Before the
National Institute of Standards and Technology
U.S. Department of Commerce
Washington, D.C.

In the Matter of: Request for Public Comment	)
on Draft Guidance for 5G Cybersecurity, NIST	)
Special Publication 1800-33B: 5G	)
Cybersecurity Volume B: Approach,	)
Architecture and Security Characteristics	)

COMMENTS OF ADVOCATES FOR SECURE BROADBAND
IN RESPONSE TO REQUEST FOR PUBLIC COMMENT

Wired Broadband, Inc.; Children's Health Defense (www.childrenshealthdefense.org); Environmental Health Trust (https://ehtrust.org/?s=environmental+impact); Kent Chamberlin, PhD, Former member of the NH Commission to Study The Environmental and Health Effects of Evolving 5G Technology; Cecelia Doucette, Director, Massachusetts for Safe Technology; Eugene J. Bazan, PA Smart Meter Work Group (Lemont, PA); Eva Bortnick (Oregon); Coloradans for Safe Technology; Linda Dance (Gainesville, Florida); David DeHaas, President Idahoans For Safe Technology; Donna DeSanto Ott, PT DPT MS, Pennsylvanians for Safe Technology (Reading, PA); Eugenia Dillard (Clearwater, FL); Antonella DiSaverio (Astoria, NY); Floris R. Freshman (Scottsdale, AZ); Ann K. Friday of Relocate the Cell Tower Group (Prescott, AZ); Martha Glaser, Member, Safe Tech for Santa Rosa & EMF Safety Network (Sebastopol, CA); Howard J. Goodman, Esq. Forest Hills, NY; Lonnie Gordon, Exec. Director, MalibuForSafeTech.org (Malibu, CA); Judith de Graffenried, CT Residents 4 Responsible Technology (Trumbull, CT), Debra Greene, PhD, Safe Tech Hawaii (Kihei, HI); Deb Hodgdon, New Hampshire for Safe Technology (Stratham, NH); Charlene Hopey (Topanga, CA); Shirley Denton Jackson (North Palm Beach, FL); Susan Jennings, Founder, Southwest Pennsylvania for Safe Technology (Mount Pleasant, PA); Phillip Lee Keup (Clearwater FL); Pittsfield Cell Tower Injured and Concerned Citizens (Pittsfield, MA); Karol Kuehn (Glen Ellyn, IL); Last Tree Laws Massachusetts; Raymond Michael LeVesque (Kelseyville, CA); Julie Levine, 5G Free California (Topanga, CA); David Morrison, Oregon for Safer Technology (Portland, OR); Paska Nayden, Connecticut For Responsible Technology; New Yorkers 4 Wired Tech (New York, NY); Nevada City Telecommunications Ordinance Public Working Group; Larry Ortega, Community Union, Inc. (Pomona, CA); Wendy Ratner, Cell Tower Free Neighborhoods (Prescott, AZ); Sheila Resseger, Co-Founder, 5G Free Rhode Island (Cranston, RI); Safe Technology Minnesota; Frederick P. Sinclair Jr. (Alfred, NY); Lisa Smith, Safe Tech Tucson (Tucson, AZ); Susan J Supp (Dalton Gardens, ID); Sustainable Upton and co-administrators Laurie Wodin, Marcella Stasa, Christine Lazar, Alisa Bernat; Virginians for Safe Technology, LLC (Fredericksburg, VA); and Anne Wilder, Wire Idaho (Priest River, ID)

(collectively, hereinafter, "Advocates for Secure Broadband") submit these comments in response to the request for public comments[1] relating to the above-captioned matter.

Introduction

NIST is asking for public comment on its Draft Guidance for 5G Cybersecurity ("Guidance").[2] This Draft Guidance is an aspirational document, only "designed" to manage risk, which is an acknowledgement that the security risk of wireless networks cannot be eliminated and only addresses what might be cyber sufficient for industry, but not cybersecure. Indeed, Sec 3.5.3, Mitigated Threats and Vulnerabilities, of the Guidance states that

> "Each security capability ... is intended to help mitigate certain types of threats and vulnerabilities so as to reduce overall risk to an acceptable level." [3]

What is "acceptable" may be sufficient for industry, but it is not secure.

The Guidance provides a risk analysis of 5G's security capabilities and its threats and vulnerabilities, discussing how it can leverage security features of cloud-based technology, but no risk analysis or assessment can eliminate the risk inherent in 5G's wireless network.

5G's Inherent Cyber Risks

NIST Guidance states that it is focusing on "leveraging the robust security features available in cloud computing architectures to protect 5G data and communications," however, there are many more risk factors inherent in 5G than in previous networks.[4] What is challenging about maintaining cybersecurity is that wireless is inherently not secure, and 5G is inherently even less so. As Wheeler pointed out, "5G networks are more vulnerable to cyberattacks than their predecessors."[5]

---

[1] NIST request for public comment, https://www.nist.gov/news-events/news/2022/04/nist-requests-public-comment-draft-guidance-5g-cybersecurity.
[2] Id.
[3] NIST Special Publication 1800-33B, Volume B: Approach, Architecture, and Security Characteristics, 5G Cybersecurity, https://www.nccoe.nist.gov/sites/default/files/2022-04/nist-5G-sp1800-33b-preliminary-draft.pdf.
[4] *Why 5G Networks Are Disrupting The Cybersecurity Industry*, Oct 29, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/10/29/why-5g-networks-are-disrupting-the-cybersecurity-industry/?sh=5186fc041fe9.
[5] *Why 5G Requires New Approaches to Cybersecurity*, Tom Wheeler and David Simpson, Brookings Institute, Sept 3, 2019, https://www.wita.org/nextgentrade/why-5g-requires-new-approaches-to-cybersecurity/.

Jeff Cichonski, a NIST information technology specialist and one of the authors of the Guidance, pointed out that:

> "A potential issue … is the current lack of 5G standards that specify how to deploy cybersecurity protections onto the ***underlying components*** that support and operate the 5G system."

This gets to the root of the problem. The 4G network is a centralized, hardware-based switching network that uses a hub-and-spoke design with hardware choke points for security; in contrast, 5G is a distributed, software-based network of digital routers without chokepoint control.[6] Therefore, there is an exponential increase of access points that a hacker can exploit. As reported in Forbes magazine:

> "***5G's dynamic software-based systems have far more traffic routing points*** than the current hardware-based, centralized hub-and-spoke designs that 4G has. ***Multiple unregulated entry points to the network can allow hackers access to location tracking and even cellular reception for logged-in users***."[7] [Emphasis added.]

It is difficult to "quarantine" a security breach with 5G because of its architecture.

> "Current 4G systems use network partition methods to limit cyber attacks. Networks are subdivided by hardware to prevent the existence of a single point of failure. If one node of the network is attacked, it can be "quarantined" to limit the attack, without ceding control of the whole network. On the other hand, 5G uses short-range, low-cost and small-cell physical antennas within the geographic area of coverage. ***Each antenna can become a single point of control. Botnet and denial of service (DDoS) type attacks can bring down whole portions of the network simply by overloading a single node.***"[8] [Emphasis added.]

The manner of 5G transmission also contributes to its heightened cyber risk.

---

[6] *Why 5G Requires New Approaches to Cybersecurity*, Tom Wheeler and David Simpson, Brookings Institute, Sept 3, 2019, https://www.wita.org/nextgentrade/why-5g-requires-new-approaches-to-cybersecurity/.
[7] *Why 5G Networks Are Disrupting The Cybersecurity Industry*, Oct 29, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/10/29/why-5g-networks-are-disrupting-the-cybersecurity-industry/?sh=5186fc041fe9.
[8] Id.

> " … 5G uses dynamic spectrum sharing, a telecommunication system that breaks data packets into "slices." Each slice from different, parallel communications is sent over the same bandwidth. ***Each slice thus contributes to its cyber risk degree***."[9]

If a hacker gains control of the 5G software managing the networks, the hacker can also control the 5G network.[10]

A cautionary note: "[t]he NotPetya attack in 2017 caused $10 billion in corporate losses. The combined losses at Merck, Maersk, and FedEx alone exceeded $1 billion."[11] Although these incidents preceded 5G, 5G's network is even less secure.

Higher-level network functions formerly done by physical appliances are done virtually with 5G. Because this virtualization is:

> "based on the common language of Internet Protocol and well-known operating systems … ***these standardized building block protocols and systems have proven to be valuable tools for those seeking to do ill."[12]*** [Emphasis added.]

With respect to 5G facilitating Internet of Things (IoT), cybersecurity measures on many IoT devices are either minimal or non-existent. IoT devices such as household appliances and driverless cars are rampantly insecure.[13]

> "***These devices are already being used by hackers as entry points to enterprise networks.*** We may soon live in a world where billions of everyday devices, from toothbrushes to coffee machines, could be connecting to the internet automatically. In the future, such unsecured IoT devices could easily

---

[9] Id.
[10] *Why 5G Requires New Approaches to Cybersecurity*, Tom Wheeler and David Simpson, Brookings Institute, Sept 3, 2019, https://www.wita.org/nextgentrade/why-5g-requires-new-approaches-to-cybersecurity/.
[11] Id.
[12] Id.
[13] *Ransomware and the Internet of Things,* Bruce Schneier, https://www.schneier.com/blog/archives/2017/05/ransomware_and_.html. Bruce Schneier is a fellow and lecturer at Harvard's Kennedy School, board member of the Electronic Frontier Foundation and Chief of Security Architecture at Inrupt, Inc.

allow for ***man-in-the-middle attacks***. ***A cybercriminal could intercept and change sensitive communication over 5G***."[14] [Emphasis added.]

Wheeler continues to point out additional 5G vulnerabilities:

> "Even if it were possible to lock down the software vulnerabilities within the network, the network is also being managed by software." [15]

Regarding penetration testing to determine potential gaps in security, the Sans Institute, which is reputed to be the largest cybersecurity research and training organization, states that:

> "… many of these [IoT] devices do not consider or only minimally consider security in the design process. While we have seen this behavior in other types of testing as well, IoT is different because it ***utilizes and mixes together many different technology stacks*** such as custom Operating System builds, web and API interfaces, various networking protocols (e.g., Zigbee, LoRA, Bluetooth/BLE, WiFi), and proprietary wireless. ***This wide range of diverse, poorly secured technology makes for a desirable pivot point into networks, opportunities for modification of user data, network traffic manipulation, and more.***"[16] [Emphasis added.]

It has been pointed out that:

> "The future will contain ***billions of orphaned devices*** connected to the web that simply have no engineers able to patch them.
>
> "Imagine this: The company that made your Internet-enabled door lock is long out of business. You have no way to secure yourself against the ransomware attack on that lock. Your only option, other than paying, and paying again when it's reinfected, is to throw it away and buy a new one."[17]

---

[14] *Why 5G Networks Are Disrupting The Cybersecurity Industry*, Oct 29, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/10/29/why-5g-networks-are-disrupting-the-cybersecurity-industry/?sh=5186fc041fe9.

[15] *Why 5G Requires New Approaches to Cybersecurity*, Tom Wheeler and David Simpson, Brookings Institute, Sept 3, 2019, https://www.wita.org/nextgentrade/why-5g-requires-new-approaches-to-cybersecurity/.

[16] Sans Institute, https://www.sans.org/cyber-security-courses/iot-penetration-testing/.

[17] *Ransomware and the Internet of Things,* Bruce Schneier, https://www.schneier.com/blog/archives/2017/05/ransomware_and_.html. Bruce Schneier is a fellow and lecturer at Harvard's Kennedy School, board member of the Electronic Frontier Foundation and Chief of Security Architecture at Inrupt, Inc.

The cyber threat and vulnerabilities of 5G appear unquantifiable. What possible guidance can be provided for that? Consider:

> " … the vulnerability created by ***attaching tens of billions of hackable smart devices*** (actually, little computers) to the network colloquially referred to as IoT. … for instance, Microsoft reported that ***Russian hackers had penetrated run-of-the-mill IoT devices to gain access to networks. From there, hackers discovered further insecure IoT devices into which they could plant exploitation software."***[18] [Emphasis added.]

Wheeler reported, back in 2019, that hackers are already setting their sights on the 5G ecosystem, well beyond consumer products:

> "***The world's hackers (good and bad) are already turning to the 5G ecosystem***, as the just concluded DEFCON 2019 (the annual ethical 'hacker Olympics') illustrated. The targets of this year's hacker villages included key parts of the 5G ecosystem such as: ***aviation, automobiles, infrastructure control systems, privacy, retail call centers and help desks, hardware in general, drones, IoT, and voting machines.***"[19]

Does that mean that IoT will facilitate a hacker to divert an airplane from its intended course or provide an entry point to hi-jack a plane, to hack into voting machines and interfere with election results, or to hijack the Pentagon's national security systems e.g. by a nation state?

The cyber threats and vulnerabilities of 5G are unquantifiable. It appears that there is no guidance that can contain the threat. The Guidance concedes the point when it cites as some of its benefits "lower[ing] the likelihood of an incident occurring, and expedit[ing] recovery." Perhaps there can be expedited recovery of a security breach for an organization's systems. But, what recovery is there when a plane is hi-jacked placing many lives in danger, or election results are hacked thereby endangering our national stability, or hacking into our national security infrastructure?

---

[18] *Why 5G Requires New Approaches to Cybersecurity*, Tom Wheeler and David Simpson, Brookings Institute, Sept 3, 2019, https://www.wita.org/nextgentrade/why-5g-requires-new-approaches-to-cybersecurity/.
[19] Id.

The Guidance cannot take in isolation the organization's systems without also taking into consideration the larger 5G ecosystem, and the likelihood, or the certainty, of the threats becoming a reality.

Fiber Optics Beats Wireless for Security and Capacity

In his testimony to Congress in 2021, former FCC Chairman, Tom Wheeler, called for the deployment of fiber optics to the premises (FTTP) as a priority, and only wireless as a last resort, not a first resort.[20] Wheeler stated that despite approximately $40 billion of government subsidies "over the last decade," those subsidies:

> "have failed to deliver the goal of universal access to high-speed broadband … because it ***failed to insist on futureproof technology***, … and focused more on the companies being subsidized than the technology being used or the people who were supposed to be served." [Emphasis added.]

Fiber is "futureproof" while wireless is not.

Optical fiber technology consists of wires that carry data encoded on light beams, and is capable of delivering data capacity about 100 times faster than wireless. In contrast, "[t]he privatized wireless market has failed to deliver adequate and sustainable connectivity, resulting in the U.S. falling in rank to #17 of 20 among developed countries in fixed broadband penetration as a percentage of the population." [21] 5G and IoT are engines of forced obsolescence.[22]

The National Telecommunications and Information Association (NTIA) has announced a "clear preference for fiber" in connection with broadband deployment under the Infrastructure Investment and Jobs Act of 2021.[23] The Fiber Broadband Association's CEO states that:

---

[20] Testimony to Congress, Tom Wheeler, 2021, https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Wheeler_FC_2021.03.22.pdf.

[21] NEW REPORT: "Re-Inventing Wires: The Future of Landlines and Networks" Wireless Networks Are Not as Fast, Secure, Reliable or Energy-Efficient as Wired Systems, Says New Report, https://gettingsmarteraboutthesmartgrid.org/wires.html.

[22] Id.

[23] *NTIA Official Acknowledges Clear Preference for Fiber in Infrastructure Deployment Program,* June 13, 2022, https://broadbandbreakfast.com/2022/06/ntia-official-acknowledges-clear-preference-for-fiber-in-infrastructure-deployment-program/.

> "The market and our government have finally come to the conclusion that ***if it's not fiber, it's not broadband.***"[24]

The former President of Microsoft in Canada, Frank Clegg, stated in his testimony to the New Hampshire legislature in Feb, 2022, that:

- "Wireless technology is no longer the preferred technology for communications. There is an insignificant number of applications that truly require a wireless connection. The majority of communications' applications can benefit from the advantages of a wired connection.
- "Wired broadband is at least 100 times faster, more reliable and resilient and is far more protective of privacy than wireless connectivity."[25]

He also stated that "[t]he industry will grumble, but they will pivot to provide superior connectivity with fiber-to-and-through-the-premises -- if they are incented to do so."[26]

The National Institute for Science, Law & Public Policy (NISLAPP) states that wireless should primarily apply to devices or products that require mobility, and that the superior means of communication is through wired connections.[27] The author of that study is Timothy Schoechle, PhD, Senior Research Fellow at NISLAPP and a telecommunications expert and international consultant in computer engineering and standardization.

With FTTP there will be greater broadband capacity and more bandwidth in the wireless spectrum to make calls[28] Spectrum deficiencies are being caused by:

> "[t]he proliferation of ***frivolous wireless uses***, such as gaming, entertainment-streaming and advertising. As wireless spectrum deficiencies become a greater problem, wireless providers ramp up the fight over less-desirable

[24] Id.
[25] Testimony from retired Microsoft Canada President Frank Clegg to the New Hampshire legislature, including the statement, "Wireless technology is no longer the preferred technology for communications." alpaca-chinchilla-x6xf.squarespace.com/s/Clegg-Comments-to-New-Hampshire-Science-Technology-and-Energy-Committee-7-Feb-2022.pdf
[26] Id.
[27] *Re-Inventing Wires: The Future of Landlines and Networks*, 2018, National Institute for Science, Law & Public Policy (NISLAPP) at 88, authored by Timothy Schoechle, PhD, https://gettingsmarteraboutthesmartgrid.org/pdf/Wires.pdf; Schoechle is an international consultant in computer engineering and standardization, former faculty member of the University of Colorado, College of Engineering and Applied Science and Senior Research Fellow at the National Institute for Science, Law & Public Policy.
[28] Testimony from retired Microsoft Canada President Frank Clegg to the New Hampshire legislature, alpaca-chinchilla-x6xf.squarespace.com/s/Clegg-Comments-to-New-Hampshire-Science-Technology-and-Energy-Committee-7-Feb-2022.pdf

> frequency bands. ***No one yet knows what will happen to wireless spectrum requirements when 50 billion IoT consumer devices are Internet-connected***. The greater the battles over spectrum, the more cell sites and DAS [Distributed Antenna System] … wireless antennas are needed ***to stretch the spectrum*** ... "[29]

A consequence of these frivolous wireless uses is insufficient bandwidth necessary for medical reporting devices such as heart monitors.[30]

> "Many of these devices are wireless and transmit short packets infrequently. ***Perversely, overuse of radio spectrum by non-essential or trivial wireless products can produce "electrosmog" pollution that can block or drown-out useful, beneficial, and necessary uses of that radio spectrum, such as [medical reporting devices]."***

The wireless technology of 5G has been touted for its social utility such as telemedicine and telesurgery, as well as for driverless cars. Wireless reception can be inherently unstable for a variety of factors – the number of people using the wireless network, weather conditions, etc. Who would want to be the patient in telesurgery when wireless connection is rendered unstable or lost because there are also 1 million users trying to download movies?

In contrast, fiber optics would allow for the simultaneous downloading of movies while providing the bandwidth needed to perform telesurgery. It would also guard against hackers trying to interfere with the telesurgery because it provides greater cybersecurity. Therefore, the most robust and more reliable network that would provide greater cybersecurity and social utility would be a fiber optics network which is inherently more secure and inherently carries far greater capacity. Wired connections are inherently more stable than wireless, especially in emergencies or bad weather.

---

[29] NEW REPORT: "Re-Inventing Wires: The Future of Landlines and Networks" Wireless Networks Are Not as Fast, Secure, Reliable or Energy-Efficient as Wired Systems, Says New Report, https://gettingsmarteraboutthesmartgrid.org/wires.html.

[30] *Re-Inventing Wires: The Future of Landlines and Networks* at Sec. 3.2.8 (Electrosmog and Interference), 2018, National Institute for Science, Law & Public Policy (NISLAPP) at 88, authored by Dr. Timothy Schoechle, PhD, https://gettingsmarteraboutthesmartgrid.org/pdf/Wires.pdf

Cyber Security and Data Privacy

Besides being vulnerable to security breaches, IoT devices also collect a massive amount of personal data,[31] that could be exposed to hackers in a security breach.

As NISLAPP points out:

> "***IoT devices are a potential weak point for security.*** Inexpensive IoT sensor and actuator devices are vulnerable because they do not generally have the processing power to manage increasingly complex security protocols and encryption schemes, and it would be a challenge to update them, even if and when processing power is adequate" [32] [Emphasis added.]

Data privacy is closely related to security. IoT devices and applications capture personal data which feeds into a provider's commercial advertising business model to collect and sell personal data. Although the propriety of this data capture is questionable, personal data on IoT devices can present a vulnerability because the data:

> "can be captured by ***"botnets"—***automated networks of computing devices that have been captured or compromised. … [A] researcher at enterprise security company Proofpoint noticed … [that] a security gateway was logging hundreds of thousands of malicious e-mails that were clearly being sent out by over 100,000 Linux-running devices, but they weren't PCs. ***Rather, they were Internet-connected consumer gadgets including routers, TVs, multimedia centers, and even a fridge.*** …He expects to see a lot more of what he refers to as ***"thingbots"*** as connected devices spread throughout the home, especially since the security in place on so many of these gadgets is just a simple Web interface that asks you to set up a username and password." [Emphasis added.]

---

[31] *The 5 worst big data privacy risks (and how to guard against them),* https://www.csoonline.com/article/2855641/the-5-worst-big-data-privacy-risks-and-how-to-guard-against-them.html.

[32] Re-Inventing Wires: The Future of Landlines and Networks, 2018, National Institute for Science, Law & Public Policy (NISLAPP), authored by Timothy Schoechle, PhD, https://gettingsmarteraboutthesmartgrid.org/pdf/Wires.pdf.

Burden of Cybersecurity Should be on Providers, Not on Customers

The burden should be on providers to protect their customers from cyber security risk. The standards provided in this Guidance may be a "good faith" effort to provide assurances to customers. But the Guidance might be used, instead, as a shield to protect providers from liability so long as they can represent to their customers (e.g., hospitals, medical offices, consumers) that they have systems "designed" to provide security under NIST standards, but never achieving it.

In effect, the Guidance is creating a "safe harbor" for organizations that may shelter them from liability in the event of any security breaches that affect their customers. If organizations can represent to their customers that they are "in compliance" with NIST standards, then providers may not be liable for security breaches. Providers should be able to represent to customers that they will affirmatively provide security and achieve it, a level of representation which can be more easily achieved with the provision of fiber optics.

Although the Guidance lists various benefits for organizations to implement the demonstrated approach in the Guidance,[33] it does not list the risks. Articulating the risks in the Guidance would provide customers with full disclosure and transparency, identifying all gaps in security. Therefore, when an organization represents compliance with NIST standards, the customers would also know where the Guidance falls short on such gaps in security.

As Wheeler points out, "good faith efforts are insufficient."[34] Wheeler's concern is that 5G networks "exacerbate[] the cybersecurity threat" and that customers (e.g., consumers, companies, government) have to assess for any cyber risk.[35] "Placing the security burden on

[33] Section 3.1 of the Guidance posits the following benefits for organizations that implement the demonstrated approach in the Guidance:
• "The components of the 5G network will be less susceptible to cyberattacks and will provide better attack visibility, detection, and control, which will reduce risk, lower the likelihood of an incident occurring, and expedite recovery.
• "The 5G network's supporting infrastructure will be more resistant to compromise and provide more visibility into the trust status of the underlying platforms.
• "The contents of 5G communications will be safeguarded from eavesdropping and tampering, and the privacy of 5G users will also be protected.
• "The demonstrated practices can play an important role as your organization embarks on a journey to zero trust."
[34] *Why 5G Requires New Approaches to Cybersecurity*, Tom Wheeler and David Simpson, Brookings Institute, Sept 3, 2019, https://www.wita.org/nextgentrade/why-5g-requires-new-approaches-to-cybersecurity/.
[35] Id.

the user is an unrealistic expectation, yet it is a major tenet of present cybersecurity activities."[36]

Customers are not able to make informed market decisions and should have "nutritional labeling" about the cyber risks.[37] Among device and application vendors there apparently are no "verifiable security indicators" which customers can assess.[38] "A 2018 White House report found a 'pervasive' underreporting of cyber events that "hampers the ability of all actors to respond effectively and immediately."[39]

Moreover, any guidance should extend to the entire 5G ecosystem,[40] beyond the security architecture in an organization, to the devices and services that are being made available to the customers. What cyber security readiness can be sustained for products after purchase? For example, as IoT devices proliferate, security should also extend to the consumers who are purchasing those devices, and should be the kind of security that extends to consumers until those devices reach their end of life. It should also include instances when consumers still want to keep their devices after the organization no longer provides support for those devices, or if the organization goes out of business.

Consumers should know at the time of purchase what the expected life expectancy is for their devices. For example, they may want to keep their IoT refrigerator for 20 years or their car for 5 years, but if security patches are no longer supported, what will an organization do if the refrigerator or car gets hacked, subjecting consumers to ransomware who cannot use their refrigerator or get into their car?

What security will be provided to the consumer for IoT devices no longer supported by the provider, be it a refrigerator, stove, air conditioner or car? By support is meant providing bug patches, such as for security.

Feedback has been requested "if the guide accurately describes technical security capabilities and related threats and vulnerabilities." It does not and cannot because of the unquantifiable nature of 5G devices and applications and the level of liability and responsibility that organizations should and must accept, but to date have not, based on the Guidance. If providers are using the Guidance as a "safe harbor" for cyber sufficiency rather than for cyber

[36] Id.
[37] Id.
[38] Id.
[39] Id.
[40] Id.

security, and cannot stand by their products and services with an affirmative obligation for cyber security, then they should not be selling them.

Public's Representation on NIST Guidance

What is lacking in the Guidelines is public stakeholders' participation in drafting the Guidelines. If these Guidelines are being put into place for the benefit of the public, as well as for the benefit of the organization, then the public should also have representation on the NIST Guidelines, not simply an opportunity to comment. The public would include charitable and non-profit organizations, and non-industry experts, working on these issues for the benefit of the public.

As an aside on the issue of the Guidelines, but necessary to put these Guidelines in perspective, it should be considered that the ethics of implementing "5G" and embellishing on its cybersecurity aspects is putting the cart before the horse. It can be argued that, because "5G" has not been safety tested, and because the weight of evidence from established and mainstream science, industry, U.S. military[41] and experts of the hazards of wireless radiation, and the Court of Appeals of the D.C. Circuit discrediting the FCC wireless emission limits in 2021 on health grounds,[42] any further rollout of "5G" should cease.

NIST's Cybersecurity Practice Guides are referred to as "user-friendly," but there is nothing user-friendly about a wireless technology that is potentially hazardous and that has already injured people.

It is ironic that wireless is being touted for telemedicine and telesurgery as life-affirming goals when wireless has been found to be the opposite, hazardous to people's health who are already disabled from wireless and potentially hazardous to those whose health has not yet been affected or who do not yet realize that their injuries arise from exposure to wireless radiation. That wireless is planned to be placed on top of hospitals is also ironic as hospitals are where people go to heal, whereas any wireless infrastructure on top or close to any hospitals may create new symptoms or make existing symptoms worse.

[41] Military Experts, https://sites.google.com/site/understandingemfs/military-experts?authuser=0.
[42] See Comments of Advocates for the EMS Disabled in Response to Notice of Inquiry, In the Matter of Implementing the Infrastructure Investment and Jobs Act: Prevention and Elimination of Digital Discrimination, GN Docket No. 22-69, Federal Communications Commission.

Conclusion

The threats and vulnerabilities of 5G are endemic to its architecture. Given 5G's distributed architecture, it is largely more susceptible than its predecessors to cyberattack. The threat of 5G security breaches is not limited to an organization, but extends to an entire 5G ecosystem. IoT will make the cyber risks unquantifiable when billions of devices are connected, with hackers poised to exploit 5G vulnerabilities.

The NIST Guidelines provide a "safe harbor" to shield providers from liability, while placing the burden of risk on the customer. The ethics of rolling out 5G to the public with such unquantifiable risks, and potentially unleashing a concatenation of security breaches extending from consumer goods to transportation to national security, mandates caution in proceeding with, or even ceasing, any further rollout of "5G" to the public.

Respectfully Submitted,
Odette J. Wilkens
President & General Counsel
Wired Broadband, Inc.
P.O. Box 750401
Forest Hills, NY 11375
owilkens@wiredbroadband.org

The following groups and individuals have granted permission to submit these comments on their behalf under the name of "Advocates for Secure Broadband:"
Wired Broadband, Inc.; Children's Health Defense (www.childrenshealthdefense.org); Environmental Health Trust (https://ehtrust.org/?s=environmental+impact); Kent Chamberlin, PhD, Former member of the NH Commission to Study The Environmental and Health Effects of Evolving 5G Technology; Cecelia Doucette, Director, Massachusetts for Safe Technology; Eugene J. Bazan, PA Smart Meter Work Group (Lemont, PA); Eva Bortnick (Oregon); Coloradans for Safe Technology; Linda Dance (Gainesville, Florida); David DeHaas, President Idahoans For Safe Technology; Donna DeSanto Ott, PT DPT MS, Pennsylvanians for Safe Technology (Reading, PA); Eugenia Dillard (Clearwater, FL); Antonella DiSaverio (Astoria, NY); Floris R. Freshman (Scottsdale, AZ); Ann K. Friday of Relocate the Cell Tower Group (Prescott, AZ); Martha Glaser, Member, Safe Tech for Santa Rosa & EMF Safety Network (Sebastopol, CA); Howard J. Goodman, Esq. Forest Hills, NY; Lonnie Gordon, Exec. Director, MalibuForSafeTech.org (Malibu, CA); Judith de Graffenried, CT Residents 4 Responsible Technology (Trumbull, CT), Debra Greene, PhD, Safe Tech Hawaii (Kihei, HI); Deb Hodgdon, New Hampshire for Safe Technology (Stratham, NH); Charlene Hopey (Topanga, CA); Shirley Denton Jackson (North Palm Beach, FL); Susan Jennings, Founder, Southwest Pennsylvania for Safe Technology (Mount Pleasant, PA); Phillip Lee Keup (Clearwater FL); Pittsfield Cell Tower Injured and Concerned Citizens (Pittsfield, MA); Karol Kuehn (Glen Ellyn, IL); Last Tree Laws Massachusetts; Raymond Michael LeVesque (Kelseyville, CA); Julie Levine, 5G Free California (Topanga, CA); David Morrison, Oregon for

Safer Technology (Portland, OR); Paska Nayden, Connecticut For Responsible Technology; New Yorkers 4 Wired Tech (New York, NY); Nevada City Telecommunications Ordinance Public Working Group; Larry Ortega, Community Union, Inc. (Pomona, CA); Wendy Ratner, Cell Tower Free Neighborhoods (Prescott, AZ); Sheila Resseger, Co-Founder, 5G Free Rhode Island (Cranston, RI); Safe Technology Minnesota; Frederick P. Sinclair Jr. (Alfred, NY); Lisa Smith, Safe Tech Tucson (Tucson, AZ); Susan J Supp (Dalton Gardens, ID); Sustainable Upton and co-administrators Laurie Wodin, Marcella Stasa, Christine Lazar, Alisa Bernat; Virginians for Safe Technology, LLC (Fredericksburg, VA); and Anne Wilder, Wire Idaho (Priest River, ID).