 24, 2021

Available via the World Wide Web: <http://www.govinfo.gov>

Printed for the use of the  
Committee on Homeland Security and Governmental Affairs



U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	ROB PORTMAN, Ohio
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	RAND PAUL, Kentucky
JACKY ROSEN, Nevada	JAMES LANKFORD, Oklahoma
ALEX PADILLA, California	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
	JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*

ZACHARY I. SCHRAM, *Chief Counsel*

PAMELA THIESSEN, *Minority Staff Director*

ANDREW DOCKHAM, *Minority Chief Counsel and Deputy Staff Director*

LAURA W. KILBRIDE, *Chief Clerk*

THOMAS J. SPINO, *Hearing Clerk*

SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT

MAGGIE HASSAN, New Hampshire, *Chairman*

KYRSTEN SINEMA, Arizona	RAND PAUL, Kentucky
JACKY ROSEN, Nevada	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
	JOSH HAWLEY, Missouri

JASON YANUSSI, *Staff Director*

JILLIAN JOYCE, *Professional Staff Member*

GREG McNEILL, *Minority Staff Director*

ADAM SALMON, *Minority Research Assistant*

KATE KIELCESKI, *Chief Clerk*



# CONTENTS

Opening statements:	Page
Senator Hassan .....	1
Senator Hawley .....	9
Senator Cassidy .....	11
Senator Rosen .....	13
Senator Ossoff .....	18
Senator Scott .....	23
Prepared statements:	
Senator Hassan .....	27

## WITNESSES

WEDNESDAY, MARCH 24, 2021

General Joseph L. Votel, U.S. Army (Retired), President and Chief Executive Officer, Business Executive Officer, Business Executives for National Security; Accompanied by the Hon. W. Craig Fugate, Former Administrator, Federal Emergency Management Agency, U.S. Department of Homeland Security; Kristi M. Rogers, Managing Partner, Principal to Principal LLC; and Michael Capps, Ph.D., Chief Executive Officer, Diveplan Corporation	
Testimony .....	3
Prepared statement .....	29

## APPENDIX

Findings and Recommendations of the BENS Report .....	32
---	----



**PREPARING FOR FUTURE CRISES:  
EXAMINING THE NATIONAL RESPONSE  
ENTERPRISE**

---

**WEDNESDAY, MARCH 24, 2021**

U.S. SENATE,  
SUBCOMMITTEE ON EMERGING THREATS AND  
SPENDING OVERSIGHT,  
OF THE COMMITTEE ON HOMELAND SECURITY  
AND GOVERNMENTAL AFFAIRS,  
*Washington, DC.*

The Subcommittee met, pursuant to notice, at 10 a.m., via Webex and in room SD-342, Dirksen Senate Office Building, Hon. Maggie Hassan, Chair of the Subcommittee, presiding.

Present: Senators Hassan, Sinema, Rosen, Ossoff, Scott, and Hawley.

Also present: Senator Cassidy.

**OPENING STATEMENT OF SENATOR HASSAN<sup>1</sup>**

Senator HASSAN. Good morning, everybody. This hearing will come to order. I want to thank our witnesses for joining us today and for volunteering to serve on the Business Executives for National Security (BENS) Commission on the National Response Enterprise.

The Commission's purpose was to bring former government leaders together with business executives to find ways to better prepare for, and respond to, future crises. Thank you all for answering that call to service.

I also want to thank Senator Paul as well as his staff for working together with me to hold the Emerging Threats and Spending Oversight (ETSO) Subcommittee's first hearing of the 117th Congress. I look forward to working together to address the emerging national, economic, and homeland security threats facing the United States and identifying ways to prevent waste, fraud, and abuse related to Federal spending. I will work with Ranking Member Paul and all of my colleagues on the Committee on a bipartisan basis to make our country safer and more fiscally responsible.

The Business Executives for National Security Commission was founded nearly 40 years ago as a national and nonpartisan organization to bring senior, private sector executives together with government policymakers to discuss business challenges faced by public and private sector organizations dealing with national security issues. While some members of BENS have previously served in

---

<sup>1</sup>The prepared statement of Senator Hassan appears in the Appendix on page 27.

government, many have spent much or all of their careers in the private sector and bring fresh perspectives to pressing national security issues.

In the summer of 2020, with the United States and the rest of the world battling the coronavirus disease 2019 (COVID-19) pandemic, the organization convened a Commission on the National Response Enterprise. They brought together some of the most respected and accomplished leaders from government and corporations to research and analyze many of the factors that lead to effective emergency preparedness and response. The Commission was prompted to make sure that it did not view issues too narrowly through the lens of the current pandemic, but to understand what needs to be done to improve preparedness and response to virtually any type of future crisis, whether it be a pandemic, a natural disaster, a coordinated cyber attack, or an act of terrorism.

The commission was co-chaired by Jeh Johnson, the former Secretary of Homeland Security; Alex Gorsky, the chairman and Chief Executive Officer (CEO) of Johnson & Johnson; and Mark Gerencser, the former managing director of Booz Allen Hamilton and the BENS Chairman of the Board. Thirty-three additional commissioners from government, business, and civil society joined these co-chairs, in addition to General Votel, the president and CEO of BENS, to identify ways to increase U.S. resiliency for future crises. I was honored to be included in the process as a guest to provide a congressional perspective alongside my colleague, Senator Cassidy, who is also joining us today.

In just a few months, the commission interviewed 165 government, private sector, and other stakeholders and developed 11 recommendations for ways to improve our preparedness and response capabilities. The Commission's recommendations focused on three key areas: facilitating communication and coordination, delivering supplies and volunteer resources, and leveraging emerging technology. Recommendations range from amending the Stafford Act to include pandemics, cyber events, and other emergencies of extended duration, to expanding the inclusion of nontraditional partners by the Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) in response efforts. The Commission also recommended consistent and pervasive exercises across the emergency response enterprise and enhancing stockpile resilience by investing in cutting-edge technology that can enable real-time information sharing and rapid decisionmaking.

The Commission's report<sup>1</sup> and the testimony provided today will provide a foundation for action for this Subcommittee. I will work with the commission, Senator Cassidy, and the Members of the Subcommittee to introduce legislation to address the issues that we will discuss today, to better prepare communities all across the United States to manage future crises.

Now we will move to introductions. I want to thank everybody for joining the Subcommittee here today, and I am going to introduce our witnesses. Ranking Member Paul, when he arrives, will have an opportunity to make an opening statement.

---

<sup>1</sup>The report referenced by Senator Hassan appears in the Appendix on page 32.

It is the practice of the Homeland Security and Governmental Affairs Committee (HSGAC) to swear in witnesses. If the witnesses would please raise your right hands? Do you swear that the testimony you will give before this Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

General VOTEL. I do.

Mr. FUGATE. I do.

Ms. ROGERS. I do.

Mr. CAPPS. I do.

Senator HASSAN. Thank you.

I will now proceed with witness introductions. First, General Votel.

Our first witness today is General Joseph Votel, the president and CEO of Business Executives for National Security. General Votel leads the organization's talented staff across seven regional offices and works with the Board of Directors and the organization's 400-plus members to develop and execute their strategy. General Votel joined BENS in January 2020 following a decorated 39-year military career where he commanded special operations and conventional forces at every level.

In his last military position, he served as the commander of U.S. Central Command (CENTCOM), where he was responsible for U.S. and coalition military operations in the Middle East, Levant, and Central and South Asia. He led the 79-member coalition that successfully liberated Iraq and Syria from the Islamic State Caliphate. He is a nonresident distinguished fellow at the Middle East Institute and the Belfer Center at the John F. Kennedy School of Government. He sits on the executive board of the Center for Ethics and the Rule of Law at the University of Pennsylvania Law School, is an adviser to the Combating Terrorism Center at West Point, and is a member of the Council on Foreign Relations.

General Votel graduated from the U.S. Military Academy at West Point and later earned a Master's degree from the U.S. Army Command and Staff College and the Army War College.

Welcome, General Votel. You may now proceed with your opening 5-minute statement.

**TESTIMONY OF GENERAL JOSEPH L. VOTEL,<sup>1</sup> U.S. ARMY (RETIRED), PRESIDENT AND CHIEF EXECUTIVE OFFICER, BUSINESS EXECUTIVES FOR NATIONAL SECURITY; ACCOMPANIED BY THE HONORABLE W. CRAIG FUGATE, FORMER ADMINISTRATOR, FEDERAL EMERGENCY MANAGEMENT AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY; KRISTI M. ROGERS, MANAGING PARTNER, PRINCIPAL TO PRINCIPAL LLC; AND MICHAEL CAPPS, PH.D., CHIEF EXECUTIVE OFFICER, DIVEPLANE CORPORATION**

General VOTEL. Good morning, Chairwoman Hassan and Ranking Member Paul and distinguished Members of the Subcommittee. Thank you for the opportunity to appear before you today to discuss the work of the Commission on the National Response Enter-

prise, convened by Business Executives for National Security last June.

Let me start and enhance on your introduction of BENS here by saying BENS is a national, nonpartisan organization of senior executives who volunteer their time, talent, and treasure to address business-related challenges faced by organizations across the national security enterprise. Since its founding in 1982, BENS' members have assisted military and government partners by sharing expertise, recommendations, and best practices from their own experiences in the private sector and proactively identifying and offering insights, perspectives, and advice on security objectives.

Just over a year ago, Americans were barraged around the clock by news of skyrocketing COVID diagnoses and deaths, the devastating toll of the pandemic on the U.S. economy and supply chain problems for everything from toilet paper to respirators to medical personnel. In these reports, our BENS members recognized business challenges with which they grapple every day and saw an opportunity to use their experience to help—if not immediately, then to strengthen the Nation's response to future crises.

With that goal in mind, BENS launched the Commission on the National Response Enterprise to create what we believed would be a new emergency response model to strengthen U.S. resiliency through enhanced coordination, communication, and cooperation between government, business, and civil society. We assembled 33 commissioners representing each of these sectors to work on the issue—former military commanders or leaders, CEOs of respected American corporations, a former Cabinet Secretary, a Nobel laureate, former homeland security advisers, Members of Congress, and State and local leaders.

Joining them were 58 additional business leaders, mostly members of BENS, who interviewed 165 government, private sector, and civil society stakeholders and researched five critical component areas of emergency response: roles and responsibilities, surge capacity, supplies management, people—the human resources—and infrastructure and economy. I want to take this opportunity to thank Senators Hassan and Cassidy for their support and guidance as commissioners throughout our 90-day work period and in the months since. It has been and continues to be invaluable to us.

The commission ultimately concluded that the Nation does not, in fact, need a new model of emergency response; the components of an integrated national response capability are present within the U.S. National Response Framework (NRF). However, significant execution challenges do exist, particularly when a crisis impacts numerous States simultaneously or extends over a prolonged time period. Gaps and breakdowns in systems and operations have disrupted communication, coordination, and surge and supply chains across all sectors throughout the COVID-19 response.

Until these weaknesses are addressed, future pandemics, natural disasters, coordinated cyber attacks, or acts of terror will have the ability to imperil our citizens, cripple our infrastructure, threaten our economy, and put our national security at risk. Now is the time

---

<sup>1</sup>The prepared statement of General Votel appears in the Appendix on page 29.

for transformational thinking about emergency response strategy, policies, and processes.

The commission's Call to Action offers 11 recommendations for redesigning our response capabilities to embrace 21st century realities in how the United States handles national crises. They are focused in three areas: facilitating communications and coordination, delivering supplies and volunteer resources, and leveraging emerging technologies.

I highlight for your awareness several actions embedded within these recommendations that appear especially relevant to the Subcommittee's mission areas. These include, as you mentioned, amending the Stafford Act to include pandemics, cyber events, and other emergencies of extended duration or with nationwide impact; biennial delivery of a National Emergency Response Strategy by the Secretary of Homeland Security; establishment of expense reporting authority for all emergency-related response spending by the Federal Government; redesign of FEMA's National Response Coordination Center (NRCC) to link responder networks and help create a common operating picture for all stakeholders; wider inclusion of nontraditional partners by the Department of Homeland Security and FEMA in response efforts; creation of a FEMA Surge Center that can deliver the situational awareness, secure information exchange, and data analytics needed to drive accurate, real-time decisionmaking; development of a secure national disaster app offering access to features like a map displaying current disaster and response activities, and artificial intelligence (AI)-enabled predictive analytics indicating future threat areas; the acquisition and use of technologies capable of engendering trust in the handling of personal data; exploration of targeted protections for organizations and businesses asked to share data with governments during times of crisis; driving information technology (IT) modernization by Federal organizations that are part of the National Response Framework; and migration of State and local legacy systems to new, secure platforms capable of integration with those National Response Framework organizations; and, finally, establishment of consistent, pervasive exercising across the emergency response enterprise.

Joining me today are three commission experts with deep subject matter knowledge related to FEMA, to surge and supply activities, and data and technology. They will help answer your questions on these or any other recommendations. They are former FEMA Administrator Craig Fugate, who was involved in all aspects of our report related to FEMA, as well as all of the recommendations related to communications and coordination; Kristi Rogers, a managing partner at Principal to Principal LLC, who spent considerable time focused on supply and surge and the human resource (HR) aspect of our recommendations; and Michael Capps, the CEO of Diveplane Corporation, who is an expert in leveraging technology.

We cannot change what has already occurred, but we can commit ourselves to doing better in the months and years ahead. BENS hopes that our commission's work can be a blueprint for elevating America's ability to respond to future crises. We stand ready to work with you, the full Committee, and all interested Representa-

tives and Senators in moving the Nation forward toward this critical goal.

Thank you very much.

Senator HASSAN. Thank you so much, General Votel. I am going to take a minute, too, to recognize the accompanying witnesses with you and say a little bit about them for the record. I am very grateful not only to you, General, but to the witnesses you mentioned for being part of this testimony today. Let me recognize all three: the Honorable W. Craig Fugate, Ms. Kristi Rogers, and Mr. Michael Capps.

Mr. Craig Fugate is a former Administrator of the Federal Emergency Management Agency, a position he held for nearly 8 years. He previously served as the Director of Florida's Division and is a recognized expert on emergency preparedness and response issues. As a member of the Commission on the National Response Enterprise, Mr. Fugate lent his experience and expertise regarding the Federal role in national emergencies, existing gaps, and how to address surge capacity.

Ms. Kristi Rogers is the managing partner of the consulting firm Principal to Principal LLC, which advises business executives and leaders. Earlier in her career, she served in several government roles, first at U.S. Customs and Border Protection (CBP) within DHS, beginning shortly after September 11, 2001, later serving 9 months in Iraq with the Defense Department (DOD). As a commissioner, she lent her expertise on a variety of emergency response issues, including supply chain and surge capacity.

Mr. Michael Capps is the CEO of Diveplane Corporation, an artificial intelligence computer that works with the Department of Defense. Mr. Capps has taught artificial intelligence and the use of virtual reality for training at the Naval Postgraduate School. He has extensive experience in the technology sector, including as president or CEO of three cutting-edge software companies. As a commissioner, Mr. Capps helped guide work on data and technology use in national crises.

Mr. Fugate, Ms. Rogers, and Mr. Capps, I understand you are all prepared to help answer the Subcommittee's questions today. I thank you so much for your work and for joining us.

We are now going to begin our round of questions. I have been notified that due to a conflict, it is unlikely that Senator Paul will be able to join us. I am going to proceed now to a set of questions, and then after that I will recognize Senator Hawley for his.

General Votel, while some people associate FEMA with disasters like major storms and wildfires, I know that FEMA, as well as State and local emergency managers, tries to make an all-hazards approach in drills and preparation. But Congress may need to clarify Federal law to reflect that all-hazards approach.

The commission's first recommendation includes amending the Stafford Act to include pandemics and cyber attacks for FEMA disaster assistance. General, can you tell us why and what would be the practical effect of such a change?

General VOTEL. Thank you, Madam Chairwoman. Yes, I think the immediate response would be inclusion of pandemics or these other types of national shocks that we have been talking about would allow for a more rapid distribution and focus of resources,



money, and leadership toward the problem. I think one of the things that we discovered in the process of this, because there was some initial confusion in the early days of the pandemic, looking at it as a medical issue, the government initially focused in on medically oriented organizations, the Department of Health and Human Services (HHS), before ultimately assigning the responsibility of this to the Federal Emergency Management Agency. In that time, valuable time was lost in focusing on the problem.

I think the key thing that this amendment does is it provides the opportunity to immediately focus on the emergency and get the necessary resources flowing toward them.

Senator HASSAN. Thank you.

General, another question. Recent events have highlighted the challenges of stocking, maintaining, and distributing emergency supplies in the Strategic National Stockpile (SNS). The Department of Health and Human Services is the lead agency when it comes to management of the Strategic National Stockpile, but should FEMA have a role in coordinating with HHS going forward?

General VOTEL. Yes, I think they should. Through the National Response Coordination Center, FEMA can have some ability in making sure that we have the appropriate resources on hand to deal with any of these particular emergencies. An important role that FEMA plays in this through things like the NRCC is the ability to have well-established relationships with industry and with other civil organizations out there who are providing the resources for this. I think it is absolutely critical that they play in this particular area.

Senator HASSAN. Thank you. I want to ask a follow-up. How can emerging technologies such as artificial intelligence help address these challenges? Certainly, if Mr. Capps or Ms. Rogers want to add thoughts about this, that would be great.

General VOTEL. Let me jump in here, and then I will defer to my colleagues here. I think one of the key things where artificial intelligence can help us in the modeling aspect of this. This is another area where the work of the commission identified some challenges here in trusting models that can be used to help predict what is happening. All of us are aware, with hurricanes and other natural disasters, we have become very confident in the models that are used by the National Weather Service (NWS) and others to predict landfalls where all that takes place so that people can get out of the way, they can prepare, we can have the necessary resources ready to go, we are thinking about it in both time and space.

I think one of the things that technology can help do, particularly artificial intelligence, is help fill that gap as we look at some of these other disasters. I will defer to Mike and others to comment.

Mr. CAPPS. Thank you, General, and thank you, Madam Chairwoman. I look at AI as both a defensive concern as well as a capability in that we need to make sure that our data, our systems, our cloud are operational, because we cannot maintain an economy or resilience without them. But then looking to what they can do for us, it is just impossible to tabletop all the scenarios with people around the table in the way that you can do with AI, so building models and then building resilient models is a real opportunity.

When we were working on this commission, we thought of issues like Hurricane Katrina and difficult it is to know where are people and what needs to be where. If you imagine, if we just simply knew where every operating Internet of Things (IOT), Internet-enabled refrigerator was in Louisiana, what that could have done for us. That is information you need to gather in advance, which is exactly what these sort of partnerships we are proposing might be able to do. Thank you.

Senator HASSAN. I assume artificial intelligence and technology can help us keep track of what we have in the National Strategic Stockpile, for example, and again, match supplies to need in a much more efficient way.

Mr. CAPPS. Absolutely. Just the tracking problem, it is interesting how hard it is to know what is on what truck and where. But that is the sort of thing that, again, with IT modernization efforts across government and partnering with private enterprise, it is the sort of thing we could do. Having a real situational picture is the first step toward prioritizing response.

Senator HASSAN. Great. Ms. Rogers, do you want to add anything? I wanted to also add about data collection and analysis in terms of identifying where distribution needs are the greatest. If you wanted to address that or just generally the use of other technologies, that would be helpful.

Ms. ROGERS. I do. Thank you. Thank you, Madam Chairwoman, again for the opportunity to speak today and the recognition for this important issue.

I will take a bit of what General Votel said in regard to the commission's recommendation to create or, actually, I would say transform, evolve FEMA's National Response Coordination Center and make it a permanent state-of-the-art organization that could be an interagency organization, meaning it could coordinate or should coordinate directly with the Strategic National Stockpile, with HHS, the Centers for Disease Control (CDC), U.S. Food and Drug Administration (FDA), and the Biomedical Advanced Research and Development Authority (BARDA) all within it, but we need one organization that is responsible for the preparedness planning and response. That is important to deliver consistent information on supply demand to the private sector. A lot of companies stepped up and wanted to help, but weaknesses in supply and demand signaling by the Federal Government and the lack of a coordinated, consistent voice by the government to the private sector really hampered the production and the delivery of much-needed personal protective equipment (PPE), medical equipments, and pharmaceuticals.

The Surge Center, as we are recommending for FEMA, could also be housed in the National Response Coordination Center, and it would be state-of-the-art, completely digitalized, allowing secure sharing of information between the government and the private sector, and it would allow a clear demand signal to be provided to government so companies would know what they needed to ramp up in production, when to deliver, and where to deliver.

Senator HASSAN. Thank you. Before I turn it over to Senator Hawley, I wanted to ask Mr. Fugate, since we got into his area of expertise, whether he has anything to add on this particular topic.

Mr. FUGATE. Madam Chair, talking about AI, talking about data, this always goes back to the question that we also talk about in the report. We have to have production capacity within the United States when we are dealing with global threats. One of our big challenges in the supply chain is even knowing where stuff is, if it is not being produced in the United States, we may not be able to get it fast enough.

Senator HASSAN. Great. Thank you so much. Now to Senator Hawley.

#### **OPENING STATEMENT OF SENATOR HAWLEY**

Senator HAWLEY. Thank you, Madam Chair. Thanks to the witnesses for being here.

General Votel, let me turn back to you. It is nice to see you again in a somewhat different capacity than when I saw you last before the Senate Armed Services Committee. Let me ask you about this report. Just on the subject of supply chains, what do you think that we should learn from the pandemic about the vulnerability of our critical supply chains in particular?

General VOTEL. Thank you, Senator, and it is good to see you again. I think the most important point is that we have to come to some resolution on what it is that we need to have stockpiled and what those essential resources and supplies are that we need to have stockpiled, of course, and ready to go. Then we need to make sure that we know where those things come from and what the supply chains are associated with those and where there are dependencies that are overseas or where production capacities are within the United States that can be invoked to address those.

I really think this gets down to overall awareness and understanding of what we are going to have on hand and then how we reach out and grab the things that we need as a crisis emerges.

Senator HAWLEY. Let me ask you about the just-in-time production. It seems to me that one of the weaknesses with our supply chains is this just-in-time production model and other efficiency measures that, while they no doubt help the corporate bottom line, also can leave us vulnerable and exposed in a crisis, as we saw this last year.

You talk about this a little bit in the report, I believe. I wonder if you could discuss the problem, some of the problems with the private sector's emphasis on just-in-time production as it relates to the National Response Enterprise.

General VOTEL. Sure, Senator. The real challenge here is that when we do just-in-time supply, what that means is that the initial surge of capabilities that we need early in a crisis to respond and bring things under control may not be immediately available to us. Of course, this is the challenge. What is needed is more coordination and discussion between those at the Federal level, and perhaps State level, who are managing these stockpiles and those who are producing the items that go into them. We will need to accept the fact that we have to work very closely with businesses to provide—have stuff on hand, rotated in and out of stock so that it stays up to date, and that the businesses will have arrangements that they are not doing this at a loss to their bottom lines. There has to be much closer coordination over this particular issue right

here. It is absolutely critical, especially in the early stages of a crisis.

Senator HAWLEY. Let me ask you about the responsibilities that our largest corporations have when it comes to this issue and, in particular, supply chain resilience. For example, what I am thinking of is if we have a major corporation that produced certain essential goods, like medical devices, for instance, should they be required to take steps to boost supply chain resilience, onshore jobs back domestically, report on where they source their products, things of that nature, given the fact that we rely on these essential products so much?

General VOTEL. Thanks, Senator. I would invite Ms. Rogers to comment on this as well, but, yes, I think we have to—for these organizations, private sector organizations that we rely on for these critical resources, they need to be incentivized and encouraged to make sure that we know with some level of reliability that we can get our hands on those particular supplies.

Ms. ROGERS. Senator, if I may address that in two different ways. You are correct that resiliency in companies today often means sort of vital capacity, which is the antithesis of a lean, efficient, profitable business model. But I do not think you have to do away with that, actually. With today's innovative technologies, the widespread adoption of them could actually build in resiliency. The adoption of 3D printing, of digital twin, of, additional AI and other data sharing, that could allow a surge capacity without delayed time and still allow a company be profitable.

You could further enhance that, as the General said, with a combination of incentives, and I would say sort of modern-day public-private partnership. The private sector has the innovation, the ingenuity, and the wherewithal to be able to do this. What the government needs is to create a path to allow those companies that want to help in the state of a crisis to do so. It could be a combination of tax incentives, of grants. It just depends upon the size of a company and what a company needs. A smaller company might need access to capital, so it could be also a loan.

I would say it needs to be a combination of integrating state-of-the-art technology along with tax incentives, grants, and loans to the private sector.

Senator HAWLEY. Very good. Thank you, Ms. Rogers, for that. Thank you, General.

General, let me switch to FEMA, if I could for a minute. FEMA, of course, took a major role in procuring and distributing PPE during the early stages of the pandemic, including Project Airbridge, which arranged air transport for PPE from other countries. How would you assess FEMA's role in that operation?

General VOTEL. I think perhaps Mr. Fugate can provide some more expert information on this, but in my view, what FEMA encompasses here is the expertise and the management skills to deal with crises. I think their role in this early on is absolutely essential, and as we have seen, they end up being an organization that becomes a go-to for many of the crises that our country faces.

Craig, thoughts, please?

Mr. FUGATE. Thanks, Senator. They did what they had to do. I think our concern on the commission was it was late to need. It

was not clear that FEMA had this role. In prior planning, we had focused on FEMA's role in supporting the Governors as a consequence of a pandemic, with HHS having the primary lead on supply chain, supply, distribution, acquisition. I think, as we point out, clarifying these roles now that FEMA does have a role supporting HHS, these are things that FEMA would likely be called upon to do, I think even improves that capability and speeds it up so it is not late in the ending before they are being utilized.

Senator HAWLEY. Very good. Thank you all. I have some more questions I will submit for the record.

Thank you for your work, and thank you for being here.

Thank you, Madam Chair.

Senator HASSAN. Thank you, Senator Hawley. As we look at timing, there will likely be an opportunity for a second round of questions as well, for everybody's awareness.

Now I want to move to Senator Cassidy, who is joining us as a special guest because of his role with BENS over the last several months.

#### OPENING STATEMENT OF SENATOR CASSIDY

Senator CASSIDY. Yes, I am not on the Committee, so they are allowing me to join from my kitchen. Thank you, Madam Chair. Thank you, BENS, for all the work you have done.

I got so many questions. Let me just start with you, Mr. Fugate. Building upon that last line of questioning, when everything hit the fan, my appropriations guy said there is no way FEMA does not take the lead because they have to dispense a lot of money very quickly, and HHS does not have the infrastructure to do that.

I was speaking to a doctor involved with disposition of ventilators, HHS had that expertise, but FEMA took it over, as I gather, because they were now writing the checks. They may have come late to the game, but they were dominating the game. They were now making decisions which, frankly, they did not have the training to do.

There has been some kind of, we need to build out HHS so they can dispense lots of money quickly. But that seems like we should be able to concentrate that in one agency, not duplicate in both. On the other hand, you do not want FEMA making decisions about health care when it is just some guy who slept in a Holiday Inn last night.

How do we reconcile those tensions?

Mr. FUGATE. It is going back to FEMA's classic role, Senator. FEMA is a support agency. They are not the lead agency. They support Governors in most disasters, or in the case of a lead Federal agency like HHS, where HHS is in charge of the response. But FEMA has a convening power. It has tools on their staff for that. It has capabilities that support that. It was not much different than our role in supporting the Centers for Disease Control during Ebola. We did not take over that response, but we sent teams in to help CDC staff the—

Senator CASSIDY. Can I ask you a group dynamic question? Because it does seem that if somebody has the convening power and somebody has the ability to dispense dollars all over the Nation and somebody, et cetera, et cetera, et cetera, that whether or not

they are technically supporting, in reality they begin to assume responsibility of leadership. You have been there. I have been in the middle of a hurricane hitting Louisiana, and it does seem at some point the Federal role becomes pretty prominent in terms of direction of activity.

I know that how it is on paper. It did not seem to work out that way. That may have been an internal dynamic within the administration. Is it possible for FEMA to only be supporting when they have such a prominent role otherwise?

Mr. FUGATE. Absolutely. FEMA had a prominent role in responding to the hurricanes in Louisiana and coordinating the Federal response, but the lead was always the Governor of Louisiana. I think that is the thing we missed when the decision was made to put FEMA in charge of the response. I would not have done that. I would have kept Health and Human Services in charge of the medical, the decisions, the policies, but I would have tasked FEMA for coordinating with the rest of the Federal family where they have a lot of built, deep relationships to support that, and then focus on supporting the Governors on a lot of the consequences.

We have looked at this in a variety of types of emergencies that fall out of that traditional Governors, State led, FEMA supported, where there is a Federal lead agency. There are always going to be personalities, but I think the role of FEMA is as the support agency, the support element to that lead role, whatever Federal agency it is. It is personalities sometimes, but I think codifying that structurally in statute, the Stafford Act and other ways, can also ensure that FEMA has that role, is called in early, but it is a support to that lead Federal agency.

Senator CASSIDY. OK. Ms. Rogers, there have been a couple questions here regarding inventory management. Now, we know the private sector will often use vendor-managed inventory, first-in, first-out, that sort of thing. We heard stories of these strategic national supplies inventory declining, having obsolete equipment, or stuff that was just on the brink of being expired—nothing that should happen in a well-run major hospital. That would have been used before it expired. Any thoughts regarding a vendor-managed inventory to manage our Nation's stockpile? For context, the buyer owns the inventory, but there is a vendor which manages the inventory without taking possession. I am asking you on that one.

Ms. ROGERS. I think a vendor-managed inventory would be an exceptional way to go. I think there needs to be increased visibility in the Strategic National Stockpile and the State stockpiles. I think it is critical. I do think it is something—the commission recommended sort of a Surge Center that would have visibility and coordinate with the Strategic National Stockpile, understanding what the supply is, and also at the same time maintaining a sort of 24/7 visibility on the supply and the demand, not just during a crisis. But it is most important to actually do it ahead of time so you have that visibility and you are able to much better manage the first-in, first-out, what is needed, and then, of course, combining the latest technological innovations. We have just not done that. If you actually look at the Strategic National Stockpile and what digital twin technology and 3D printing could do to dramatically im-

prove the response capability and capacity of the SNS, it would be incredible.

Senator CASSIDY. Let me ask you, though, I think of 3D printing as being kind of a one-off, not the sort of surge and supply we needed for ventilators, or at least we thought we needed for ventilators. Am I wrong? Can 3D printing actually give you that volume of, you name it, say ventilators, pretty complex, et cetera?

Ms. ROGERS. We have worked with several companies, small and large, including some of the largest companies, like Siemens Government Technologies, 3M, General Motors, Ford, with some of the small ventilator companies. The biggest concern with the company that has the technology that is producing the ventilator is the proprietary information. Once you deal with the proprietary information and maybe license the technology, the 3D printing as well as the digital twin can actually greatly enhance and strengthen the volume and capacity.

Senator CASSIDY. Can you give me a sense of how many ventilators you can make with—I mean, do we have to build out our 3D manufacturing capacity? Or is there right now the ability to make 10,000 ventilators in a week using 3D printing?

Ms. ROGERS. I would say yes and yes. We do need to enhance and strengthen, and, yes, we currently have the capacity. 3M was creating—building ventilators—I am going to get this—let us say in a month, 300,000 on a normal basis pre-COVID. During the height of COVID, it was up to 10 million, 300 million, and it vastly enhanced their capability when they looked at implementing the digital twin, the 3D printing.

Senator CASSIDY. I will have a second round, but I see Senator Rosen is on, so I will log off for a second.

Senator HASSAN. Thank you very much, Senator Cassidy.  
I now recognize Senator Rosen.

#### **OPENING STATEMENT OF SENATOR ROSEN**

Senator ROSEN. Thank you, Madam Chair. Thank you, Senator Cassidy. Thank you to all the witnesses for being here today and for your service.

I am going to talk a little bit about coordinating with nontraditional partners, particularly as it relates to natural disasters, because in 2020 the wildfire season was incredibly devastating, burning more than 10 million acres nationally and hundreds of thousands of acres in my home State of Nevada. As communities continue to recover from COVID and natural disasters like wildfires, we have to provide the support and the investment to prevent further catastrophes. For wildfires in Nevada, various stakeholders coordinate response and recovery efforts. They include our Federal land management agencies, State and local governments, first responders, and one of the report's recommendations is to expand the inclusion of nontraditional partners when responding to incidents.

In Nevada, farmers, ranchers, conservation groups, they play a key role in defending against wildfire and recovering the lands after, but they are not always brought to the table.

Mr. Fugate, how can FEMA and the Federal Government expand outreach to these kind of nontraditional partners, encourage the kind of collaboration we need, particularly for us in Nevada, the

west coast, we have wildfires, but other natural disaster responses even more broadly?

Mr. FUGATE. Senator, this is something I came to the conclusion a long time ago that government-centric problem solving does not scale up the bigger the disaster is. We developed the term “whole of the community” and looked at the public as a resource and not a liability. How do you bring in those nontraditional folks that are on the ground that are going to take action anyway. There is a bias in the Federal Government not to engage outside those partnerships. At FEMA, we had to make the disasters big enough to break the system to force people into those relationships.

I think as we talk about the pandemic and we saw how that introduced new partners, it is a bias that the Federal Government has to get through, that you do not have to always be the traditional organization, you do not have to have the incident command certification. We spend a lot of time talking about credentialing, but in a disaster, who is going to show up and work that we need to be looking at. I think part of this is lowering the barriers to the public and to those nontraditional folks to be part of the team.

Senator ROSEN. I agree. I would think that there might be potential cost savings and really proactive efficiencies when you strengthen these relationships. For example, farmers and ranchers, they could be doing things ahead of time to mitigate—of course, in the case of wildfires, you can do some mitigation, maybe other things not so much. But do you think there is cost savings there for the efficiencies?

Mr. FUGATE. There is cost savings, and it speeds up response. But if you go into the wildfire community, they are traditionally not going to be very receptive to people who do not have their training and are not part of their system. They are very much focused on their safety and working with people they are comfortable with. That is when you have enough resources. When you do not have enough resources, who are you going to call? I grew up and I lived in the State of Florida, and I can tell you a lot of our brushfires here, it is a farmer with a tractor and a disc plow out there cutting a fire break. I know that works. I think it is the question of how do we bring this from the one-offs to systemically in the Federal Government recognizing the public as a resource in a crisis, not a liability, and how do we engage them more effectively.

Senator ROSEN. I agree with you there. I want to turn and build on this subject in our cybersecurity arena. Of course, speaking of nontraditional partners, we have to think about that in cybersecurity as well, so I am particularly concerned that the Federal Government, of course, alone cannot secure our critical infrastructure from the evolving, increasingly complex cyber threats that we face.

To General Votel and then Ms. Rogers, how do you think the Federal Government can expand the partnerships and information sharing with the companies that possess the cybersecurity knowledge and experience to better protect us all and kind of create that grid, if you will, of security?

General VOTEL. Thank you, Senator. I really like this discussion we are having about the nontraditional partners. This is really important. What the commission recommends here is that we look and organize to make sure that we have a point of contact for busi-



nesses in things like the National Response Coordination Center that they can reach out there to link into them.

I think what we have recognized throughout the pandemic is that while we have a tendency to think about the traditional private sector that we would go out to, in many cases, as you just highlighted, there are parts of the private sector that are not normally concerned, but are, of course, very key to this, and cybersecurity is absolutely central to this.

I agree with the assessment that you are laying out here, and I think maybe Kristi or Mike Capps can add some additional details to this particular area.

Ms. ROGERS. Thanks, Senator. I appreciate the question on this. If I may just add a little bit of context, because my answer will make more sense. Just after 9/11 I was brought in to the Department of Transportation (DOT) to work with New York City's Metropolitan Transit Authority on response. I then went to the Department of Defense and was in Iraq working on a contingency operation, then Homeland Security at Customs and Border Protection during severe acute respiratory syndrome (SARS) and Hurricane Katrina, directly involved.

My two companies in which I was CEO after, one was a contingency operation company helping the government emergency response, and the last one was we ran nine Ebola treatment units in Sierra Leone and Liberia. I had a different perspective on government response and preparedness, and an unfortunate reoccurring theme in all of those has been the government's inability to reach out and grab nontraditional partners, because it is not as though the partners—the private sector, civil society—does not want to participate in health; they do.

One of the things that I will add is in what we call Phase Zero, in the planning and preparation phase of any crisis, bring in private sector, bring in civil society to help prepare, help respond, so they are not caught off guard, so it is an integrated, systemic response.

Furthermore—and you saw this in COVID—so often there are examples where U.S. manufacturers volunteer to address needed, but could not get a go or no-go decision from the government. There was not one single authority responsible, and, two, the contracting processes did not exist. I would further recommend and the commission further recommends implementing executive emergency purchase orders, issue predefined or indefinite delivery, indefinite quantity Federal contracts, also issue blanket purchase agreements in the time of non-crisis, which means you issue a contract to, let us say, seven companies you identify. You award a nominal fee annually to those companies just to hold the capacity and capability in times of a crisis.

Senator ROSEN. I think that is very informative, and we all need IT modernization to do a lot of this. I look forward to speaking with you about that.

Thank you. My time has expired.

Senator HASSAN. Thank you, Senator Rosen.

I am going to go ahead and start a second round of questions, and I think we may have one other Senator who wants to do the same after I finish my second round.

I think the first thing I want to ask is, in this last set of questions, General Votel, you and the panel have been asked generally about supply chain. I want to drill down on that a little bit and give you all an opportunity to add anything you have not said and then move on to a couple other topics.

Early in the pandemic, the supply chain issues regarding certain items needed amid the pandemic reinforced what many of us already knew, that the United States was overly reliant on Chinese manufactured goods. General Votel, how can we reduce U.S. reliance on Chinese goods before or during the next national crisis?

General VOTEL. Certainly this is something that the commission looked at, as you know, Madam Chair. I think, the answer lies in making the deliberate decisions about where we are getting our supplies from and understand exactly what the supply chains are. The idea that we talked about within the commission is the idea of right-shoring, that there are some dependencies that we do have overseas, that are OK to maintain. Obviously, there are real concerns with China, but we also are very dependent on a number of our other international partners for these things who are fairly reliable in terms of delivering supplies to us. I think it is absolutely critical to understand where our supply chains lead us and what we need to have on hand to address the initial response to these types of emergencies.

Senator HASSAN. Thank you.

Ms. Rogers, you addressed this at a certain level and so did you, General Votel, but we obviously need to know where our critical assets are in the supply chain during an emergency. We also acknowledged and you have testified about the high levels of stress that the pandemic put on different parts of several supply chains.

I will start with you, General, and then the rest of the panelists can add if they would like to. How can we improve the government's visibility into the Nation's supply chains? You have all talked about it a little bit, but I want to give you a chance to expand on it if you would like to.

General VOTEL. One of the recommendations that we make is the establishment of a national disaster app that is kind of an opt-in ability, that gives people, particularly the private sector, really all stakeholders, civil society as well, an opportunity to see how a crisis is developing, what the future looks like for that, and then the ability to share data with government partners here to understand where supplies may be and how they may be applied to the situation.

As a military man, in looking at this, the development of a common operating picture of how we are looking at the crisis is absolutely essential in this. This is absolutely critical when it comes to both maintenance of our supplies and surge capacity, which essentially is getting the right tools to the right place at the right time. The establishment of a common operating picture through a redesigned National Response Coordination Center, and the establishment of an app to which stakeholders can opt in, I think are two very critical recommendations that the commission makes that will help go a long way toward this.

Senator HASSAN. Great. Thank you.

Would any of the other panelists like to add anything?

Ms. ROGERS. I will, briefly. I think with this newly redesigned National Response Coordination Center, whether it is within FEMA or within DHS, it needs to be one responsible, accountable body. The first thing I would say is that we do need to review and make clear to all parties what the critical goods are. What is a critical good and what are critical infrastructure? Then work backwards in that supply chain and see where the supply chain is.

If a large portion of the critical goods supply chain is in China, then we need to look at a strategy to re-shore some of it, and that might include incentivizing some of these companies. It could be re-shoring domestically, or it could actually also mean re-shoring it to an allied nation. I think that is critical, because regional diversification, whether it is regional domestically or regional amongst our allied nations, will further strengthen the resiliency of our supply chains, especially in a crisis. But I do think that a Surge Center or this National Response Coordination Center needs to have sort of state-of-the-art supply chain asset mapping capability, and it could be then downloaded to a digital app. But I think one of the first steps in the preparation planning stage is it needs to map our supply chain assets. We have not done that. We do not know where they are and where the vulnerabilities are.

Senator HASSAN. Thank you. Let me quickly move to one other and maybe two other issues before I turn to Senator Ossoff for a first round of questions.

General Votel, the commission proposes the creation of a leadership position within the Department of Homeland Security to oversee the development of a National Crisis Response Exercise Framework. How would this build upon the existing national exercise program at FEMA?

General VOTEL. Thank you. That is an excellent question, Madam Chair. The idea here is to put leaders in charge of our exercises and in our response planning, and there is no more definitive way of doing that than actually to have somebody that is held accountable for that, that can work across the organizations in the National Response Framework and bring them together to participate in exercises and rehearse plans that are in place, but also has the ability to compel leadership to participate in this. Oftentimes what we see in these instances is that we have mid-level staff participating in these, but not the leaders who are going to be making decisions. Adding leadership into the creation of this position I think gives us the best ability to really focus in on this critical task that is so important for the preparation of the Nation for these disasters.

Senator HASSAN. It is the right stakeholders as well as leadership of those stakeholders to make sure that they are at the table.

General VOTEL. That is exactly right. It is getting all the right organizations and then getting the participation at the right level of leadership that is going to be involved in making decisions in an actual emergency.

Senator HASSAN. Thank you very much.

I am over my time, and I will now recognize Senator Ossoff for his first round of questions.

**OPENING STATEMENT OF SENATOR OSSOFF**

Senator OSSOFF. Thank you, Madam Chair, and thank you to the panel for your work in preparing these recommendations for the Committee and for Congress.

General VOTEL, I want to ask you about financial infrastructure and resilience in a crisis. We saw during this COVID-19 pandemic that the provision of emergency and swift financial support directly to households has been vital to sustaining an economy that was crippled by all of the mitigation measures that were necessarily implemented in response to the pandemic. Did your working group consider what changes may need to be made to our payments infrastructure or to our macroeconomic policymaking apparatus so that in a future crisis, whether a pandemic or some other contingency, if we need to swiftly get financial support directly to households rather than via the banking system, we can do so more efficiently?

General VOTEL. Senator, the aspect that we addressed in this was not necessarily focused on amounts and that type of stuff, but it really was focused on the technology and the reliance in getting those payments to families. In the event that we do not have the right databases, we do not have the right technology to move this very quickly, these resources, to where they need to be, this was an area of some focus for us. We did make some specific recommendations, particularly as we looked at leveraging technology to help do this. It is one thing for the administration and Congress to authorize payments; it is another thing to make sure that those payments actually get to the recipients who need it in a timely fashion. In this particular area, this is where, again, technology can help us do this much faster and make sure that it gets to the targeted individuals and families and others who require these payments.

Senator OSSOFF. Thank you, General. In the event of a crisis or an attack which undermines the integrity of our telecommunications infrastructure or our financial system, particularly our payments infrastructure, what recommendations do you present for improving both the resilience but also the redundancy of those core systems?

General VOTEL. Thank you, Senator. The report talks about making use of multi-cloud technologies that are available to us today to help build resiliency into our overall system of storing data and then relying on that data at a particular time in the crisis. There are a variety of technologies that are available out there and that will actually help us do this and will actually build a level of robustness into this.

I might invite Mr. Capps to comment on this since the technology area was an area in which he focused specifically on during the commission.

Mr. CAPPS. I am happy to, General. Thank you, Senator, for the question. I would say that decentralization is critical for resilience, and decentralization requires modernization across State, local, Federal Government. I do not think we are on the path to that. The last infrastructure protection plan was in 2015, maybe, and cloud is mentioned as a future exercise of investigation. But every one of the services that we are talking about are completely built upon data links that are in the cloud. There is no notion of infrastruc-

ture resilience for the cloud. It is not part of the current mission. AI is not even mentioned anywhere on the Cybersecurity and Infrastructure Security Agency (CISA) website. CISA is a fantastic organization. They work hard. But it is not part of their mission, and so I think we have a lot of basic work to do to catch up to where private enterprise is first before we start thinking about the next steps of how would we handle black sky post a well-built cyber defense.

Senator OSSOFF. Thank you, Mr. Capps. While I have you, any recommendations or I would even invite speculation beyond the constraints of this report with respect to how mobile technology might have multi-band capacity in the event predominant cell networks are deteriorated? Any comments on whether or not we need to enhance satellite communication capacity, the ability to use satellite links to generate more local networks, either via the cell system or WiFi networks or mesh networks so that we can have decentralized, effective communication in the event that some of the centers of our telecommunications network are degraded?

Mr. CAPPS. Sir, that is a wide question, and I will say that I think we are seeing civilian advances in satellite communication. 5G is nothing but resilient. It is meant to have machine learning right in the radio centers so that it can adapt anytime systems go down. You will see the migration of mesh networks, when you think of Internet of Things devices, within a few years we will be at a million-ish devices on network per square kilometer in urban centers. If you think of the pure availability of radios, our job is going to be let us make sure those devices are secure, which there is really no handling of that right now, which I could go into detail on if you would like, and then open networks, 4- or 5G like ORAM, that allow devices to plug and play together. It is all about interface and letting them communicate with each other so that they can be resilient. Then as we transition to edge computing, which is when we have cloud at the edge, that is going to allow that small town in North Carolina to be able to be completely severed from Amazon Web Services or whatever else, but still have plenty of data locally, plenty of computation locally, and be able to be functional if they need to be in a decentralized manner.

Senator OSSOFF. Thank you. I think you touched upon this briefly or at least referenced it—any comments or observations, conclusions, recommendations you have with respect to encryption on prevailing communications networks. Also, are there any lessons that should be drawn from the recent SolarWinds and Microsoft Exchange Server breaches that touch upon some of the recommendations in the report, please? Thank you.

Mr. CAPPS. Thank you, sir. I would start with cyberspace as a sovereign entity. It is something that is difficult for us in the United States to think about. We grew up with the Internet as a public space, but our competitors treat cyberspace as sovereign for their nations. We like to joke in the IT industry that if guys with guns show up at the front door, then there will be somebody on our side to defend us. But if Russians attack or the Chinese attack or North Koreans attack the website, which they do. Even from my small AI company, I get 30,000 attacks a day. I get warnings from CISA letting me know that I might be attacked. But there is no

notion of defending critical infrastructure. I think that step one is we cannot treat our companies as a critical part of resilience for the national enterprise and also assume that they can take care of themselves. That is a bad combination.

Senator OSSOFF. Thank you. Thank you all for your testimony. Madam Chair, I yield back.

Senator HASSAN. Thank you.

Senator Scott, for his first round of questions? Do we have Senator Scott?

[No response.]

Senator HASSAN. If not, I see Senator Cassidy on my screen. Senator Cassidy, I will recognize you for your second round of questions.

Senator CASSIDY. I will start with you again, Ms. Rogers, regarding the supply chain. Now, there has been interest in the administration and the Senate to re-shore some things that we found were embargoed for shipment to the United States when the pandemic began in China. For example, N95 masks made by 3M, by force majeure, the Chinese decided not to allow them to be shipped to us.

But we have to recognize that some of this being manufactured depends upon a low labor cost in order for it to be otherwise marketable, not just during a pandemic but also in normal times. If we have a pandemic every decade, which is far more than we currently have been having one we may have a stranded asset in the 10 years between by which point the manufacturing equipment is outdated.

Now, one thing I have been interested in is a question of re-shoring and near-shoring. If we had some of this placed in a low-cost country, for example, Central America or Mexico, in which the PPE was made there or some other product made there, we would have the advantage of not having to cross an ocean, but you would have something that could remain competitive selling as goods in the interim. Any thoughts on that?

Ms. ROGERS. I agree. First, I would go back to we need to be clear on what we deem a "critical good," depending on which crisis. Then we need to look at where those supply chains are and where they are manufactured. When we do that and we say it is a critical good as manufactured in a nonallied country, we need to implement strategies, and that might be incentivizing the company to re-shore or near-shore. Mexico and Central America are great options. There are so some Far East, Near East, that are also other options that are allies.

I think we really need to be clear on what the critical goods are, and when we talk about incentivizing companies to do this, we need to recognize that there are a lot of government obstacles, impediments, and regulations that have forced companies overseas to produce these goods.

That needs to be a recognition on behalf of the Federal Government. The companies are looking at their bottom line saying we need to produce this for the United States, and if these are U.S. companies, they want to help the United States. There is no doubt about that. I have seen that throughout COVID. But they also need to sort of protect their bottom line and ensure they are still in busi-

ness, and there are a lot of bureaucracies and regulations in place that impede some of the re-shoring.

Senator CASSIDY. I agree with that. By the way, I think during the cold war that North Atlantic Treaty Organization (NATO) or NATO allies, there was a distribution of essential materials so that in every country there was something. But we did not have to depend upon a non-NATO ally for penicillin, for example. I bring up penicillin because right now so-called beta-lactam drugs, which penicillin is one of, so essential, is only produced in China. I am told that creating a strategic stockpile of the active pharmaceutical ingredient is just not practical. But I am also told that companies do not like to make it in the United States because it involves fermentation, and that in turn brings Environmental Protection Agency (EPA) upon them in a way which is onerous to comply with.

I am not saying other countries like Mexico have a lower standard, but I think the company may be more comfortable producing a fermented product in a country like Mexico as they currently are in China.

Now, China greatly subsidizes this industry, so you already have a lower cost basis because they have a State subsidy. Are you suggesting—and just to be explicit—that we may consider doing a U.S. subsidy for a manufacturing facility that would be built not in the United States but in a near-shore country?

Ms. ROGERS. I would emphasize “may.” You may consider it. I would weigh the cost option of doing that. I will give you an example. In Ireland right now, there are numerous companies, pharmaceutical and medical manufacturing, that have deemed it less expensive and cost-prohibitive to have their plants in Ireland. Ireland is now sending 20 flights a week to the United States with no passengers but full of supply. That is an allied country that we are relying on for supply and U.S. companies that actually have their manufacturing plants there. That has not been subsidized.

Senator CASSIDY. Yes, but there must be some reason for it. There must be a lower cost of doing business.

Ms. ROGERS. Yes, it is.

Senator CASSIDY. What is the source of that lower cost of doing business? Tax Code?

Ms. ROGERS. It is Tax Code, EPA regulations primarily.

Senator CASSIDY. If we are saying Tax Code, taking you someplace you may not want to go, but knowing that the administration currently wants to raise corporate tax rates, you are, implicitly stating that they may indeed drive companies to move operations out of the United States elsewhere if that were the case?

Ms. ROGERS. That would be counterproductive to our recommendations on increasing resiliency and surge capacity in the United States, correct.

Senator CASSIDY. That is very interesting. Also, you mentioned EPA, but I still think of the European Union (EU) as having fairly stringent, in some cases more stringent than ours, environmental regulations. It is not just the regulation you are implying, but it is also the means of enforcement and/or penalty. Is that something I can take from your statement? I am getting you in trouble here maybe, Ms. Rogers.

Ms. ROGERS. You could, and I could get you specific examples, but I am not prepared to name those companies now.

Senator CASSIDY. I got that, but you can give me specific examples with a little preparation in terms of—

Ms. ROGERS. Yes.

Senator CASSIDY [continuing]. How it is not just the regulation but it is otherwise enforcement.

Ms. ROGERS. I can do that.

Senator CASSIDY. OK. That is good.

Then, Mr. Capps, in the report they speak of a distributed ledger/blockchain. I am interested in the distributed ledger in a variety of ways. Can you explain how we would be able to use that to better manage pandemic response or any other kind of natural disaster or manmade disaster response?

Mr. CAPPS. Distributed ledger, all it is is a notebook that everyone has a copy of and that you can trust. When we were speaking earlier to Senator Ossoff's question about decentralization, if everyone has a full copy of every, let us say, procurement contract that has been related to PPE, everyone has it, and they all know where the material is. Then when we have some event that pinches you off from the rest of the network, you have still got all the information you need and it is a trustworthy copy.

Senator CASSIDY. Let me interrupt you for a second.

Mr. CAPPS [continuing]. It is just about that.

Senator CASSIDY. When the pandemic hit, New Orleans was getting slammed, and Los Angeles was wide open, but there was a nationwide shutdown on elective surgery. I got a call from an anesthesiologist saying, "I cannot believe there is a shortage of machines. I got 100 machines no one is using. Yes, they are anesthesia, but you could still use them for general if you had to. But we also have general anesthesia machines. We could ship them to New Orleans and then get them back, when inevitably you go down there and we go up here."

But no one had an inventory, a nationwide inventory of this. On the other hand, if we use blockchain for such an inventory, it would have to be low cost, easily done, with minimal friction cost, and still protect proprietary information.

You are the expert. Is it possible that we can have such a national inventory such as that, low cost, minimal friction, and protecting proprietary information?

Senator HASSAN. I am going to ask you to be fairly quick in your response, please?

Mr. CAPPS. It is a good question you are asking, and it kind of depends on what is within the purview of that. If we are just talking about anesthesia devices nationwide, that feels like a sort of thing that would be quite tackleable. If you are talking about any resource in the United States in order to be applied to, obviously that is very hard. But the notion of this is a trusted system, data is encrypted so I cannot access the information until there is some key given, everyone has a copy of it, and we are not spending tons of energy burning a blockchain to do it. Yes, those are totally solvable problems. You see it in supply chain management in private enterprise all the time. It all comes down to: Can I ask you some simple questions and get a simple answer—not unlike these hear-



ings, sir—where if you can do that, you can get a lot done quickly. That is exactly how the Web works, and there is no reason this could not work the same way.

Senator CASSIDY. I yield back.

Senator HASSAN. Thank you.

Senator CASSIDY. Thank you for your indulgence, Madam Chair.

Senator HASSAN. Thank you, Senator Cassidy.

Senator Scott.

#### **OPENING STATEMENT OF SENATOR SCOTT**

Senator SCOTT. All right. First, I want to thank Chair Hassan and Ranking Member Paul for holding this hearing today.

General Votel, in an op-ed in December, Director Ratcliffe declared China would be our number one national security threat. On his first day in office, President Biden revoked an order blocking Chinese components in the U.S. power grid. It seems like this would be a dangerous door to open to Communist China, and imposes an unnecessary risk to our critical infrastructure and Nation's security. Do you think Chinese components should be allowed to be used in the U.S. power grid? Or should this decision be revoked?

General VOTEL. Senator, thank you very much. My view is we are accepting unnecessary risk by incorporating Chinese components into things that we depend upon for our citizens, and especially for things that we depend upon for emergency response. Yes, I think it is a great vulnerability for us.

Senator SCOTT. We all need to understand—every American needs to understand the risk of Communist China, whether it is that they are stealing our jobs or technology, they are building a military to dominate us, they take away the basic rights of Hong Kong citizens, and are imprisoning Uyghurs. What do you think of the idea that all Americans ought to just say, look, the Communist Party of China has decided to become our enemy, our adversary, and all of us need to say we are going to stop buying Chinese products, it is a national security threat, from the standpoint if they can be in our power grid, but on top of that, it is a national security threat if they continue building their economy to use those dollars to ultimately dominate Americans.

General VOTEL. Senator, this topic is a little bit beyond what the commission addressed, but what I would share with you is that I agree with you. It is important for American citizens, American business, to understand exactly what is at stake in this competition that we have with China, and that their very aggressive, centralized approach that they execute, things like the Belt and Road Initiative and some of the predatory practices that they impose on other countries around the world to gain resources, is, in fact, a threat to our national security. I think it is absolutely vital that all American citizens in the private sector, public sector, and in the civil sector understand what is at stake with respect to our competition with China.

Senator SCOTT. Thank you, General.

Last year I introduced the American-Made Protection for Healthcare Workers and First Responders Act to ensure the United States built its stockpile of personal protective equipment so our

first responders and health care workers have everything they need to keep everybody safe from COVID-19 or the next pandemic. I think we ought to focus on making American-made products.

What do you think about the need to build an American-made stockpile and also put ourselves in a position that American companies have the ability to ramp up when we have the next pandemic?

General VOTEL. Thanks, Senator. As we have discussed a little bit previously, I think it is really important that we understand what are the critical resources, what are the critical supplies that we must have on hand. Then once we identify what those are, then we have to look at the sources of those. Certainly we have to be very careful about dependencies on countries like China or critical resources that we need in terms of an emergency, and we need to look at where those supply chains go. Producing them in the United States or perhaps producing them in friendly allied countries are certainly options that we ought to look at in this, but I absolutely agree with you, and the report recommends that we look very closely at where these supply chains take us, particularly with these critical resources that we need in times of emergency.

Senator SCOTT. We have seen Russia and we have seen Communist China try to steal sensitive data. What do you think our Federal Government ought to be doing in conjunction with our business community to make sure that we deal with our biggest cyber threat, which I think clearly part of it is Russia, but I think with the economy that China is building, it appears to me that our biggest risk will continue to be China?

General VOTEL. Senator, I would invite Mr. Capps to address this as well, but what I would just say to you is that we should look at these as serious threats, that we would protect our borders from these type of things, and there needs to be more focus from the Federal Government in helping protect some of our private companies and the data and the technology that they have.

Mr. CAPPS. Yes, sir, I would agree with that. I think the notion of protecting our private enterprises—some of our most valuable assets are exactly there. I worry about us not taking the time now and the massive expense it will take to re-shore technology like, let us say, Internet of Things. If we allow China to keep making that at cheaper rates, selling it cheaply in the United States, they are just getting better and better and better. We can argue about who has the better position in artificial intelligence or computing. It does not matter. Their velocity is faster than ours. They are putting \$1.4 trillion into networks in AI over a 6-year period. We will fall behind as long as we are sending our money to them for innovation, and that is something we are going to have to solve. It is a very big problem.

Senator SCOTT. What do you think about the idea—it might be outside of your purview, but I have a bill that requires companies like Amazon and other online resellers to disclose country of origin, because Americans are fed up with China. If you look at the national polls now, people realize what China is doing. But companies like Amazon will not disclose the country of origin of products, so it makes it very difficult when you are buying a product to know where it is from. When we buy products from China, we just keep

building their economy so they can use it eventually to dominate us. What do you think about—

Mr. CAPPS. It is, of course, outside of my technical expertise area, but I absolutely agree with the notion of disclosure. As a small business, I need to know who I feel comfortable taking money from, and finding the Chinese LPs that are supporting that venture capital firm that are the ones that are funding my company is nearly impossible. The same issue happens with provenance of data. Where did it come from? Was that done in a responsible manner, that it fits the way we like to operate our freedoms in this country, and then for manufacturing, same exact thing. Do not tell me to “Buy American” and then tell me I cannot figure out how to do it.

Senator SCOTT. Yes, you cannot figure out how to do it. I thank each of you for being here.

Senator HASSAN. Thank you, Senator Scott.

We do not have any other Senators who have signed on for either a first or second round of questions, and we are going to have votes in a few minutes. I am going to call the Subcommittee hearing to a close, noting that we did not get to a couple of topics that I will submit for the record concerning particularly financial accountability in disaster response and IT modernization, both of which are issues that the commission addressed, and I look forward to the written responses.

I would like to thank all of our witnesses for appearing before the Subcommittee today. Thank you, General Votel, Mr. Fugate, Ms. Rogers, and Mr. Capps, for your testimony and for answering our questions. I appreciate the work of all the BENS commissioners and the BENS staff in crafting the report.

With unanimous consent (UC), I ask that a copy of the report be included in the hearing record.<sup>1</sup>

The Emerging Threats and Spending Oversight Subcommittee will continue to look at emergency preparedness and emerging threats and hold further hearings and take legislative action when and where it is needed.

With that, the hearing record will remain open for 15 days, until 5 p.m. on April 8th, for the submission of statements and questions for the record.

The hearing is now adjourned. Thank you all very much.

[Whereupon, at 11:24 a.m., the Subcommittee was adjourned.]

---

<sup>1</sup>The report referenced by Senator Hassan appears in the Appendix on page 32.



# A P P E N D I X

---

## **HSGAC Subcommittee on Emerging Threats and Spending Oversight Chair Maggie Hassan Opening Statement As Prepared March 24, 2021**

Good morning. I want to thank our witnesses for joining us today, and for volunteering to serve on the Business Executives for National Security (BENS) Commission on the National Response Enterprise. The Commission's purpose was to bring former government leaders together with business executives to find ways to better prepare for, and respond to, future crises. Thank you all for answering that call to service.

I also want to thank Senator Paul as well as his staff, for working together with me to hold the Emerging Threats and Spending Oversight subcommittee's first hearing of the 117th Congress. I look forward to working together to address the emerging national, economic, and homeland security threats facing the United States, and identifying ways to prevent waste, fraud, and abuse related to federal spending. I will work with Ranking Member Paul and all of my colleagues on the committee on a bipartisan basis to make our country safer and more fiscally responsible.

The Business Executives for National Security was founded nearly 40 years ago as a national and non-partisan organization to bring senior, private-sector executives together with government policymakers to discuss business challenges faced by public and private sector organizations dealing with national security issues. While some members of the Business Executives for National Security have previously served in government, many have spent much or all of their careers in the private sector, and bring fresh perspectives to pressing national security issues.

In the summer of 2020, with the United States and the rest of the world battling the Covid-19 pandemic, the organization convened a Commission on the National Response Enterprise. They brought together some of the most respected and accomplished leaders from government and corporations to research and analyze many of the factors that lead to effective emergency preparedness and response. The Commission was prompted to make sure that it did not view issues too narrowly through the lens of the current pandemic, but to understand what needs to be done to improve preparedness and response to virtually any type of future crisis, whether it be a pandemic, natural disaster, a coordinated cyberattack, or an act of terror.

The BENS Commission was co-chaired by Jeh Johnson, the former Secretary of Homeland Security; Alex Gorsky, the Chairman and CEO of Johnson & Johnson; and Mark Gerencser, the former managing director of Booz Allen Hamilton, and the BENS Chairman of the Board. 33 additional Commissioners from government, business, and civil society joined these co-chairs, in

1

addition to General Votel, the President and CEO of BENS, to identify ways to increase U.S. resiliency for future crises. I was honored to be included in this process as a guest to provide a congressional perspective alongside my colleague, Senator Cassidy, who is also joining us today.

In just a few months, the Commission interviewed 165 government, private sector, and other stakeholders, and develop 11 recommendations for ways to improve our preparedness and response capabilities. The Commission's recommendations focused on 3 key areas: facilitating communication and coordination, delivering supplies and volunteer resources, and leveraging emerging technology. Recommendations range from amending the Stafford Act to include pandemics, cyber events, and other emergencies of extended duration, to expanding the inclusion of non-traditional partners by DHS and FEMA in response efforts. The Commission also recommended consistent and pervasive exercises across the emergency response enterprise, and enhancing stockpile resilience by investing in cutting-edge technology that can enable real-time information sharing and rapid decision-making.

The Commission's report and the testimony provided today will provide a foundation for action for this subcommittee. I will work with the Commission, Senator Cassidy, and the members of the subcommittee to introduce legislation to address the issues we will discuss today, to better prepare communities all across the United States to manage future crises.

**Statement of General Joseph L. Votel (USA, ret.)  
President & CEO, Business Executives for National Security  
before the Subcommittee on Emerging Threats and Spending Oversight  
Senate Committee on Homeland Security and Governmental Affairs  
on “Preparing for Future Crises: Examining the National Response Enterprise”**

**March 24, 2021**

Good morning Chairwoman Hassan, Ranking Member Paul, and distinguished members of the Subcommittee. Thank you for the opportunity to appear before you today to discuss the work of the *Commission on the National Response Enterprise*, which was convened by Business Executives for National Security (BENS) in June of last year.

With your permission, I will begin with an introduction to BENS. Business Executives for National Security is a national, non-partisan organization of senior executives who volunteer their time and talent to address business-related challenges faced by organizations across the national security enterprise. Since its founding in 1982, BENS’ members have responded to requests for assistance from military and government partners by sharing expertise, recommendations, and best practices from their own experience in the private sector, as well as by proactively identifying and offering insights, perspectives, and advice on security objectives.

We will all remember, just over a year ago, being constantly barraged by 24-hour news cycles filled with stories about skyrocketing numbers of COVID diagnoses and deaths around the country; about the devastating toll of the pandemic on the U.S. economy; and about supply chain problems for everything from toilet paper to PPE and respirators to qualified medical personnel. Most Americans were understandably left feeling frightened, helpless, and many hopeless. In these news reports, though, our BENS recognized business challenges similar to the ones they grapple with every day and saw an opportunity to use their experience and expertise to help -- if not immediately, than to strengthen the Nation’s response to future crises.

With that goal in mind, BENS launched the *Commission on the National Response Enterprise* to create what we believed would be a new model for emergency response to strengthen U.S. resiliency through enhanced coordination, communication, and cooperation between all levels of government, business, and civil society. We pulled together 33 Commissioners representing all three of these sectors to work this issue -- former senior military leaders, CEOs of some of the most respected American corporations, a former cabinet secretary, a Nobel laureate, former White House homeland security advisors, members of Congress and state and local leaders.

Joining our Commissioners in this effort were 58 additional business leaders who interviewed 165 government, private sector, and civil society stakeholders and researched five critical

components of emergency response: Roles, Surge, Supplies, People, and Infrastructure & Economy.

I'd like to take this opportunity to especially thank Senators Hassan and Cassidy for their support, deep knowledge and guidance throughout the Commission's 90-day work period and in the months since.

Following all of this research and analysis, the Commission concluded that the Nation does NOT, in fact, need a new model of emergency response -- the components of an integrated national response capability are essentially in place within the US National Response Framework (NRF). However, very significant execution challenges do exist, particularly when a crisis impacts numerous states simultaneously, with limited time to acquire and pre-position needed supplies and other resources.

Throughout the response to COVID-19, gaps and breakdowns in systems and operations disrupted communication, impeded coordination, and negatively impacted surge and supply chains for critical goods and services among stakeholders across all sectors. In short, they 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."

Unless these weaknesses are addressed, future pandemics, natural disasters, coordinated cyberattacks, or acts of terror will have enormous potential to again imperil our citizens, cripple our infrastructure, threaten our economy, and put our national security at risk. Now is the time for transformational thinking about emergency response strategy, policies, and processes.

The final report of the *Commission on a National Response Enterprise, a Call to Action*, offers 11 recommendations for ways in which we should reimagine and redesign our response capabilities to reflect and embrace 21st Century realities in how the Nation handles crises that affect the country's entire fate. These recommendations are focused in three areas: facilitating communication and coordination, delivering supplies and volunteer resources, and leveraging emerging technology.

The *Call to Action* has been submitted for inclusion in the record so I won't take up time in walking through all 11 recommendations. Instead, I highlight for your awareness several actions embedded within the recommendations which appear particularly relevant to the Subcommittee's mission areas. These include:

- Amending the Stafford Act to include pandemics, cyber events, and other emergencies of extended duration or with possible nationwide impacts.
- Requiring biennial delivery of a National Emergency Response Strategy by the Secretary of Homeland Security.



- Establishment of expense-reporting authority for all emergency-related response spending by the Federal government.
- Re-design of FEMA's National Response Coordination Center to link responder networks and help create a common operating picture for all stakeholders.
- Expanding inclusion of non-traditional partners by DHS and FEMA in response efforts.
- Creating 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.
- Development of 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.
- Enhancing 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.
- Developing a strategy, framework, secure capabilities, and the computational resources necessary to guide 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.
- Exploration of targeted protections for organizations and businesses asked to share information and data with governments during times of crisis.
- Driving and incentivizing IT modernization by the federal agencies and departments that are part of the National Response Framework, as well as efforts to migrate state and local legacy systems to new, secure platforms capable of integration across the NRF.
- The establishment of consistent, pervasive testing and exercising across the emergency response enterprise.

Should the members of the Subcommittee have questions about these points or any of the other material included in the *Call to Action*, I am accompanied today by three experts from the Commission who have deep subject matter knowledge related to FEMA; surge and supply; and data and tech. They are: Former FEMA Administrator Craig Fugate; Ms. Kristi Rogers, Managing Partner of Principal to Principal LLC; and Michael Capps, CEO, Diveplane Corp. and former President of Epic Games.

Senators, we cannot change what has already occurred—but, going forward, we can commit to do better. BENS hopes the Commission's *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. We stand ready to work with the members of the Subcommittee, the full Committee, and any other interested members of the House of Representatives and the Senate in moving the Nation toward this critical goal. Thank you.

Findings and Recommendations  
of the BENS

**Commission on the  
National Response  
Enterprise:  
A CALL TO ACTION**





## 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 Paulson**  
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

<b>Executive Summary</b>	1
<b>Supporting Explanations</b>	8
<b>Finding #1: Facilitating Communication and Coordination</b>	8
<b>Recommendation #1:</b> Create Transparent Emergency Response Roles, Strategy, and Spending	9
<b>Recommendation #2:</b> Strengthen Responder Relationships	10
<b>Recommendation #3:</b> Link Responder Networks to Enable a Common Operating Picture	11
<b>Recommendation #4:</b> Expand Inclusion of Non-Traditional Partners	12
<b>Recommendation #5:</b> Prioritize the Exercising and Testing of Plans	13
<b>Finding #2: Delivering Supplies and Volunteer Resources</b>	14
<b>Recommendation #6:</b> Maximize Surge and Supply Capabilities	14
<b>Recommendation #7:</b> Harness All Available Skills and Support	16
<b>Finding #3: Leveraging Technology</b>	18
<b>Recommendation #8:</b> Improve Ability to Access, Use and Share Information and Data	18
<b>Recommendation #9:</b> Connect Every American	19
<b>Recommendation #10:</b> Expand Access to the Benefits of Emerging Technologies	20
<b>Recommendation #11:</b> Keep Pace with Security and Technology Advances	20
<b>Acknowledgements</b>	23



## 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 with-

out 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.

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.

**The Federal government must lead the way to better define and establish clear lines of communication and coordination during 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 transportation, 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 community 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 "BlackSky" 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, potentially 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 non-partisan, 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	Max Kelly Co-Founder & CEO, [redacted]	Roy Shaposhnik Owner, RS Logistical Solutions
John Huntz Managing Partner, Huntz & Co. – Co-Chair	Doug Kitani CEO & Director, Erickson	Jeff Stone Chairman, Indigo BioAutomation
Mandy Cavanaugh Owner, Team Housing Solutions	Suzet McKinney CEO & Executive Director, Illinois Medical District	Glenn Vogel CEO, Espire Services
Jim Evans President, Sevan Multi Site Solutions	Sean Murphy Managing Director, BDO USA	Rory Yancheck Vice President, 3M Company

### WORKING GROUP 2: SUPPLIES

Stan Walz President & CEO, Vector CSP – Co-Chair	Roosevelt Giles President & CEO, Endpoint Consulting LLC	Carrie Kinsler Chief Executive Officer, TXR Logistics
Major General Jim Hodge (ret.) President, Institute for Defense and Business – Co-Chair	VADM. Mark Heinrich (ret.) Founder & Managing Director, Oakleaf Partners	Jeff Lucas Office of Senator Bill Cassidy (R-LA)
Bill Banta General Manager, Enterprise Solutions	Andrew Hersh Head of Critical Infrastructure Resiliency, Lockton Companies	David O'Brien Senior Vice President & Chief Supply Officer, Exelon
Len Botkin Global Corporate Services Executive, Bank of America	Ellen Houlihan Lecturer on Effective Leadership, Catalyzer	Fred Roberts Director, Comman, Control, and Interoperability Center for Advanced Data Analysis, DHS Center of Excellence
Jeff Campbell Vice President, the Americas, Global Government Affairs, Cisco	Beth Jones Managing Director, Center for Accelerating Operational Efficiency, DHS Center of Excellence	Maria Sierra Office of Senator Bill Cassidy (R-LA)
Catherine H. Crawford, PhD IBM Fellow, Research, IBM Corp.		Ben Trowbridge Managing Partner, Acelros

**WORKING GROUP 3: PEOPLE**

Roger Shedlin, MD, JD Principal, CEO & Chairman, OrthoNet – Co-Chair	John Carder Vice President, Information and Technology, & Chief Information Officer, Messer Construction Co.	Matthew Lawlor Executive Chair, Ceca Foundations
Chris Smith Principal, Business Consulting, Grant Thornton LLP – Co-Chair	Catherine H. Crawford, PhD IBM Fellow, Research, IBM Corp.	Brendan Marshall Founder, Flow
Stephen Baum President, The Point Group Network LLC	Scott Drach Vice President, Human Resources, Boeing Defense, Space & Security	Steve Mathias Vice President, Global Military Sales and Strategy, Bell
Jim Brown Founder & General Partner, Arena Growth Partners	John Driscoll CEO, Carecentrix	John McCartney Chairman, Huron Consulting
		Chip Whitaker Executive Vice President, Metis Solutions

**WORKING GROUP 4: INFRASTRUCTURE & ECONOMY**

Sam Cole Principal, Stonecutter Ventures – Co-Chair	David Christian Executive Vice President (ret.), Dominion Energy	James Smith Senior Managing Director, Ankura Consulting
Chris Marlin President, Lennar International – Co-Chair	Catherine H. Crawford, PhD IBM Fellow, Research, IBM Corp.	Chris Vincze CEO, TRC Companies
Steve Cannon CEO, AMB Group	Dan Hesse Former CEO, Sprint	Samuel Visner Director, National Cybersecurity FFRDC, MITRE
Mike Capps CEO, Diveplane	Dan Holland Managing Director, Goldman Sachs	Mark Wassersug Chief Operating Officer, Intercontinental Exchange
Paul Cheng President, Famecast Media	Frank LaPrade Chief Enterprise Service, Officer Capital One	

**WORKING GROUP 5: ROLES**

Thurbert Baker Former Attorney General, State of Georgia – Co-Chair	David Bonfil CEO, ACME General Corp.	Murang Pak President & CEO, Global Risk Advisers
Chris Musselman Head of US Commercial Business, Palantir Technologies – Co-Chair	Edward Davis Founder, Edward Davis Company	Riaz Siddiqi Chairman, Clovis Point Capital
Lauren Bedula Senior Vice President, Beacon Global Strategies	Christopher Frech Senior Vice President, Global Government Affairs, Emergent BioSolutions	Anthony Vinci Managing Director, Cerberus Capital Management
Alfred Berkeley Chairman, Princeton Capital Management	Lori Hennon-Bell Vice President, CSO, Prudential Financial	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	Steven E. Darnell President & CEO, SPG International, LLC	Bruce E. Mosler Chairman, Global Brokerage, Cushman & Wakefield, Inc.
Raphael Benaroya Managing Director, Biltmore Capital Management, LLC	John K. Hurley Managing Partner & CIO, Cavalry Asset Management	William "Bill" F. Murdy Chairman, Thayer Leader Development Group
Denis A. Bovin Senior Advisor, Evercore Partners, Inc.	Ramon P. Marks Sr. Partner (Ret.), Arnold & Porter, LLP	
Norman "Norm" C. Chambers Former Chairman, NCI Building Systems		

**BENS STAFF**

Sean Berman Senior Associate, Policy/Projects	Debbie McCarthy Senior Vice President, Engagement & Strategy	David Smith Research Associate
Peter Crail Director, Policy/Projects	Nicole McCloskey Research Associate	James Whitaker Vice President, Emerging Challenges
Sally Hayes Research Associate	Patrick Sweeney Vice President, Member Engagement	Sean Withington Research Director, Emerging Challenges
Courtney Joline Director, Policy/Projects	Caroline Preston Senior Policy Associate, Policy/ Projects	Aaron Woolf Vice President, Policy/Projects
Samantha Kirsch Policy Associate, Policy/Projects	Noah Riley Research Associate	
Clinton Long Senior Director, Publications/ Communications		







**Business Executives  
for National Security**

1030 15th St. NW • Suite 200 East  
Washington, DC 20005  
[www.BENS.org](http://www.BENS.org) | 202.296.2125  
Twitter: @BENS\_org