USTELECOM | THE BROADBAND ASSOCIATION

October 19, 2020

VIA EMAIL

Gloria Norwood
Defense Information Systems Agency
Defense Information Technology Contracting Organization – National Capital Region
Department of Defense
[redacted]

Re: Request for Information from Industry Regarding Dynamic Spectrum Sharing

Dear Ms. Norwood:

USTelecom[1] appreciates the opportunity to comment upon the Department of Defense's ("Department") request for information ("RFI") on innovative solutions for dynamic spectrum sharing, and it urges the Department in the strongest possible terms to abandon its apparent consideration of owning and operating a national, "independent" 5G network of its own.

Introduction

As USTelecom noted in its response to the Administration's earlier request for comments on the Implementation Plan for the National Strategy to Secure 5G, we are at a critical crossroads in determining how government and industry will together tackle the challenge of deploying secure, reliable 5G across the country.[2] Particularly in light of the unprecedented demands that COVID-19 has placed on the communications networks that enable remote connectivity, this productive and innovative partnership between government and industry is both a national security imperative and also a fundamental prerequisite for U.S. technological and strategic leadership in the 5G era.

With this critical crossroads and the broader National Strategy in mind, it is appropriate to ask industry for its expert insights on how it should approach its currently allocated spectrum in order to accelerate spectrum sharing decisions and to leverage "5G and beyond" technologies for military operations.[3] Almost all of the questions in the RFI pertain to spectrum issues that are crucial to the future of 5G, and we are confident the Department will receive a rich and robust

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives — all providing advanced communications service to both urban and rural markets.

[2] Comments of USTelecom—The Broadband Association, *In the Matter of The National Strategy to Secure 5G Implementation Plan*, Docket No. 200521-0144, RIN 0660-XC047, submitted to the National Telecommunications and Information Administration on June 25, 2020, *available at* https://www.ntia.gov/files/ntia/publications/ustelecom_ntia_comments_on_secure_5g_6.25.20_final.pdf.

[3] *See* comments of Fred Moorefield, Deputy Chief Information Officer for C3, Department of Defense, at FCBA Wireless Telecommunications Committee webinar, *Commercial Wireless in the 3.45-3.55 GHz Band*, Oct. 13, 2020.

record of information about these questions from global industry leaders, many of whom are USTelecom members. Our comments, however, focus on the RFI's first set of questions, namely the following:

> "How could DoD own and operate 5G networks for its domestic operations? What are the potential issues with DoD owning and operating independent networks for its 5G operations?"

These questions rest on a dangerous false premise. The idea that a U.S. government agency might seek to own and operate its own national 5G network would not only reverse decades of the Department's approach to leveraging industry innovation for its complex communications needs, but, further, it would undermine U.S. national security, technological leadership, and economic prosperity in the 5G era. To be blunt, neither the Department nor any other government agency could own and operate such a national network without security risks and technology and cost inefficiencies that would outweigh any possible benefits. Rather than trying to do so, the Department and the federal government more broadly should instead leverage and build on existing models for U.S. government support for private sector innovations in network deployment and operation.

It is our hope that this particular set of questions in the RFI is simply a miscommunication of the Department's intent. Indeed, we have taken heart in recent public comments that indicate that the Department did not wish to imply that it is looking to develop its own national 5G network – that instead, the intent of the RFI is to help the Department "change the game" in spectrum management to allow for the most efficient use of the Department's spectrum.[4] USTelecom strongly supports such efforts to develop innovative spectrum sharing solutions; however, for the reasons outlined below, we categorically oppose any effort to nationalize our country's 5G network infrastructure as apparently contemplated in the RFI.

I. A NATIONAL 5G NETWORK OWNED AND OPERATED BY THE GOVERNMENT WOULD NOT BE A SECURE AND RESILIENT NETWORK BY THE UNITED STATES' WORLD-LEADING STANDARDS.

For decades, USTelecom and its members have played a prominent role in the security, resiliency and innovation of the U.S. communications infrastructure, in close and collaborative partnership with the U.S. government. USTelecom helped the National Institute of Standards and Technology ("NIST") develop the Cybersecurity Framework, and we led the Federal Communications Commission's ("FCC") Communications Security, Reliability, and Interoperability Council's ("CSRIC") landmark effort to implement the Framework in the communications sector. USTelecom also chairs both the Communications Sector Coordinating Council (CSCC) and the ICT Supply Chain Risk Management Task Force (SCRM Task Force), the two principal organizations that serve as the government's industry partners for developing cybersecurity and supply chain security policies.

[4] *Id.* Moorefield stated that any impression that DoD is looking to compete with industry by building its own national 5G network is a "misrepresentation" of the RFI.

More broadly, the roots of the CSCC and its partner organizations – the government-industry National Coordinating Center for Communications ("NCC") and the Communications Information Sharing and Analysis Center ("Comm ISAC"), both housed in the Department of Homeland Security – reach back to the government's need for industry expertise and support in addressing nuclear threats to government communications and continuity of operations during the Cold War era. Likewise, the President's National Security Telecommunications Advisory Committee ("NSTAC"), established by President Ronald Reagan via executive order at the height of the Cold War in 1982, has provided six Presidents U.S. industry's best expertise and recommendations for national security and emergency preparedness communications.

NSTAC's most recent report evaluated the nation's ICT infrastructure resilience during the increased connectivity demands of the early months of the COVID-19 pandemic (roughly the five months from March through July).[5] The report found that due to a variety of positive response factors – for instance, significant capital investments, business continuity and work-from-home planning, diversity in information and communications technology ("ICT") supply chains, and information sharing and response coordination – communications providers responded well to the pandemic's unprecedented demands. In the words of the report, "the overall ICT ecosystem response was strong."

The NSTAC report contained no indication of any security or resilience benefit that might have arisen from a government owned and operated network; to the contrary, the ICT ecosystem's robust response to the pandemic was a result of private sector investment and innovation, leveraged for security and resilience through partnership with the government. In short, since the existential nuclear threats of the Cold War, the U.S. government has recognized that government-run national networks are inferior and impractical substitutes for the world-leading, well-resourced and expertly staffed and managed U.S. privately owned and operated communications networks. The world's most secure and resilient networks are those that are owned and operated by U.S. private industry.

In contrast, no U.S. government agency has ever deployed or managed a national network. Given today's ever-increasing threat environment, now is not the time to try to start doing so. For the Department to seek to become a network owner and operator now, in the entirely new architecture of 5G – as opposed to pursuing the alternatives outlined below that draw on decades of private sector innovation and network management – would turn decades of government-industry collaboration on network security and resilience on its head and would lead to avoidable shortfalls in security and resiliency. Instead, the Department should ramp up its engagement efforts with industry, including USTelecom members, to advance security innovations through 5G test-beds and partnerships such as those focused on developing Zero Trust Architecture and quantum encryption. USTelecom members are the world's leading experts in architecting networks with security by design principles, in operating them securely, and in providing specialized security for special use cases like those of the Department. Our members stand ready to engage and work with the Department in this regard – indeed, many of

[5] Letter from Mr. John Donovan, NSTAC Chair, to Pres. Donald J. Trump (Oct. 6, 2020) *available at* https://www.cisa.gov/sites/default/files/publications/NSTAC%20Letter%20to%20the%20President%20on%20Communications%20Resiliency%20.pdf.

them are already at work with the Department on groundbreaking 5G and related security projects.

II. A NATIONAL 5G NETWORK OWNED AND OPERATED BY THE GOVERNMENT WOULD BE PROHIBITIVELY EXPENSIVE, INEFFICIENT, AND UNDERPERFORMING.

Advocates of government owned and operated networks must confront the fact that in real-world deployments, such approaches have proven expensive, inefficient, and underperforming. For instance, Australia's National Broadband Network, a government owned broadband network that has provided slower service to fewer customers than planned at a higher cost than expected. The Institute of Electrical and Electronics Engineers described the network as "a lumbering disaster that began as an ambitious effort by the Australian government to construct a countrywide broadband network."[6] The U.S. should learn from their example.

In the United States, such an approach would be at odds with more than a century of private sector-led and government-supported innovation and investment in communications networks since our invention of long-distance telegraph and telephony. Put simply, it is not how we build, deploy and operate networks in America. From access to spectrum to fiber backhaul infrastructure to antennas and radios to all other elements necessary to power resilient, secure and fast 5G networks, we will always be better off with private innovation and competition – and government policies that support those principles.

Collectively, U.S. broadband providers have invested trillions of dollars in private capital to build resilient, competitive and efficient networks that power our innovation economy and ensure millions of Americans benefit from broadband connectivity. The diversity of technologies and providers that make up our networks – fixed, wired, and wireless – provide unique services and promote sustainable and secure connections based on the market imperative of high performance. This efficient private investment is based on a highly competitive and accountable market that rewards performance. It is not network design or architecture by committee. That is among the primary reasons why the United States is the undisputed global leader in communications, and it is the model for America's – and the Department's – bright 5G future.

Moreover, it is unlikely that the Department or any other U.S. government agency could build a network that altogether bypasses existing or to-be-deployed private sector infrastructure such as cell towers, poles, radios, base stations, and backhaul fiber. This begs the question of whether a government owned and operated 5G network would require altogether new inefficiencies, such as the government building duplicative infrastructure for every component of the network, from the small cell to the fiber backhaul. If the Department envisions nationalizing only some components of the 5G network's infrastructure services from private carriers for the

[6] IEEE Spectrum, *Australia's Troubled National Broadband Network Delivers a Fraction of What Was Promised*, April 24, 2019, *available at* https://spectrum.ieee.org/telecom/internet/australias-troubled-national-broadband-network-delivers-a-fraction-of-what-was-promised.

purposes of a government owned and operated network, while leasing or procuring other network infrastructure or services, then what cost efficiencies or technological benefits would the Department expect to gain from owning and operating those particular parts of the network's infrastructure? How would this approach be better than the present model of procuring private network services? These questions illuminate that there is no benefit or efficiency gained from a government owned and operated network, and therefore we recommend the steps outlined below as the best path forward for the Department and the government more broadly.

III. THE DEPARTMENT SHOULD LEVERAGE AND BUILD ON EXISTING MODELS FOR U.S. GOVERNMENT SUPPORT FOR PRIVATE SECTOR INNOVATION IN NETWORK DEPLOYMENT AND OPERATIONS.

Rather than attempting to create an altogether new model of network communications, the Department should build on the model of enterprise networks and procured private commercial network services through secure gateways that DoD has used to build and manage its global network, the DoD Information Network (DODIN).[7]

In addition to DoD's own network needs, the U.S. government should also expand and improve upon models of U.S. government support for private network deployment that are powered by private innovation and market incentives. For instance, the FCC's ongoing proceeding to replace untrusted network equipment pursuant to the Secure and Trusted Communications Network Act and the related legislative proposals provides a significant opportunity for advances in private network deployments in high-cost rural areas.[8] Likewise, the FCC has proposed a 5G Fund for Rural America that would make $9 billion available to bring 5G mobile broadband to rural areas.[9] The Department should look to the deployments under these programs for examples of specialized private network services in austere or otherwise unique environments and topographies that could provide real-world lessons for the Department's own 5G network needs.

Finally, because USTelecom members are leaders in both wireless and wireline technologies, we can vouch for the fact that spectrum considerations (including the dynamic spectrum sharing considerations that are the most important inquiries in the Department's RFI) are of course central to 5G policies – and also that a holistic 5G strategy cannot be focused on spectrum alone. Enlightened spectrum policy is certainly necessary for successful 5G deployment, but it is only one piece of the puzzle, and fiber backhaul facilities are just as important.

---

[7] *See, e.g.*, Defense Information Systems Agency, *DODIN Capabilities Framework Overview* (presented by Jon Marcy, DISA Senior UC Architect), May 14, 2019 (at slides 10-11 regarding gateways), *available at* https://www.disa.mil/-/media/Files/DISA/News/Events/DCR-IAC/05142019_AFCEA-TechNet-Cyber-Symposium---DC-Framework-Slides.ashx?la=en&hash=7B5762B642B311F1755FC5362E82F8650598544C.

[8] *See generally Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Report and Order, WC Docket No. 18-89, 34 FCC Rcd 11423 (2019). *See also* Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609).

[9] Establishing a 5G Fund for Rural America, Notice of Proposed Rulemaking and Order, 35 FCC Rcd 3994 (2020).

Simply put, the fiber optic networks that exist or are being deployed are the result of decades of USTelecom members' innovation and investment, and they will play a prominent role in enabling 5G infrastructure. Once fiber is in place, it can easily scale to accommodate higher speeds and expected growth in capacity demands. Thus, fiber will necessarily be deployed broadly throughout emerging 5G networks as an essential component in implementing 5G capabilities and capacities. Fiber also will enable the secure transmission of enormous quantities of data, via wireline fronthaul and backhaul facilities, as consumers, businesses including IoT, and manufacturing become more fully connected. As part of its 5G strategy, the U.S. government therefore should take steps to streamline the deployment of fiber facilities necessary for 5G.

At present, numerous impediments to that deployment remain, which USTelecom and others have documented extensively in other governmental arenas and proceedings. These obstacles include, but are not limited to, unreasonable zoning, permitting, power, construction moratoriums, and aesthetic restrictions on antenna placement. We recommend that the Department lend its considerable influence to removing these barriers; doing so will ensure competitive positioning and thereby increased resiliency of U.S. wireless networks. It will also accelerate customer adoption of the virtually limitless applications that the new generation of 5G wireless services will enable.

Conclusion

USTelecom looks forward to working with the Department and other key stakeholders in industry and the Administration to develop and implement policies that promote the deployment of secure and resilient 5G infrastructure and, in so doing, preserve the technological leadership of the United States.

Respectfully submitted,

/signed/
Robert Mayer
Senior Vice President, Cybersecurity
(202) 326-7300

/signed/
Michael Saperstein
Vice President, Policy & Advocacy
(202) 326-7300

USTelecom – The Broadband Association
601 New Jersey Avenue, NW, Suite 600
Washington, DC 20001