THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

Mr. John Donovan
NSTAC Chair
6306 Norway Road
Dallas, Texas 75230

September 14, 2020

The Honorable Donald J. Trump
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Dear Mr. President:

As the Administration considers the long-term impacts of the Coronavirus pandemic (COVID-19) on U.S. networks and the American way of life, the President's National Security Telecommunications Advisory Committee (NSTAC) seeks to provide analyses and immediate-term guidance to the Administration on how to strengthen the resiliency of the Nation's Information and Communications Technology (ICT) infrastructure. The purpose of this letter is to report on ICT resiliency during COVID-19 and recommend steps that the Administration take to ensure the resiliency of U.S. national security and emergency preparedness (NS/EP) communications. While the overall ICT ecosystem response to the pandemic was strong, this letter highlights three areas for improvement that could support the Nation's resiliency moving forward.

Specifically, the NSTAC recommends the following:

1) The U.S. Government should modify protocols and hierarchical responses for multi-region or large-scale events to ensure consistent communications across the federal, state, local, tribal, and territorial (FSLTT) levels.
2) The U.S. Government—the Executive Office of the President (EOP) and the Cybersecurity and Infrastructure Security Agency (CISA) in particular—should communicate and reinforce the responsibilities of enterprise leaders to ensure their employee home-points and—by extension—enterprise networks, systems, and cloud-based services, are secure, thereby upholding the national security imperative and delivering broad economic benefits.
3) The Administration should utilize and expand existing federal funding database capabilities to identify and leverage all FSLTT funding or resourcing tools available to expedite delivery of future-ready broadband access to the Nation.

BACKGROUND: Now more than ever, the stability of the U.S. economy is contingent on the reliability, security, and integrity of the ICT ecosystem—which has historically demonstrated great resilience during large-scale incidents. ICT industries have a long history of planning for disaster response and recovery. Before the COVID-19 pandemic, events like the 2019 California wildfires

and Midwestern floods, 2012 Superstorm Sandy in the Northeast, 2005 Hurricane Katrina on the Gulf Coast, and September 2001 attacks on the United States presented obstacles to effective cross-sector communications, coordination, and response.

The nationwide scale of the COVID-19 response presented its own unique and unprecedented challenges. The ICT sectors' response focused on two key areas: 1) provisioning additional capacities and capabilities for customers, who were also scaling their systems to work and learn from home; and 2) managing rapidly changing volumes and usage patterns of traffic globally. Despite the challenges, reliable and distributed connectivity was maintained across the United States and important lessons were learned around improving national coordinated response to incidents of this scale and persistence.

The NSTAC received 19 briefings from subject matter experts representing various facets of the ICT ecosystem (see *Appendix: NSTAC Communications Resiliency Subcommittee Briefer References* for the full list). Briefers included: communication service providers; ICT and cybersecurity vendors; cloud and application platform providers; sector representatives from energy and financial services; user communities, such as healthcare and education; and organizations and government agencies responsible for cybersecurity measures. The statements and assertions made in this letter are based on the NSTAC's findings from these briefings, unless otherwise noted. For the purposes of this letter, the "COVID-19 analysis period" is defined as a roughly 5-month period from early March 2020 through July 2020.

Factors Supporting ICT Resiliency:

ICT within the United States maintained a high-level of performance and resilience through the first 5 months of COVID-19. During the assessment period, peak network traffic demand shifted in location, time of day, duration, and the types of services leveraged as working from home (WFH), telehealth, and distance learning increased. USTelecom members reported an average usage increase of 25.7 percent early in the COVID-19 period, which more recently leveled off at a 10 percent increase.[1] CTIA, which represents the U.S. wireless communications industry, reported that its mobile operator members experienced a 19.6 percent increase in data traffic, 24.3 percent increase in voice traffic, and 25 percent increase in texting.[2] Consistent with societal isolation strategies, increase in mobile data usage was also accompanied by a decrease in mobile subscriber movement, with a 25 percent initial reduction that has since tapered to a 14 percent reduction.[3] While overall traffic demand and utilization increased greatly, the geographic distribution of that demand also changed dramatically. U.S. network infrastructure, which is designed to support peak capacity demands, served the needs of the Nation well. **Several factors contributed to the strong performance of the U.S. ICT ecosystem during this nationwide event:**

Capital Investments. Historic and ongoing investments in the ICT infrastructure, products, and services played a major role in the resilience of operations during COVID-19. These investments enabled information technology (IT) and communication companies and their suppliers to respond quickly to the rapidly changing traffic behavior. Among other capabilities, these ongoing investments had 12 to 18 months of projected growth capacity in transport, content delivery networks, and data centers built in, strengthened and diversified supply chains, and deployed architectures that leveraged next generation technologies to support network agility, resiliency and traffic load balancing.

Societal isolation strategies led to a massive increase in video consumption, live streaming, and videoconference applications and the ICT infrastructure demonstrated the ability to support these services along with the increased use of WFH, telehealth, and distance learning platforms. Additionally, many major platform providers own and operate global network infrastructure separate from the public internet. Traffic increases across those commercial private infrastructures enabled high capacity and dedicated global connectivity, circumventing the need to send traffic over the public internet. Private infrastructure has connection points with the public internet and directly with end customers via dedicated connections.

Using deployed software-defined network technology, the platform providers responded to congestion on the public internet by routing traffic to interconnects that delivered the best route performance, dynamically prioritizing traffic by throttling data and caching the data at distributed edge locations to relieve congestion further.

The increase in online collaboration tool use created significant two-way bandwidth demands. Platform providers mitigated this by using their own content delivery networks as well as integrated adaptive bit rate (ABR) technology to adjust video quality automatically to adapt to dynamic traffic conditions and device types. For example, a major search engine changed its ABR behavior to default to standard definition rather than high definition at video start and then dynamically adjusted the video quality based upon network conditions. In another example, personnel from a major content service provider based in the United States reported that, while they capped subscriber bit rates at the request of some operators in other regions of the globe, the network capacity and agility investments in the United States made that decision unnecessary for domestic connections.

Planning. While not all service providers had pandemic-specific plans, most of the ICT sectors had established business continuity plans that featured WFH elements, which were executed proactively and quickly amidst the pandemic. Several briefers reported that their workforces were able to transition almost entirely to a remote environment in a relatively short time with little to no disruption in service delivery or operations. This was evident in the report from NCTA – the Internet and Television Association, that 97 percent of their members' workforce ended up working from home.[4]

Sector-Peer Resiliency. The communications, finance, and energy sectors have historically leveraged business continuity and disaster recovery (BC/DR) planning, as well as intra- and inter-sector processes to coordinate response and recovery plans, including conducting periodic exercises. Both the finance and energy sectors cited these efforts as aiding their COVID-19 response operations. While they did not contemplate 100 percent sustained WFH scenarios in their plans, the existing plans enabled swift action and proved adaptable as challenges arose. The Securities Industry and Financial Markets Association reported that more than 90 percent of financial staff moved to WFH early on and will continue to do so for the foreseeable future.[5] While there were some initial issues in scaling enterprise system capacity as employees shifted to WFH and adjusted for end-user capabilities, they were quickly remediated within these sectors. The resiliency of the energy and finance sectors, as well as other key critical infrastructures sectors, minimized the need to address external factors and allowed ICT industries to focus solely on assuring their own operations and supporting their customers.

ICT Supply Chain. While short-term disruptions were experienced in personal protective equipment (PPE) and WFH and distance learning equipment (e.g., laptops, monitors, cameras, mobile hot spots), in general the diversified supply chains that support the ICT industry were stable as noted by numerous ICT briefers. The Department of Homeland Security (DHS) ICT Supply Chain Risk Management Task Force is examining possible mid- to long-term supply chain impacts on a broader scale due to COVID-19; they expect to complete the review by the end of 2020.[6]

Information Sharing and Response Coordination. Existing information sharing and response mechanisms used amongst the ICT industries and in coordination with the U.S. Government provided an important foundation for the successful execution of business continuity strategies as well as continued operations through the COVID-19 analysis period. Response support from the U.S. Government was, and remains, critical. Such support included DHS *Guidance on Essential Critical Infrastructure Workforce: Ensuring Community and National Resilience in COVID-19 Response*, which supported the ICT's ability to continue to provision, repair, and sustain operations.[7] Furthermore, direct dissemination of PPE to key sectors amidst early COVID-19 response when supply chains were disrupted, was also a critical factor in maintaining the performance of ICT network infrastructure. Finally, the cross-sector information gleaned from Emergency Support Function (ESF) #14, Long-Term Community Recovery, provided insights of value to the ICT representatives, who are members of ESF #2, Communications.[8]

Cyber Readiness. Cybersecurity events targeted at ICT providers, enterprises, or networks were not significantly different in scope or impact than those experienced pre-COVID-19. However, phishing attacks targeting ICT customers increased greatly as malicious actors shifted to leverage COVID-19 themes and targeted popular technology. The mass adoption of collaboration platforms over a short period of time was an observed COVID-19 related target. Incremental security measures were added to certain collaboration platforms in order to mitigate early COVID-19 cyber events and vulnerabilities; these will continue to be updated as platforms continue to play a major role in supporting remote work.

In summary, the investments and technology advancements of the IT and communications sectors, coupled with practiced execution of BC/DR plans, allowed the ICT ecosystem to adapt and rapidly change in response to dynamic conditions. The COVID-19 response differed from earlier large-scale events, as there was no physical destruction of infrastructure (e.g., hurricanes). The response also differed in that the Nation needed to rationalize the conflicting strategy of imposing isolation policies to respond to the public health crisis, while concurrently promulgating a newer and far broader classification of essential workers, who continued working to support the isolated population. This response stressed the incident management protocols and processes at a scale previously untested to date and—while many successes were realized—it did reveal unexpected gaps in preparedness and capabilities that should be addressed.

Areas for Improvement:

The COVID-19 response uncovered areas for improvement in disaster response coordination and alignment to better ensure nationwide unity of messaging and effort. The nationwide scope of the COVID-19 response provided insights into whether governmental response protocols were able to scale to meet the country's needs. NSTAC briefers identified three high-level areas that the Government should review for potential modifications to prepare the Nation better for any future widescale event:

Messaging Alignment Across All Levels of Government: During the early stages of the pandemic, there was inconsistent messaging from various federal actors, such as the Federal Emergency Management Agency (FEMA), Department of Health and Human Services, Centers for Disease Control and Prevention, and the EOP, on several important issues. Such issues included PPE use, sourcing, and distribution; essential worker definitions and access procedures; and safe working guidelines. This was further complicated by states' and municipalities' differing interpretations of the information. Attempts to reconcile these conflicts, particularly by ICT companies that operate throughout the country, added delays and created significant uncertainties in developing risk-based response plans to ensure continued ICT operations.

NSTAC fully acknowledges that response to a crisis is generally "locally-executed, state-managed, and federally supported,"[9] but variances in FSLTT guidance during national or multi-regional events are an impediment to whole-of-Nation mobilization. When circumstances require state or regional variances, the rationale for such variance should be communicated clearly and a single federal entity should act as a definitive source for those differences. Efforts undertaken now to ensure that government at all levels can create and convey unified messaging and courses of action would serve the resiliency of the Nation well should Americans be confronted by a future nationwide incident that is accompanied by destruction of critical infrastructure.

Issue Resolution: Every large-scale incident has the potential to raise unanticipated challenges that often must be addressed and mitigated by on-the-ground teams. Given the scale of response during COVID-19, new challenges presented themselves in unique and unforeseen areas with no clear-cut guidelines or processes to ensure rapid, aligned government approvals. If these issues had developed in the context of a single FEMA region disaster, the ESF #2 mechanism would generally have been leveraged to drive resolution. This national, all-region incident did not have such a mechanism.[10] While issues uncovered were ultimately addressed, an upfront, well-understood process for bringing locally-discovered, incident-specific, national-impact problems to the forefront for resolution should be an additional area for future review. Moving forward, the U.S. Government should revise protocols to create a process to bring whole-of-Nation issues to the forefront for rapid and coordinated resolution and ensure they are clearly communicated.

Essential Workers: DHS's guidance to state and local governments on critical infrastructure services was essential and helped immensely in those jurisdictions that adopted it. However, ICT providers noted that certain government functions, such as local permitting and inspection services, were not recognized as "essential" in the early days and delayed initial response activities. Moving forward, the COVID-19 response provides the opportunity to review, refine, and expand what types of services and activities are "essential," not only in the private sector but in the public sector as well. When reviewing the preceding recommendations on messaging alignment and issue resolution, the U.S. Government should consider and adjust as well for any revisions to essential workers, services, or activities.

The rapid transition of enterprise workloads to home environments has elevated the risk of cyber threats in ways that enterprises may not have fully addressed or mitigated. The

cybersecurity attack surface changed dramatically as COVID-19 drove businesses and governments to send employees home to continue operations. The massive shift to WFH during COVID-19 constituted an expansion of the ICT enterprise attack surface, highlighting security challenges in protecting critical infrastructure and data. While great efforts have occurred in enterprises over the years to harden and protect their own infrastructure, COVID-19 forced an extension of the infrastructure to the employees' homes overnight. This rapid shift to working from unsecured and unmanaged environments (IT, Internet of Things, mobile, cloud, etc.) has provided opportunities for malicious activities across threat vectors and at a scale not seen before.

Many enterprises were not prepared for their entire workforce to work remotely, or for personal devices and applications suddenly to be used to connect with core business systems. Since initial enterprise problems included procuring the devices, access, and network capacity to provide basic operational functionality, cybersecurity concerns were not wholly addressed and may have left both the remote workforce and the core business systems vulnerable.

Enterprise and government leaders increasingly recognize the need to extend the same security capabilities traditionally deployed within internal networks to all environments, regardless of the location from which an employee connects. Such threats targeted at the work from home environment were known, as evidenced by the more than 50 COVID-19 related cyber activity alerts released by the Federal Bureau of Investigation and DHS during this time.[11,12] Nonetheless, it is not clear whether the majority of non-ICT enterprises fully understand or have mitigated these risks.

Government and enterprise leaders should not view WFH or work-from-anywhere as a fleeting trend. In many ways, COVID-19 merely accelerated network transformation and workforce flexibility trends that were already in motion, which will likely continue in some form long after the pandemic recedes. To address this reality, the U.S. Government—the EOP and CISA in particular—should publicly communicate and reinforce the responsibilities of enterprise leaders to ensure their employee home-points and—by extension—enterprise networks, systems and cloud-based services, are secure, thereby upholding the national security imperative, and delivering broad economic benefits.

Access to broadband is a pre-requisite to fully leverage the digital economy and support national resilience goals associated with economic continuity. As noted, some critical infrastructure sectors had developed pandemic plans more than a decade ago in response to concerns about Avian Flu.[13] While some of the factors associated with the COVID-19 outbreak were significantly different than those for Avian Flu, these early plans led to insights that recognized WFH strategies could be a significant tool in an enterprise BC/DR plan. Since that time, the ICT environment has also changed significantly, punctuated by broader access to and deeper adoption of ICT capabilities at all levels, from consumers to major institutions. This access and adoption played a major role in the United States' economic resilience to the current pandemic. The degree to which the country was able to leverage the ICT ecosystem to support the economy while in physical isolation reflects the progress the Nation has achieved towards becoming a more digital economy. When coupled with the efforts that DHS and CISA took to recognize and expand the understanding of essential worker functions, the Nation demonstrated societal and economic resilience at a macro level. As noted in the March 2020 findings of the Cyberspace Solarium Commission, the continuity of the digital economy is a major factor in supporting the country's

NS/EP posture.[14] This insight provided the foundation for NSTAC to consider the impact of economic resilience on NS/EP communications.

Telehealth and distance learning are two representative scenarios used in the study to understand the challenges of transitioning traditional in-person activities to equivalent remote functions based on support from ICT services. The use of these two services has grown exponentially throughout the pandemic. Unlike the WFH environment, the end-user or recipient of these services is not known in advance, nor do they remain constant. The key enabler to leveraging such services becomes the user's access to broadband. Unfortunately, a significant number of individuals are unable to participate effectively in important services due to lack of broadband access, inadequate bandwidth, and/or financial constraints. This event reinforces the need to rapidly address the digital equity and digital inclusion issues facing the Nation to increase national security and resilience. NSTAC's focus however, will remain primarily on access concerns, only minimally on bandwidth constraints, and will not include financial aspects to operate within the parameters of the committee's charter.[15,16]

> **Telehealth:** Pre-COVID-19, telehealth practices were primarily limited to the delivery of care between rural hospitals and clinics and major medical centers. Within days of the early COVID-19 response, a large majority of health services, including primary care, behavioral, and social services, migrated to telehealth options.[17] Internal analysis from the Centers for Medicare and Medicaid Services found that while 14,000 beneficiaries received one telehealth service per week before the COVID-19 analysis period, this increased to over 10.1 million beneficiaries during the analysis period.[18] Despite this surge in telehealth services, usage in rural areas is problematic, primarily manifested as a client broadband availability problem. According to the Dartmouth College Center for Global Health Equity, more than 20 percent of residents in northern New Hampshire and 23 percent of Vermont residents lack access to broadband.[19]
>
> **Distance Learning:** As one briefer commented: "You can't learn online, if you can't get online."[20] ICT used by education institutions has been predominately successful at enabling online learning for the majority of students, but a significant number have been unable to participate because they do not have access to broadband or sufficient bandwidth at home. California State University (CSU) estimated that between five to 10 percent of its 500,000 students (approximately 25,000 to 50,000 students) have essentially no internet access at home. CSU further voiced concerns that current bandwidth speeds may be increasingly inadequate for future distance learning, particularly interactive learning where a higher degree of parity between download/upload speeds is required.[21]

NSTAC briefings highlighted the efforts of wireless, wireline, and cable providers to address the immediate access needs for telehealth, and distance learning. Mobile wireless services, for example, has proven to be an effective and agile solution for distance learning. Moreover, while higher bandwidth speeds may be the goal, the standard is closely coupled with the economics of broadband deployment and has been subject to many Federal Communications Commission (FCC) proceedings over time. Recent FCC actions associated with the upcoming Sixteenth Broadband Deployment Report Notice of Inquiry suggest that the 25/Megabits per second (Mbps) broadband standard (service that has a download speed of 25 Mbps and an upload speed of 3 Mbps) may remain for the immediate future.[22]

Telehealth and distance learning are only two examples of digital economy services that cannot be fully leveraged at this time. Other critical services used throughout the COVID-19 response included product/service ordering, financial transactions, and government service delivery. As noted in the Dartmouth report, "Nothing about a pandemic works if you can't work from home and if your kids can't get schooled."[23] If one assumes that a major pillar in the Nation's economic resiliency is continuity of the digital economy, then access to broadband internet, as the first step, becomes an even more critical goal that must be achieved on an expanded and expedited basis.

Universal access to broadband internet is not a new issue; how to accomplish this goal has been an ongoing subject of analysis and effort for years. The economics of universal broadband access are well understood at all levels of government and the FCC has conducted multiple proceedings in this area associated with the Connect America Fund (CAF), CAF phase II, and the ongoing Rural Digital Opportunity Fund (RDOF).[24] The key impediment to broadband availability in unserved or underserved areas remains the costs associated with initial deployment and ongoing operations, which is a function of greater geographic distance, more challenging terrain, and significantly less subscriber density.

There are numerous Government initiatives underway to address broadband availability, capacity, and related digital equity issues. At the federal level, there are more than 50 broadband programs spanning a dozen federal agencies with billions of dollars for broadband grants, loans, and other resources. Most notably, the FCC spends more than $4 billion per year on CAF phases 1 and 2, RDOF phase 1, the Alternate-Connect America Cost Model, and other initiatives.[25]

States and localities have also been heavily engaged in developing programs. As outlined in the April 2020 Congressional Research Service report, "While many state broadband initiatives focus on broadband infrastructure deployment, some address other aspects, such as adoption, mapping, feasibility, digital equity and digital inclusion." There is a wide diversity in the range of approaches used at the state and local levels, such as direct grants for infrastructure deployment, re-use of existing state and local infrastructure, as well as public-private partnerships (P3), designed to leverage the assets and capabilities of all parties to the stated broadband goals.[26]

With the wide diversity of FSLTT programs, there has been substantive public dialogue on concerns that some areas might receive duplicative funding from multiple broadband programs. This may lead to overbuilding areas already served at the expense of unserved areas, or alternatively directing funds to areas already served, which might further erode the economics of the existing provider.

Since the COVID-19 experience "magnifies the need for actions that make broadband accessible for all"[27] and these unserved areas remain the hardest to address, the universal service goal might be expedited if all governmental initiatives were aligned or cross-leveraged to ensure connectivity first, and then, incremental augmentation to reach broadband standards. Alignment around a stated goal to leverage and/or combine all possible federal, state, and local resources, including P3s, to address these markets collectively should lead to a more beneficial outcome.

In support of aligning these resources, the National Telecommunications and Information Administration (NTIA) has already developed a searchable database of 50 federal broadband programs, spanning a dozen federal agencies with billions of dollars for broadband grants, loans, and other resources. This database fulfills a goal set out in the American Broadband Initiative to

make it easier for state and community leaders to find federal funding and permitting information.[28] The NSTAC applauds NTIA's initiative and suggests it could be a foundation for a more comprehensive system. NTIA should consider including state and/or other opportunities, playing an active role in highlighting conflicts or overbuilding, and identifying potential situations where programs could work together to create or leverage synergies. This comprehensive source could provide an even better mechanism to use the full range of FSLTT and P3 programs to achieve national broadband goals.

In summary, the ICT ecosystem demonstrated a high-level of resiliency and adaptability to the wholesale shift in traffic patterns caused by the COVID-19 response, while maintaining performance and security of the networks that provide enabling functions for the digital economy. Notable factors that contributed positively to the performance of the U.S. ICT ecosystem during this nationwide event include: capital investments; planning; resilience of interdependent sectors; supply chain stability; information sharing and response coordination; and ICT sectors' cyber readiness.

The response to COVID-19 uncovered key challenges and strategic opportunities for improvement: 1) disaster response coordination and alignment across FSLTT should be re-assessed to better ensure unity of messaging and unity of effort for whole-of-Nation events; 2) the transition of enterprise workloads to residential and remote settings has created an environment vulnerable to cyber threats; as such, strengthening the cybersecurity readiness of a remote workforce is critical to ensuring the security and resilience of critical infrastructure as well as the digital economy; and 3) access to broadband to underserved areas is a pre-requisite to fully leverage the digital economy and support national resilience goals associated with economic continuity.

Recommendations:

1. Emergency Preparedness/ICT Resilience (Government Processes):
    a. Government protocols and hierarchical responses for multi-region or large-scale events should be modified to ensure consistent communications across the FSLTT levels. To the extent that state and federal guidelines differ, establish a mechanism whereby a single federal entity can act as the definitive source for such variances.
    b. Further, these revised protocols should ensure a mechanism is established to bring whole-of-Nation issues to the forefront for rapid and coordinated resolution and ensure they are clearly understood.
    c. Continue to refine and promote the identification of essential workers, clarify relevant messaging, and encourage the expeditious resolution of related issues. Review the roles of FSLTT entities to ensure that the functions uncovered at these governmental levels are accounted for as public essential services going forward.
2. National Security (WFH/Enterprise Security):
    a. The U.S. Government—the EOP and CISA in particular—should publicly communicate and reinforce the responsibilities of enterprise leaders to ensure that their employee home-points and, by extension, enterprise networks, systems, and cloud-based services are secure, thereby upholding the national security imperative and delivering broad economic benefits.
3. Economic Security (Digital Equity Issues):
    a. The Administration should utilize and expand existing federal funding database capabilities to identify and leverage all funding or resourcing tools available at the

FSLTT levels to expedite delivery of future-ready broadband access to the Nation.

b. The FCC should continue its leadership and efforts in the following areas towards the goal of broadband access throughout the Nation:
    i. Providing even greater financial support through future phases of the RDOF and other broadband access initiatives;
    ii. Increasing the availability of spectrum, while protecting against harmful interference; and
    iii. Reviewing current broadband standards to ensure deployment of broadband access to the Nation, supporting current and future digital economy needs.

Future Study and Next Steps:

Preparations are underway for phase II of this study, which will incorporate the findings of phase I, address future technological capabilities within ICT and their applicability to NS/EP efforts, and include a review of NS/EP ICT resiliency challenges beyond those realized in recent emergencies.

Sincerely,

(signature)

Mr. John Donovan
NSTAC Chair

[1] Michael Saperstein, "NSTAC Network Performance" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 1, 2020).
[2] Tom Sawanabori, "How Wireless Kept Americans Connected During COVID-19" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 2, 2020).
[3] Noman Alam, "Impact of COVID-19 on Networks in the U.S." (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 16, 2020).
[4] Jill Canfield, et. al., "NSTAC Communications Resiliency Subcommittee Briefing" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 2, 2020).
[5] Ronald Green, Thomas Price, and Thomas Wagner, "Briefing from Security Industry and Financial Markets Association" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 15, 2020).
[6] "Information and Communications Technology Supply Chain Risk Management Task Force," *Cybersecurity and Infrastructure Security Agency*, last modified June 15, 2020, https://www.cisa.gov/ict-scrm-task-force.
[7] "Guidance on Essential Critical Infrastructure Workforce: Ensuring Community and National Resilience in COVID-19 Response," *Cybersecurity and Infrastructure Security Agency*, last modified August 25, 2020, https://www.cisa.gov/publication/guidance-essential-critical-infrastructure-workforce.
[8] "National Response Framework," *Federal Emergency Management Agency*, last modified July 31, 2020, https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response.
[9] Ibid.
[10] Ibid.
[11] Gordon Kirsch and Nicholas Moon, "Cyber Threat Briefing" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 28, 2020).
[12] Ibid.
[13] "Past Pandemic-Related Reports," *U.S. Government Accountability Office*, https://www.gao.gov/coronavirus/past_pandemic-related_reports.
[14] U.S. Cyberspace Solarium Commission, *Cyberspace Solarium Commission Report*, (Washington, DC: March 11, 2020), https://www.solarium.gov.
[15] Elizabeth Carpenter-Song and Anne Sosin, "COVID-19 and Rural Health Equity in Northern New England" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 21, 2020).
[16] Michael Berman, "Telecommunications in the COVID-19 Era: The View from the California State University" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 23, 2020).
[17] Elizabeth Carpenter-Song and Anne Sosin, "COVID-19 and Rural Health Equity in Northern New England" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 21, 2020).
[18] "Trump Administration Proposes to Expand Telehealth Benefits Permanently for Medicare Beneficiaries Beyond the COVID-19 Public Health Emergency and Advances Access to Care in Rural Areas," *Centers for Medicare and Medicaid Services*, last modified August 3, 2020, https://www.cms.gov/newsroom/press-releases/trump-administration-proposes-expand-telehealth-benefits-permanently-medicare-beneficiaries-beyond.
[19] Elizabeth Carpenter-Song and Anne Sosin, "COVID-19 and Rural Health Equity in Northern New England" (Briefing to the NSTAC

Communications Resiliency Subcommittee, Arlington, VA, July 21, 2020).
[20] Michael Berman, "Telecommunications in the COVID-19 Era: The View from the California State University" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 23, 2020).
[21] Ibid.
[22] "Sixteenth Broadband Deployment Report Notice of Inquiry," *Federal Communications Commission*, last modified August 19, 2020, https://www.fcc.gov/document/sixteenth-broadband-deployment-report-notice-inquiry.
[23] Elizabeth Carpenter-Song and Anne Sosin, "COVID-19 and Rural Health Equity in Northern New England" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 21, 2020).
[24] "NTIA Releases Comprehensive Guide to Federal Broadband Funding," *National Telecommunications and Information Administration*, last modified June 3, 2019, https://www.ntia.doc.gov/press-release/2019/ntia-releases-comprehensive-guide-federal-broadband-funding.
[25] Ibid.
[26] Colby Leigh Rachfal, *State Broadband Initiatives: Selected State and Local Approaches as Potential Models for Federal Initiatives to Address the Digital Divide*, (Washington, DC: Congressional Research Service, April 6, 2020), https://crsreports.congress.gov/product/pdf/R/R46307.
[27] Jonathan Spalter, "The State of Broadband Amid the COVID-19 Pandemic" (Testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, Washington, DC, May 13, 2020).
[28] "NTIA Releases Comprehensive Guide to Federal Broadband Funding," *National Telecommunications and Information Administration*, last modified June 3, 2019, https://www.ntia.doc.gov/press-release/2019/ntia-releases-comprehensive-guide-federal-broadband-funding.

Appendix: NSTAC Communications Resiliency Subcommittee Briefer References

Brandon Welch, email message to the President's National Security Telecommunications Advisory Committee (NSTAC), July 30, 2020.

Christopher Butera, "Cybersecurity During the COVID-19 Pandemic" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 28, 2020).

David Fullager and Gina Haspilaire, "Netflix Traffic in 2020" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 14, 2020).

Elizabeth Carpenter-Song and Anne Sosin, "COVID-19 and Rural Health Equity in Northern New England" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 21, 2020).

Gordon Kirsch and Nicholas Moon, "Cyber Threat Briefing" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 28, 2020).

Jill Canfield, et. al., "NSTAC Communications Resiliency Subcommittee Briefing" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 2, 2020).

Loretta Polk and Matt Tooley, "COVID-19: Cable's Response" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 7, 2020).

Mark Ryland, Tom Scholl, and Jordana Siegel, "Briefing from Amazon Web Services" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 22, 2020).

Matt Desch and Tom Stroup, "State of the Satellite Industry" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 8, 2020).

Michael Berman, "Telecommunications in the COVID-19 Era: The View from the California State University" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 23, 2020).

Michael Saperstein, "NSTAC Network Performance" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 1, 2020).

Nasser Elaawar, "Impacts of COVID-19 on Facebook Network Logistics, Supply Chain, and Planning" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 8, 2020).

Noman Alam, "Impact of COVID-19 on Networks in the U.S." (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 16, 2020).

Patrick Flynn and Dave Marcus, "McAfee COVID Global Threat Briefing" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 23, 2020).

Richard Friedel, et. al., "COVID-19 and Broadcast Operations" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 1, 2020).

Robert Huber and Brad Pollard, "Business Continuity, Security, and Resilience" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 22, 2020).

Ronald Green, Thomas Price, and Thomas Wagner, "Briefing from Security Industry and Financial Markets Association" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 15, 2020).

Scott Aaronson, "ESCC: COVID-19 Global Pandemic Response" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 9, 2020).

Scott Deutchman, et. al., "Google Operations, Growth in Products, and Working with Telecom Providers" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 16, 2020).

Tom Sawanabori, "How Wireless Kept Americans Connected During COVID-19" (Briefing to the NSTAC Communications Resiliency Subcommittee, Arlington, VA, July 2, 2020).