March 27, 2024

U.S. Senate Committee on Commerce, Science and Transportation
Washington, DC 20510

Re: Comments related to the hearing of March 21, 2024 on Spectrum and National Security

Oppose the following bills:

S. 3909 Spectrum Pipeline Act of 2024
S. 4010 (HR 1338) Satellite and Telecommunications Streamlining Act
S. 1648 Launch Communications Act
S. 3781 ITS Codification Act
S. 3690 Amateur Radio Emergency Preparedness Act
HR 3565 Spectrum Reauthorization Act of 2023

Support only with amendments

HR 1353 Advanced, Local Emergency Response Telecommunications Parity Act
HR 4510 NTIA Reauthorization Act of 2023
S.2238 PLAN for Broadband Act

Dear Chair Cantwell, Ranking Member Cruz, and Members of the Committee,

We respectfully submit these comments in opposition to any legislation or policies that would endanger our national security or public safety.

A. Diverting Military Spectrum

Diverting military spectrum for commercial, for-profit uses does not serve our national security. Military spectrum is now being used for critical national security systems, e.g., military satellites, NASA, NOAA, military aircraft telemetry and air defense missile systems. Reallocating or relinquishing military spectrum can potentially cost taxpayers billions of dollars.

For instance, for the Department of Defense to relinquish 350 MHz of C-band would cost "hundreds of billions of dollars."[1]

Sharing military spectrum with commercial, for-profit uses risks hacking of our vital military communications. These commercial interests are expected to use spectrum for 5G, which increases the risk of cyberattacks. "5G networks are much more vulnerable to cyberattacks than their predecessors," as noted by former FCC Chairman, Tom Wheeler.[2] Wheeler co-authored an article in which he coined the term "the 5G Cyber Paradox," the more efficient the more cyber insecure it is.

> "Fifth generation wireless networks are a paradox: As they improve the efficiency and capability of the communications infrastructure to enable a new generation of services, they also introduce **new security vulnerabilities that threaten both the networks and those who rely on their connectivity**."

Security vulnerabilities are inherent in 5G architecture and, while 5G is being deployed, these vulnerabilities have not been resolved. **No commercial interest is worth risking our national security.**

B. The Market Has Spoken,[3] and It Wants Wired Connectivity

Our recommendation is for the military to retain its spectrum, and for commercial, for-profit entities to deploy wired connectivity, e.g., fiber or coaxial cable. The free market has spoken, and it prefers wired connectivity. For instance, two-thirds of people prefer fiber as the best internet service in terms of speed and reliability.[4] "Among 17% of consumers changing internet service providers in the past two years, fiber delivery had a net gain of 15 market share points."[5]

C. Section 6409(a) Preemptions Work Against Consumers

The greater proliferation of wireless infrastructure that would result from diverting military spectrum to for-profit uses will trigger Section 6409(a) of the Middle Class Tax Relief and Job Creation Act of 2012 (Public Law 112–96, 47 USC 1455) that can be invoked to preempt state and local rights. It provides that once an antenna is deployed in a particular location, that facility can be modified or expanded and the state or local government is required to approve it. Hundreds of localities around the country have sued the FCC over its rules implementing this section.[6]

---

[1] https://sgp.fas.org/crs/misc/IF12351.pdf

[2] 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/.

[3] https://www.fiberbroadband.org/p/cm/ld/fid=978.

[4] https://www.fibre-systems.com/article/fiber-connect-2023-two-thirds-us-consumers-prefer-fibre?iframe=1

[5] Ibid.

[6] *Montgomery County v. FCC* (2015 Fourth Circuit, No. 15-1240)
https://www.ca4.uscourts.gov/Opinions/Published/151240.P.pdf

Therefore, diversion of military spectrum will exacerbate the preemptions under this section, working against consumers.

D. Market Distortion

Legislation diverting military spectrum for commercial, for-profit uses would rely on heavy-handed, 6409 preemption to subvert and distort market forces. That is because the legislation is expected to work synergistically with Section 6409, as described above, and other bills and laws otherwise mandating the further proliferation of wireless infrastructure which the public **does not want.** As Adam Smith stated, in free markets, the interests of the consumer comes first and should not be sacrificed to commercial interests.[7]

Here, however, the interests are reversed where the interests of for-profit entities are given priority to the detriment of our national security and to the detriment of the consumer who has made it clear, across the country, **does not want wireless infrastructure outside of their homes, their children's bedroom windows, outside of their classrooms.** Consumers oppose the irresponsible placement of wireless infrastructure. For instance, in New York City, community boards representing 2 million residents, over 25% of the NYC population, have sent a clear message to the Mayor that **they do not want the 5G Towers in their neighborhoods and they do not need them**. No evidence of any gap in service has been proffered, and when requested the response has been that the information is proprietary, much to the ire of NYC residents. Low-income communities are bristling at being branded equity districts or part of the "digital divide," without their consent. They view this as just more *noblesse oblige*. They know what they need for their communities without onerous government mandates.

What is currently being considered, along with these bills, would work synergistically in rewriting The Telecommunications Act of 1996 (TCA) eroding any remnant of cooperative federalism in balancing local and federal interests.

The collateral damage of diverting more military spectrum for commercial, for-profit entities is to deny broadband freedom of choice to the consumer, increasing special privileges for wireless permitting by forcing approval over strenuous consumer objections. This creates market distortion by having a government agency substitute its own judgement for the free market by giving special privileges for wireless, an inferior technology, that many consumers strenuously oppose. This also creates a disincentive for industry innovation, where these for-profit entities should otherwise compete on the basis of safe technology.

City of Boston v. FCC (pending in the Ninth Circuit)

https://dockets.justia.com/docket/circuit-courts/ca9/20-72749

[7] "Consumption is the sole end and purpose of all production; and the interest of the producer ought to be attended to, only so far as it may be necessary for promoting that of the consumer. The maxim is so perfectly self-evident, that it would be absurd to attempt to prove it. But in the mercantile system, the interest of the consumer is almost constantly sacrificed to that of the producer; and it seems to consider production, and not consumption, as the ultimate end and object of all industry and commerce." https://oll.libertyfund.org/quotes/adam-smith-consumption-only-purpose-production .

E. Admission of Cancer Risk and Court Order of Remand of FCC Rules

Industry should compete on safety. In 2021, the D.C. Circuit Court of Appeals remanded the FCC's wireless emission guidelines for failure to review accounts of personal injuries and 11,000 pages of scientific, peer-reviewed, studies showing harm, long-term exposure and its effect on children.[8] Those limits date back to 1996 when the age of technology was just taking off. To date, they have not been updated. Not updating the limits is creating market distortion, rather than encouraging innovation and competition for safe technology, from which the consumer can choose. The limits, however, function now as a safe harbor to immunize industry from personal claims of injury, no matter how severe or fatal.

An example of innovation and competing on safety can be seen in a patent of a Swiss telecom carrier.[9] Switzerland had reduced its emission limits. The carrier was applying for a process that would reduce wireless radiation. The reason given in the patent– because electro-magnetic radiation carries high risk of cancer and has no bearing on whether the effect is thermal or not.

The science is clear for people who understand the science. Thousands of scientific and medical studies show neurological disorders; increased risk of cancer and brain tumors; DNA damage; oxidative stress; immune dysfunction; cognitive processing effects; altered brain development, sleep and memory disturbances, ADHD, abnormal behavior, sperm dysfunction, and damage to the blood-brain barrier.[10]

The potential harmful interference of Wi-Fi is not limited to spectrum frequencies, but harmful interference to people and the environment. Until we address the latter, addressing sharing military spectrum frequencies for commercial use is premature and putting the cart before the horse, so to speak.

---

[8] Appeals Court Tells FCC to Address Non-Thermal Health Impacts of Radiation from Wireless Technology on Children, the Public, and the Environment, Aug. 25, 2021, https://ehtrust.org/appeals-court-tells-fcc-to-address-non-thermal-health-impacts-of-radiation-from-wireless-technology-on-children-the-public-and-the-environment/; see also the 27 volumes of evidence in the FCC Docket (click on "Documents Filed with the Court: The Evidence") https://childrenshealthdefense.org/legal_justice/chd-successfully-challenges-the-fccs-outdated-wireless-radiation-exposure-guidelines/#documents.

[9] https://www.avaate.org/spip.php?article2061

[10] A Rationale for Biologically-based Exposure Standards for Low-Intensity Electromagnetic Radiation, 2022, https://bioinitiative.org/conclusions/; see also, Adverse health effects of 5G mobile networking technology under real-life conditions, May 1, 2020, https://pubmed.ncbi.nlm.nih.gov/31991167/; Wireless Radiation (RFR) – Is U.S. Government Ignoring Its Own Evidence for Risk? March, 28, 2019, https://electromagnetichealth.org/electromagnetic-health-blog/u-s-gov-ignoring-own-evidence/; Oxidative Mechanisms of Biological Activity of Low-Intensity Radiofrequency Radiation, Electromagnetic Biology and Medicine, 35(2), 186-202, Yakymenko, I., Tsybulin, O., Sidorik, E., Henshel, D., Kyrylenko, O., & Kyrylenko, S. (2016), https://pubmed.ncbi.nlm.nih.gov/26151230/.

There is a dangerous way to deploy wireless infrastructure and a safe way to do so. We should be encouraging **competition based on safety**. The FCC must comply with the court order for any wireless deployment to the public to continue.

F. Radiation Injuries and Barrier to Access

Many individuals across the U.S. have been and continue to be injured or permanently disabled by electro-magnetic radiation (EMR), essentially radiation poisoning. Being irradiated by EMR is akin to Superman touching Kryptonite – all of his powers gone and crippled. With EMR, you cannot see it or smell it, like gas on a stove, except that a smell has been added to the gas to alert of impending danger.

This gives a visual depiction of EMR:

Figure 7. Gervais Street: Cell phone base station antenna placed close to street level and causing high exposure to pedestrians and nearby café visitors (exposure scenario illustration). The antenna appears camouflaged and seemingly part of a utility pole. The measurer only discovered the antenna due to the high radiofrequency levels in the vicinity.

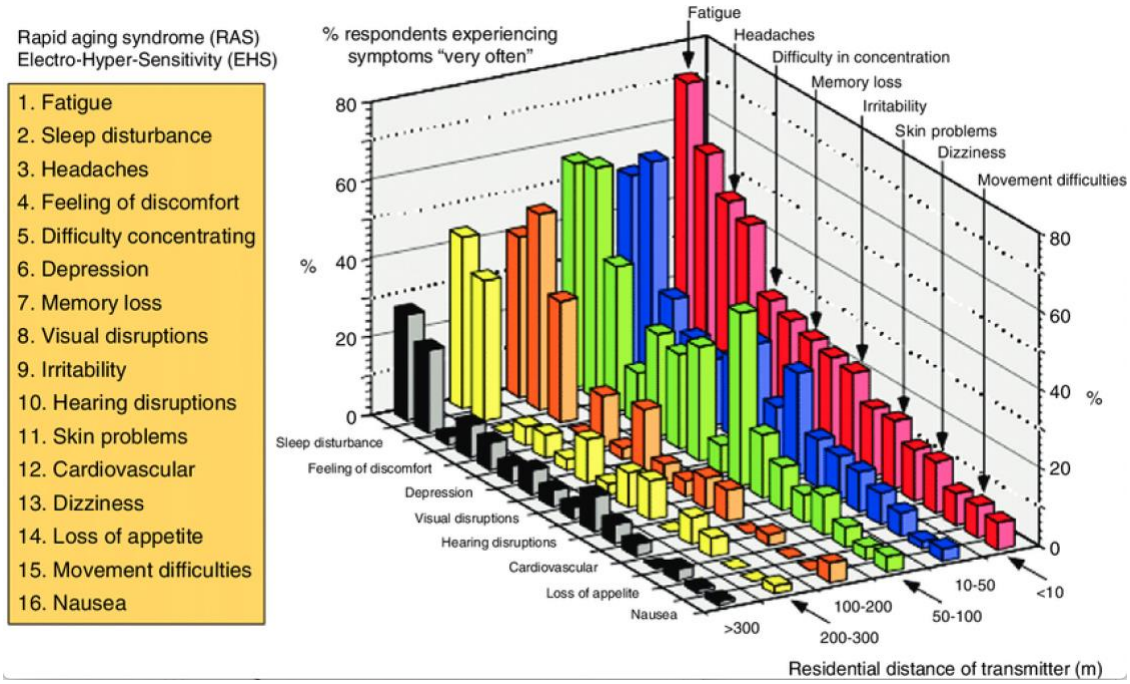
A 2019 Bevington study[11] analyzed the prevalence of symptoms from radiation sickness within any given population. Based on a population of 332.4 million people in the U.S., the numbers are staggering:

Prevalence of EMS Percentages	Number of EMS in U.S.
Can't work – 0.65%	2.16 million
Severe symptoms – 1.5%	4.99 million

[11] The Prevalence of People with Restricted Access to Work in Manmade Electromagnetic Environments, https://mdsafetech.files.wordpress.com/2019/10/2018-prevalence-of-electromagnetic-sensitivity.pdf.

Moderate symptoms – 5%	16.6 million
Mild symptoms – 30%	99.7 million

The following chart shows a worsening of symptoms when closer to a cell tower but a lessening of symptoms when farther away from a cell tower.



Symptoms experienced by people near cellular phone base stations; RF radiation affects the blood, heart and autonomic nervous system.12 Source: Santini, et al (France): Pathol Biol. 2002;50:S369-73. Chart by Magda Havas, PhD.

As the U.S. population becomes increasingly sick from the proliferation and densification of EMR from 4G and 5G installations, there may result a national security risk if there aren't enough healthy individuals to recruit for our military and national defense.

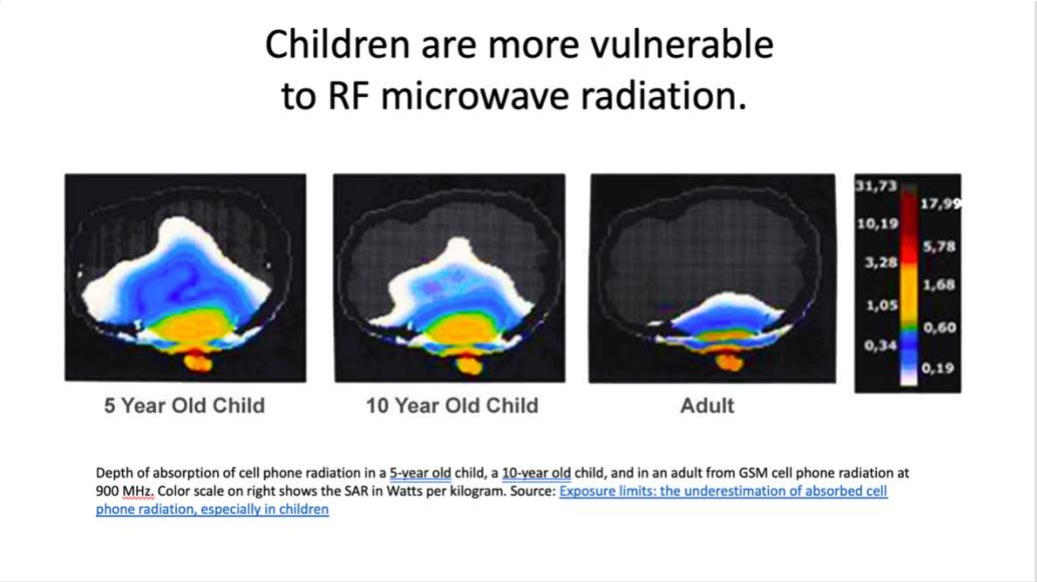
The American Academy of Pediatrics has pointed out that children are disproportionately affected by cell phone radiation due to their lower bone density and amount of fluid in the brain allowing for absorption of greater quantities of RF radiation than in adults.[13]

---

[12] Dr. Magda Havas, https://www.researchgate.net/figure/Symptoms-experienced-by-people-near-cellular-phone-base-stations-based-on-the-work-of_fig2_258313941.

[13] *Key Scientific Evidence and Public Health Policy Recommendations*, Supplement 2012, at 21, David O. Carpenter, MD, Director, Institute for Health and the Environment University at Albany, Cindy Sage, MA, Sage Associates, https://bioinitiative.org/wp-content/uploads/pdfs/sec24_2012_Key_Scientific_Studies.pdf.https://bioinitiative.org/.

Children absorb more RF radiation than adults, and fetuses are at even greater risk.[14] Children's "brain tissues are more absorbent, their skulls are thinner and their relative size is smaller."[15] RF radiation penetrates more deeply into the skulls of children compared to adults,[16] as shown below in cell phone usage.[17]



Source: Exposure limits: the underestimation of absorbed cell phone radiation, especially in children, Gandhi, Morgan, Augusto de Salles, Han, Heberman, Davis, October 14, 2011.[18]

Exposure to RF radiation "can result in degeneration of the protective myelin sheath that surrounds brain neurons" and "[d]igital dementia has been reported in school age children."[19] It also increases the risk of childhood leukemia.[20]

---

[14] *Why children absorb more microwave radiation than adults: The consequences,* Morgan, Kesar and Davis, Journal of Microscopy and Ultrastructure, Vol. 2, Issue 4, December 2014, 197-204, https://www.sciencedirect.com/science/article/pii/S2213879X14000583.

15 Ibid.

[16] See, Dr. Melnick, London 5G Conference at 39:00, https://www.youtube.com/watch?v=zSx_yDzxvM8&t=2295s; https://ehtrust.org/research-on-childrens-vulnerability-to-cell-phone-radio-frequency-radiation/ and https://ehtrust.org/science/scientific-imaging-cell-phone-wi-fi-radiation-exposures-human-body/.

[17] *Exposure limits: the underestimation of absorbed cell phone radiation, especially in children,* Gandhi, Morgan, Augusto de Salles, Han, Heberman, Davis, October 14, 2011, https://pubmed.ncbi.nlm.nih.gov/21999884/.

[18] Ibid.

[19] *Why children absorb more microwave radiation than adults: The consequences,* Morgan, Kesar and Davis, Journal of Microscopy and Ultrastructure, Vol. 2, Issue 4, December 2014, 197-204, https://www.sciencedirect.com/science/article/pii/S2213879X14000583.

[20] *Key Scientific Evidence and Public Health Policy Recommendations*, 2007, at 19, David O. Carpenter, MD, Director, Institute for Health and the Environment University at Albany, Cindy Sage, MA, Sage Associates, https://bioinitiative.org/wp-content/uploads/pdfs/sec24_2007_Key_Scientific_Studies.pdf.

There are also neurological implications to RF radiation exposure for children.[21] Cell towers near schools and Wi-Fi in schools are potentially hazardous to children.[22]

- Elementary school children who were exposed to high levels of RF radiation generated from mobile phone base stations 200 meters from their schools "had a significantly higher risk of type 2 diabetes mellitus" than those exposed to lower RF radiation.[23]

- A ten-year old child testified of his cardiac condition being caused by exposure to RF radiation in a library where he was being tutored.[24]

RF radiation "… has toxic effects in pregnancy, to the fetus and subsequent offspring … and is tied to developmental problems in later life, including attention deficit and hyperactivity."[25]

Children born of mothers who used cell phones during pregnancy developed more behavioral problems by school age than those whose mothers did not use cell phones during pregnancy, with the following results: "25% more emotional problems, 35% more hyperactivity 49% more conduct problems and 34% more peer problems."[26] A study involving 24,499 children found a 23% increase of emotional and behavioral difficulties.[27]

A survey on EMR exposure conducted on several hundred people[28] concluded that although prior to their exposure to EMR they had no problem navigating in the world, after exposure their access to basic services such as hospital care, post offices and libraries became

---

[21] See generally, https://ehtrust.org/research-on-childrens-vulnerability-to-cell-phone-radio-frequency-radiation/; see also, https://ehtrust.org/cell-towers-and-cell-antennae/compilation-of-research-studies-on-cell-tower-radiation-and-health/.

[22] Dr. Magda Havas: WiFi in Schools is Safe. True or False?, https://www.youtube.com/watch?v=6v75sKAUFdc.

[23] *Association of Exposure to Radio-Frequency Electromagnetic Field Radiation (RF-EMFR) Generated by Mobile Phone Base Stations (MPBS) with Glycated Hemoglobin (HbA1c) and Risk of Type 2 Diabetes Mellitus*, Sultan Ayoub Meo et al, International Journal of Environmental Research and Public Health, 2015; https://www.researchgate.net/publication/283726472_Association_of_Exposure_to_Radio-Frequency_Electromagnetic_Field_Radiation_RF-EMFR_Generated_by_Mobile_Phone_Base_Stations_with_Glycated_Hemoglobin_HbA1c_and_Risk_of_Type_2_Diabetes_Mellitus.

[24] Child With Heart Problems From Wireless: 5G Health Risks California SB 649 Hearing, https://www.youtube.com/watch?v=OgNLR9fQOX4&list=PLT6DbkXhTGoDakSqp1i_7milpwGx4xMFq.

[25] Letter by Dr. Beatrice Golomb, Professor of Medicine, UC San Diego School of Medicine, Aug. 22, 2017, https://mdsafetech.org/wp-content/uploads/2017/09/golomb-sb649-5g-letter-8-22-20171.pdf.

[26] *Key Scientific Evidence and Public Health Policy Recommendations*, Supplement 2012, at 8, David O. Carpenter, MD, Director, Institute for Health and the Environment University at Albany, Cindy Sage, MA, Sage Associates, https://bioinitiative.org/wp-content/uploads/pdfs/sec24_2012_Key_Scientific_Studies.pdf.

[27] Miller AB, Sears ME, Morgan LL, Davis DL, Hardell L, Oremus M, Soskolne CL. Risks to Health and Well-Being From Radio-Frequency Radiation Emitted by Cell Phones and Other Wireless Devices. Front Public Health. 2019 Aug 13;7:223. doi: 10.3389/fpubh.2019.00223. PMID: 31457001; PMCID: PMC6701402, also available at https://www.frontiersin.org/articles/10.3389/fpubh.2019.00223/full#B42.

[28] Letter by Dr. Beatrice Golomb, Professor of Medicine, UC San Diego School of Medicine, Aug. 22, 2017, https://mdsafetech.org/wp-content/uploads/2017/09/golomb-sb649-5g-letter-8-22-20171.pdf; Dr. Beatrice Golomb's Curriculum Vitae, https://www.golombresearchgroup.org/pagecv.

restricted. As a result of their injuries, they reported their condition cost them up to 2 million dollars, many lost their homes, and "a number became homeless." [29] Their exposure to EMR became a barrier to access basic services and public anchor institutions. Many had been high-functioning individuals, such as engineers, doctors and lawyers.

> ***"The best and the brightest are among those whose lives – and ability to contribute to society –will be destroyed.*** High profile individuals with acknowledged electrohypersensitivity include, for instance, ***Gro Harlem Brundtland*** – the former 3-time Prime Minister of Norway and former Director General of the World Health Organization; [and] ***Matti Niemela,*** former Nokia Technology chief … [30] [Emphasis added]
>
> "[T]heir problems arose ***due to actions of others, against which they were given no control*** – and can be reversed, in most cases, if the assault on them is rolled back." [31]

RF radiation is analogous to second-hand smoke from cigarettes which is now prohibited. Similarly, individuals should not be subjected to second-hand RF radiation that they do not want or need and to which they did not consent.

G. Wi-Fi is Not Reliable

Wi-Fi is clearly not reliable or resilient as we recently saw with reports of over 70,000 people in the San Francisco Bay area, and others across various states, where a carrier's cellular equipment went down, with no redundancy, and the inability to make a 911 emergency call.[32] One news report stated: "If you are an AT&T customer and cannot get through to 911, then please try calling from a landline."[33]

Copper lines that have served us for a century in our ability to dial 911, are being retired without a resilient substitute.[34] Moreover, if you can't recharge your cell phone in an electrical outage, you can't dial 911. That will make the digital divide look like a digital / communication chasm, with communities across the socio-economic spectrum, not just low-income or rural communities, not having a connection to a phone.[35]

---

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] https://www.nbcnews.com/news/us-news/t-verizon-t-mobile-customers-hit-widespread-cellular-outages-us-rcna139938

[33] Ibid

[34] https://www.mercurynews.com/2024/02/28/opposition-mounts-to-atts-plan-to-stop-landline-service-in-most-of-bay-area/?campaign=sjmnbreakingnews&utm_email=A44A2485044E648595A6E461AE&active=no&lctg=A44A2485044E648595A6E461AE

[35] https://www.smcgov.org/ceo/news/county-demands-answers-att-seeks-cut-landlines

The Communications Act of 1934 made it clear that all of the U.S. must be connected to a phone – a landline. The industry trend has been to cut off the copper landlines. That is the lifeline for many rural communities, which are now being threatened with disconnection.[36] Unfortunately, other areas of the country have already been disconnected, with their only resort to a wireless network which is unreliable given its lack of resiliency.

H. Built-In Obsolescence of Wireless Does Not Make It Resilient

There is a planned, built-in obsolescence to wireless. There is a trend, as reported by an industry publication, where "companies have turned to planned obsolescence to artificially render older products obsolete."[37] It is a tactic used to ensure that tech companies "can consistently turn a profit every time they launch new products."[38]

For instance, the major telecom carriers are already sunsetting their 3G networks, by design, as reported by the FCC. [39] That means that 3G-enabled only phones will become obsolete and consumers will be forced to buy a new cell phone for the new network.[40] It would also apply to other 3G-enabled equipment, such as "medical devices, tablets, smart watches, vehicle SOS services, home security systems." [41] This is artificially creating demand for later generation services, such as 5G as people are forced to buy 5G-enabled cell phones and equipment, and soon 6G and beyond.

Those within the "digital divide" will be experiencing a **perpetual cycle of wireless obsolescence**, as carriers come out with the next "G" as it becomes necessary for more devices to be connected to ever-newer generations of wireless in order for devices to work. Those who cannot afford new devices will be left behind, perpetuating, if not guaranteeing, the digital divide.

Wireless equipment and facilities have a much shorter, 5-year life span, and require continuous periodic maintenance and replacement, compared to wired connections. For instance, there is no planned, built-in obsolescence with copper lines (which have lasted a century), or fiber (which lasts at least 25-50 years), and is therefore more cost effective for underserved communities, ensuring that they are not left behind.

While our attention has been diverted to expanding broadband services to bridge the "divide," our copper lines are being taken away as they are being rendered obsolete while still functional and resilient. This creates an artificial dependence on our cell phones which can prove problematic in case of an emergency during a cellular outage.

---

[36] https://mdsafetech.org/wp-content/uploads/2024/03/PST-Letter-to-CPUC-ATT-Landline-Removal-Proposal-COLR-MArch-4-2024-LTH-PDF-.pdf; https://kymkemp.com/2024/02/23/outcry-against-atts-bid-to-drop-landline-commitments-at-yesterdays-puc-meeting-in-ukiah/

[37] https://cellularnews.com/mobile-phone/planned-obsolescence/.

[38] Ibid.

[39] https://www.fcc.gov/consumers/guides/plan-ahead-phase-out-3g-cellular-networks-and-service.

[40] Ibid.

[41] Ibid.

I. Forcing U.S. Population to Partake in Commerce Activity

Further to working synergistically with other proposed bills that would mandate involuntary exposure to wireless infrastructure that the public does not want or need, violates the Commerce Clause of the U.S. Constitution (Art. 1, Sec. 8, Cl. 3) by (a) interfering with, and creating shot clock and deemed approved deadlines that conflict with, local governments' codes over health, life and safety and open government laws that require adequate notice, time and deliberation for decisions to be rendered, and (b) not providing the public the choice of abstaining, but forcing them to partake in the commerce activity, and suffer the consequences, whether or not they subscribe to that activity.

An example is having a wireless facility close to one's front yard even if not subscribing to the wireless service, yet forcibly exposed to an ugly, radiating facility, that is energy consumptive, environmentally damaging and property devaluing.

J. Cell Towers are Electrical Installations

5G arrays of antennas are reported to run "hot."[42] A lot of heat needs to be dissipated because, as reported in a trade publication, of the amount of equipment, conversions and inefficiencies.[43]

Cell towers are, essentially, electrical installations and should require compliance with strict electrical building codes.[44] There were four notable fires in California that were started in whole or in part by failures or overload of telecommunications equipment. The Guejito Fire in San Diego in 2007, [45] the Malibu Canyon Fire in 2007,[46] the Silverado Fire in 2020, and the Woolsey Fire in 2018 being the worst in California history.[47] The Woolsey Fire caused $6 billion of damage, evacuation of 295,000 people, almost 100,000 acres of land destroyed, and several deaths.

K. Addenda

---

[42] 5G Heats Up Base Stations, https://semiengineering.com/5g-heats-up-base-stations/.

[43] Ibid.

[44] Guest Commentary: Is 5G a Potential Fire Hazard?, Tony Simmons, P.E., The Aspen Times, June 13, 2021, https://www.aspentimes.com/opinion/guest-commentary-is-5g-a-potential-fire-hazard/.

[45] PROTECTING LA COUNTY'S FUTURE: HOW FIRE RISKS FROM TELECOMMUNICATIONS EQUIPMENT, CLIMATE CHALLENGES & A DANGEROUS SHIFT AWAY FROM ENVIRONMENTAL REVIEW THREATEN LOS ANGELES COUNTY'S FUTURE, Susan Foster, November 15, 2022, p. 11.

[46] *California Public Utilities Commission, Incident Investigation Report*, 10/21/2008, at 6, http://file.lacounty.gov/SDSInter/bos/bc/115889_ReportBack-BoardMotion60A-SessionWildfireReport.pdf.

[47] *City of Los Angeles, After Action Review of the Woolsey Fire Incident*, Citigate Associates, LLC, Nov. 17, 2019, at 4, http://file.lacounty.gov/SDSInter/bos/supdocs/144968.pdf; Guest Commentary: Is 5G a Potential Fire Hazard?, Tony Simmons, P.E., The Aspen Times, June 13, 2021, https://www.aspentimes.com/opinion/guest-commentary-is-5g-a-potential-fire-hazard/.

Attached hereto and incorporated by reference is a letter of September 19, 2023 to this Committee about the national security and cybersecurity risks of various bills (Addendum A), and a fact sheet of those bills (Addendum B).

L. Conclusion

For the foregoing reasons, diverting military spectrum for commercial, for-profit uses does not serve our national security or public safety. Therefore, we respectfully request that the Committee review the guidance provided at the beginning of this letter on the bills to oppose and the bills to amend. In that way, our national security and public safety can be better protected.

Respectfully submitted,

On behalf of The National Call for Safe Technology and those joining in this submission, listed below, all of whom have given permission to submit on their behalf

Odette J. Wilkens, Esq.
Chair
The National Call for Safe Technology
Thenationalcall.org
owilkens@thenationalcall.org
646.939.6855

Joining in this submission of comments:

Scott Tips, JD, President
National Health Federation (Mossyrock, WA)

Michael Muadin, President
Alliance for Microwave Radiation Accountability, Inc. (East Chatham, NY)

Ruth Moss
Safe Tech Westchester (White Plains, NY)

Howard J. Goodman, Esq. (Forest Hills, NY)

Sue Peters
New Yorkers 4 Wired Tech (New York, NY)

Tiffany Fletcher (San Diego, CA)

Susan Jennings, MPA BA, Founder
Southwest Pennsylvania for Safe Technology (Mount Pleasant, PA)

Mark Baker, President

Soft Lights Foundation (Beaverton, OR)

The Leto Foundation (Westborough, MA)

Alison McDonough (Cambridge, MA)

Linda Becker (Lincoln, NE)

Cynthia Franklin, Director
Consumers for Safe Cell Phones (Bellingham, WA)

Valerie Borek (Chesapeake City, MD)

Katherine Katzin (Takoma Park, MD)

Paul Heroux, PhD
McGill University (Montreal, Quebec, Canada)

Sheila Resseger, M.A.
5G Free RI (Cranston, RI)

Stop 5G Jax (Jacksonville, FL)
Lisa Lovelady
Searcy Danneheim
Raymur Rachels
Lisa Baker

Safe Tech Tucson (Tucson, AZ)

Lisa Smith, PhD, EMRS
EMF Wellness Tucson (Tucson, AZ)

Jodi Nelson
Californians for Safe Technology (Dahlonega GA)

Julie Levine
5G Free California (Topanga, CA)

Cristina Shonk
Southwest Ohio for Responsible Technology (Cincinnati, OH)

Vicki Sievers
EMF Safety Network: Marin Outreach/Education (San Rafael, CA)

Deborah Shisler (CO)

Jenny DeMarco, Communications Director
Mary Bauer, Retired RF Engineer
Virginians for Safe Technology, LLC (Fredericksburg, VA)

Sara Aminoff (Union City, CA)
Safe Tech International

Kate Kheel (Taneytown, MD)
Safe Tech International

Patricia Burke (Mills, MA)
Safe Tech International

Sharon Behn (Arden, NC)

Longmont for Safe Technology (Longmont, CO)
Doe Kelly, Founder
Kimberly Edmundson
Addie McHale
Marianne Niehaus
Lily Skye
Kim Zimmer
Ana Harrison
Deborah Rutt

Greg Jensen
Patriots Serving Patriots (Longmont, CO)

Donna DeSanto Ott, PT DPT MS, President
Pennsylvanians for Safe Technology (Reading, PA)

Ingrid Iverson
LaPlata for Safe Technology (La Plata, CO)

Kristie Sepulveda-Burchit
Educate. Advocate. (Guasti, CA)

Charlene Hopey (Topanga, CA)

Gene Wagenbreth (Topanga, CA)

Floris R. Freshman (Scottsdale, AZ)

Amy Harlib (New York, NY)

Andrea Mercier
Nancy Van Dover DVM, OMD, Dipl Acup
Coloradans for Safe Technology (CO)

Susie Molloy (Snowflake, AZ)

Frances Miriam Reed (Ashland, OR)

ADDENDUM A

FACT SHEET
BILLS THAT JEOPARDIZE NATIONAL SECURITY AND CYBERSECURITY
September 30, 2023

The following bills will jeopardize national security and will impair national infrastructure resilience and cybersecurity. Set forth below are the most dangerous provisions in these bills and recommendations to vote against or support amendments for the most problematic sections. The National Call for Safe Technology is a coalition of over 100 organizations and individuals advocating for technology that, among other things, preserves individual privacy and security.

- **S 1648 / HR 682: Diverting spectrum from the military. Disapprove.**
  - Makes military spectrum available for commercial uses, now used for critical national security (e.g., military satellites, NASA, NOAA, military aircraft telemetry, air defense missile system). Risks hacking of military communications. Neither bill was referred to Armed Services Committee. No impact study on nat'l security.
- **HR 1123: Studying cybersecurity vulnerabilities should include 5G. Approve only with amendments**
  - Expressly excludes 5G from cybersecurity study without justification. Dept of Commerce (NTIA) to do the study, even though it lacks expertise in cybersecurity. Significant security risks of 5G networks are well documented.[48] **The "5G Paradox:" increased efficiency increases security risks[49] – 5G's inherent design flaw.**

[48] *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/.

[49] https://www.lawfaremedia.org/article/lawfare-podcast-tom-wheeler-and-dave-simpson-making-5g-secure.

- **Amend** section 405 to expressly include 5G and direct DHS/CISA, who have expertise, to conduct study; if NTIA conducts the study, then must get DHS input and sign-off.[50]

- **HR 4510: NTIA Reauthorization Act. Approve only with amendments**
  - Subordinates the Pentagon to centralized authority of the NTIA and FCC by requiring them and other federal users (e.g., DOD, FAA) to first submit comments to NTIA who will filter and summarize them for FCC. For DOD, creates security risks and risks of connectivity interruptions for DOD operators.[51] Includes HR 3557, 4141, 1123.
  - **Delete** Title II (to remove creating new bureaucracy for reallocating spectrum for commercial uses) and section 406 (to remove taxpayer subsidy to promote mobile network standard, not as cybersecure as wired). **Delete** HR 3557 and 4141 language. **Amend** section 405 to expressly include 5G and direct DHS/CISA to conduct this study.
- **HR 1338: Greenlighting unlimited additional satellites. Disapprove.**
  - Subordinates assessing national security risk of satellite deployment to FCC (not qualified). Will exponentially increase satellite launches and space debris, with 25,000 collision avoidance maneuvers already recorded for Starlink Dec 2022 – May 2023.[52] Requires FCC to fast-track commercial satellite approvals (60,000 pending) with licenses that almost never expire. Unsustainable.
- **HR 3565: Reauthorizing FCC spectrum auction authority. Approve only with amendments**
  - **Delete** Titles IV, V, VI, VII, VIII in order to preserve spectrum for federal users, and not allow FCC to ignore comments from federal users. **Amend** section 901 to define broadband as a wired connection.
- **HR 1353: Granting FCC emergency spectrum power. Approve only with amendments**
  - Allows FCC to grant military spectrum for commercial use in emergencies. Compels military to expend resources on commercial interests. With no time limits, can be used as a backdoor for reallocating spectrum without going through proper legal channels, and subverting national security.
  - **Amend:** Authority must be a) limited to spectrum that is already approved for commercial purposes, b) only for bona fide emergencies and c) time-limited.

https://www.TheNationalCall.org; hello@thenationalcall.org

[50] https://www.cisa.gov/sites/default/files/publications/open-radio-access-network-security-considerations_508.pdf.

[51] https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_study_04.03.19.pdf.

[52] https://www.space.com/starlink-satellite-conjunction-increase-threatens-space-sustainability.

ADDENDUM B

Hon. Maria Cantwell, Chair
Senate Committee on Commerce, Science & Transportation

Hon. Ted Cruz, Ranking Member
Senate Committee on Commerce, Science & Transportation

Hon. Jack Reed, Chair,
Senate Armed Services Committee

Hon. Roger Wicker, Ranking Member,
Senate Armed Services Committee

Hon. Gary Peters, Chair
Senate Committee on Homeland Security

Hon. Rand Paul, Ranking Member
Senate Committee on Homeland Security

Hon. Ben Ray Lujan, Chair
Senate Subcommittee on Communications, Media, and Broadband

Hon. John Thune, Ranking Member
Senate Subcommittee on Communications, Media, and Broadband

Hon. Mike Rogers, Chair
House Armed Services Committee

Hon. Adam Smith, Ranking Member,
House Armed Services Committee

September 19, 2023

Re: National Security Risks of S.1648 (HR 682), HR 1123, HR 1353, HR 4510, HR 3565, HR 1338

Dear Chairs Cantwell, Reed, Peters, Lujan, and Rogers, and Ranking Members Cruz, Wicker, Paul, Thune, Smith:

You will soon be asked to support six dangerous bills— S.1648 (HR 682), which is already on the legislative calendar for the full Senate, HR 1123, and HR 1353, which have already passed the House and are before the Senate Commerce Committee, and three others likely to arrive soon in the Senate, HR 4510, HR 3565, and HR 1338, which passed unanimously out of committee in the House.

Please be forewarned. These bills will jeopardize national security and homeland security and together with HR 3557, and other wireless industry-drafted bills, will impair national infrastructure resilience and cybersecurity--all for the narrow commercial benefit of the wireless industry. This

memo documents the most dangerous provisions in these bills and urges that you either vote against them or support amendments to these bills for the most problematic sections, as set forth below.

These bills concern serious national, homeland, and cyber security issues which are so grouped below. A summary of the recommendations are listed first, followed by the issues.

The National Call for Safe Technology is a coalition of over 100 organizations and individuals advocating for technology that preserves individual privacy and security. The preservation of those principles would be affected by any threats to cybersecurity or to our national security.

Summary of Recommendations:

- **S. 1648 (HR 682): Disapprove.**
- **HR 1338: Disapprove.**
- **HR 3565: Approve only with amendments**
  - Delete Titles IV, V, VI, VII, VIII to preserve spectrum for federal users, and not allow FCC to ignore input from federal users.
  - Amend section 901 to define broadband as a wired connection.
- **HR 1353: Approve only with amendments**
  - Authority must be a) limited to spectrum that is already approved for commercial purposes, b) only for bona fide emergencies and c) time-limited.
- **HR 1123: Approve only with amendments**
  - Amend section 405 to expressly include 5G and to direct DHS/CISA to conduct the cybersecurity study. If it is not practical for DHS to conduct this, at a minimum require Department of Commerce to incorporate input and obtain signoff from DHS.
- **HR 4510: Approve only with amendments**
  - Delete Title II in its entirety to avoid creating new bureaucracy dedicated to reallocating federal spectrum to commercial users.
  - Amend section 404(c) to include educating the public and local governments on the cybersecurity risks of wireless networks and the cybersecurity benefits of wired networks (such as fiber optics).
  - Amend section 405 (same text as HR 1123) to expressly include 5G and direct DHS/CISA to conduct the cybersecurity study of mobile networks. If it is not practical for DHS to conduct this study, at a minimum, require Department of Commerce to incorporate input and obtain signoff from DHS/CISA.
  - Delete section 406 to remove a taxpayer subsidy to promote a new mobile network standard that carries additional security risk.

National Security Risks

S. 1648/ HR 682 (Launch Communications Act) – Diverting Spectrum from the Military
Disapprove.

- S 1648 makes spectrum available for commercial satellite use in three frequency bands; these bands are currently used for critical national security uses, including military

satellites, NASA, and NOAA (2025-2110 MHz);[53] military aircraft telemetry (2200-2290 MHz);[54] and the National Missile Defense Program (2360-2395 MHz)[55], among other uses.

- HR 682 is similar; in addition to the three bands above it makes a fourth band available which is used for the air defense missile system (5650-5925 MHz).[56]
- These activities are critical functions for national security and should not be subverted for or subordinated to commercial purposes. According to Congress.gov, neither bill has been referred to the Armed Services committee for review in either chamber, nor does the House report indicate any consideration of the impact of these bills on, or input from, the national security community.[57]
- In addition to national security users losing access to these frequencies, the spectrum under these bills would be shared for commercial and defense purposes, creating new vulnerability for hacking military communications by domestic or foreign actors, or accidental encroachments by commercial users sharing spectrum.
- Proponents might argue that spectrum under these bills is only being made occasionally for launches: however given the 5-year lifespan of low Earth orbit satellites,[58] and 70,000 applications already received,[59] commercial providers impliedly anticipate at least 14,000 satellites launched per year, just for maintaining the network. The "sharing" of spectrum from national security users would be a daily occurrence, not occasional.

HR 1338 (Satellite and Telecommunications Streamlining Act) -- Green Lighting Unlimited Additional Satellites
Disapprove.

- Requires the FCC to fast-track approvals of commercial satellites, including 60,000 applications already pending,[60] and requires that these licenses almost never expire.
- Subordinates national security interests by leaving FCC to decide whether or which satellite deployments pose a national security risk.
- Will increase exponentially the number of satellite launches, satellites in orbit, and collision avoidance maneuvers in space, threatening critical national security infrastructure in space. Starlink made 25,000 collision avoidance maneuvers in just six months from Dec 2022 to May 2023, "to avoid potentially dangerous approaches to other spacecraft and

[53] https://www.ntia.doc.gov/files/ntia/publications/compendium/2025.00-2110.00_01MAR14.pdf

[54] https://www.ntia.doc.gov/files/ntia/publications/compendium/2200.00-2290.00-01MAR14.pdf

[55] https://www.ntia.gov/files/ntia/publications/compendium/2360.00-2390.00_01MAR14.pdf

[56] See paragraph 96 https://www.federalregister.gov/documents/2021/06/10/2021-11063/allocation-of-spectrum-for-non-federal-space-launch-operations

[57] https://www.congress.gov/118/crpt/hrpt156/CRPT-118hrpt156.pdf

[58] https://www.space.com/spacex-starlink-satellites.html

[59] https://www.congress.gov/118/crpt/hrpt157/CRPT-118hrpt157.pdf

[60] https://www.osstp.org/fcc-analysis

orbital debris, according to a report filed by SpaceX with the U.S. Federal Communications Commission (FCC) on June 30."[61,62]

- Orbital debris alone already threatens national security infrastructure, according to GAO.[63] Experts say that it will only get worse with more satellite launches, as the steep increase in maneuvers "follows an exponential curve leading to concerns that safety of operations in the orbital environment might soon get out of hand."[64]
- As described above, we can anticipate at least 14,000 satellites launched per year, just for maintaining the network.[65] The continuous launching of thousands of satellites without regard to national security or safety in orbit from debris and other satellites, is unsustainable, and it is only a matter of time when U.S. and foreign countries' satellites collide to pose potentially dangerous national security threats.

HR 3565: (Spectrum Auction Reauthorizing Authority) -- Reauthorizing FCC Auction Authority

Approve only with amendments

- Delete Titles IV, V, VI, VII, VIII in their entirety to preserve spectrum for federal users, and not allow FCC to ignore input from federal users.
- Amend section 901 to define broadband as a wired connection.

The issues with HR 3565:

- Reauthorizes FCC spectrum auction authority, which lapsed in March 2023 after objections from the military.
- Prepares for a spectrum auction of 3.1-3.45 GHz, which is currently used for defense purposes, and which Congressional Research Service reported would cost the Pentagon "hundreds of billions of dollars" to relinquish in order to be re-purposed for commercial use.[66]
- Paves the way to repurpose additional military spectrum for commercial use which could disrupt military operations Seeks to make available 4.4-4.94 GHz for commercial use, which is currently used by all branches of the military, including for controlling drones, and by Department of Energy for counterterrorism known as the "Nation's Nuclear Fire

[61] https://www.space.com/starlink-satellite-conjunction-increase-threatens-space-sustainability

[62] GAO discussed orbital debris in a November 2022 report

https://www.gao.gov/products/gao-23-105005

[63] GAO reported in a September 2022 report: "Debris in space can [affect] national security."

https://www.gao.gov/products/gao-22-105166

[64] https://www.space.com/starlink-satellite-conjunction-increase-threatens-space-sustainability

[65] https://www.space.com/spacex-starlink-satellites.html

[66] At a September 2022 NTIA Spectrum Policy Symposium, DOD's CIO noted "it would take us two decades and hundreds of billions of dollars to be able to refactor and move those radars out of there." https://sgp.fas.org/crs/misc/IF12351.pdf.

Department";[67] also seeks to make available 7.125-8.5 GHz, which is used by the Defense Satellite Communications System and the Space Force.[68]

- Contains identical provisions as HR 4510 (section 202 as described below), which subordinates input from federal users, via NTIA, during FCC spectrum reallocation rulemaking.
- Encourages applications for broadband grants that may be used on substandard, insecure wireless infrastructure.

HR 1353 (Advanced Local Emergency Response Telecommunications Parity Act) -- Granting FCC Emergency Spectrum Power

Approve only with amendments:

- Authority must be a) limited to spectrum that is already approved for commercial purposes, b) only for bona fide emergencies and c) time-limited.

The issues with HR 1353:

- Allows the FCC to grant commercial access to spectrum, otherwise used for national security, on an emergency basis, and forces national security users to engage with commercial providers to consider these uses.
- Although the purported purpose is for the spectrum to be used on an emergency basis, this bill (a) compels the military to expend resources on commercial interests and (b) does not require that commercial entities act in the interest of national security.
- With no time limits, this bill could be used as a backdoor for reallocating spectrum without going through the usual process, and unintentionally or unknowingly subverting national security interests.

Cybersecurity Risks

HR 1123 (Understanding Cybersecurity of Mobile Networks Act) — Undermining Infrastructure and Cyber-Security

Approve only with amendments:

- Expressly include 5G in the study of cyber security vulnerabilities of mobile networks.
- Direct that DHS/CISA conduct this study. If it is not practical for DHS to conduct this study, at a minimum, require Department of Commerce to incorporate input and obtain signoff from DHS.

The issues with HR 1123:

- Expressly excludes 5G from a Department of Commerce study on cybersecurity risks without justification for doing so. In fact, there is much justification for including 5G

[67] http://web1.see.asso.fr/ICTSR1Newsletter/No003/Band Range 4point4 thru 4 point 99 (1).pdf

[68] https://www.fcc.gov/sites/default/files/SpectrumSharingReportforTAC%20%28updated%29.pdf

because a) it comprises a substantial portion of today's mobile networks and b) it poses significantly higher cybersecurity risks. The security vulnerabilities of 5G networks are well documented. 5G is a distributed, software-based network of digital routers with thousands of nodes and access points that a hacker can exploit; there is no choke point control to quarantine security breaches.[69] If a hacker gains control of the 5G software managing the networks, the hacker can also control the 5G network.[70] The FCC recognized early on the need to address the security vulnerabilities of 5G.[71] Former FCC Chairman and former CTIA CEO Tom Wheeler points out that "5G networks are more vulnerable to cyberattacks than their predecessors."[72]

- Nominates the Assistant Secretary of Commerce for Communications and Information to conduct the study when the Department of Homeland Security (DHS) and its Cybersecurity and Infrastructure Security Agency (CISA) have far greater domain expertise and independence from influence of the wireless industry. There is no need to create competition and incoherence among federal agencies, when one agency is already responsible for this critically important task. The mission of Department of Commerce is to promote industry,[73] whereas the mission of DHS is to protect national security.[74] CISA is better suited for the task as it is already responsible for "overseeing 16 critical infrastructure sectors, communications being one."[75]
- Supports and accelerates increasing reliance and dependence on wireless-based infrastructure, which will impair resilience and increase vulnerability at all levels of government—federal, state, and local—to cyberattacks. Local communities are highly vulnerable and prime targets for cyber-attacks. For instance, in NYC, it was pointed out at length in a 2020 letter from the Chief Technology Officer and Chief Information Security Officer of NYC to the National Telecommunications and Information Administration (NTIA).[76] A Brookings Institution report points to the "5G Cyber Paradox," because as

---

[69] *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/; see also, *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.

[70] *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/.

[71] https://docs.fcc.gov/public/attachments/DOC-343096A1.pdf.

[72] *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/.

[73] Department of Commerce's mission is to "strengthen domestic industry"

https://www.commerce.gov/about

[74] https://www.dhs.gov/mission

[75] https://www.brookings.edu/articles/protecting-the-cybersecurity-of-americas-networks/.

[76] https://www.dropbox.com/scl/fi/0cxjktjxstmb825gqih25/NYC-Comments-5G-to-NTIA-6-25-20.pdf?rlkey=dgmc3m04dxd57qfz7z1g12ckh&dl=0. The letter states, in relevant part: "Such complex systems [5G] present more opportunities for security and privacy breaches. By moving away from firmware-based technology of 4G telecommunication components to software-based 5G telecommunication components that will need to be updated, the opportunity for manipulation exists within the supply chain. Furthermore, movement away from

5G networks "improve the efficiency and capabilities of the communications infrastructure… they introduce new security vulnerabilities that threaten both the networks and those who rely on network connectivity."[77] This can also imperil national security and homeland security. This appears to be a design flaw inherent in 5G architecture and execution. Therefore, there is ample justification that the study of the cyber security of 5G protocols and networks should be expressly **included** in the bill. No report on mobile networks could be considered comprehensive without including 5G, which makes up an increasingly large part of wireless networks today and in the future.

HR 4510 (NTIA Reauthorization Act of 2023) —Subordinating the Pentagon to Centralized Authority of the NTIA and FCC

Approve only with amendments:

- Delete Title II in its entirety (which includes section 202 referenced below) to avoid creating new bureaucracy dedicated to reallocating federal spectrum to commercial users.
- Amend section 404(c) to include educating the public and local governments on the cybersecurity risks of wireless networks and the cybersecurity benefits of wired networks (such as fiber optics).
- Amend section 405 (same text as HR 1123) to expressly include 5G and direct DHS/CISA to conduct the cybersecurity study of mobile networks. If it is not practical for DHS to conduct this study, at a minimum, require Department of Commerce to incorporate input and obtain signoff from DHS/CISA.
- Delete section 406 to remove a taxpayer subsidy to promote a new mobile network standard that carries additional security risk.[78]

The issues with HR 4510:

- Incorporates HR 1123 language. All issues cited above for HR 1123 are incorporated hereby reference.
- Subordinates all federal spectrum users, including Dept of Defense (DOD), by requiring them first to submit their comments to NTIA, which in turn will filter and summarize them for FCC (as set out in section 202).
- Allows the FCC, when engaging in rulemaking to reallocate spectrum from other federal users, such as Dept of Defense (DOD) and the Federal Aviation Administration (FAA) to

centralized network systems to decentralized network systems increases the attack surface of a network. That increased attack surface is amplified by the anticipated introduction of the increasing number and variety of connected devices (IoT) and big data industries … The problem of IoT vulnerabilities will only become exacerbated by the increased speeds of 5G and other future wireless broadband technologies … IoT protection is historically poor and malware distribution is easily scalable, which suggests that the creation of IoT botnets ("robot networks") for malicious purposes, including large-scale distributed denial of service (DoS) attacks, is likely to increase as well. This poses a significant threat to vital digital infrastructure and resident services at all levels of government, as well as private sector enterprise."

[77] https://www.lawfaremedia.org/article/lawfare-podcast-tom-wheeler-and-dave-simpson-making-5g-secure.

[78] https://www.cisa.gov/sites/default/files/publications/open-radio-access-network-security-considerations_508.pdf

commercial uses, to ignore comments and record evidence from other federal agencies, unless they are filtered through NTIA. For instance, if DOD is required to share its spectrum, it "will create … security vulnerabilities" and increase "the risk of connectivity interruptions for DOD operators."[79]

- Incorporates language from HR 1345 (NTIA Policy and Cybersecurity Act) for the NTIA to develop policies that promote "security and resilience to cybersecurity incidents,"[80] even though the NTIA does not have expertise in cybersecurity.
- Codifies in statute and expands the scope of NTIA's Institute for Telecommunication Sciences (ITS), with a mandate to "promote activities relating to access to federal spectrum by nonfederal users" and facilitate ways to "enhance" sharing electromagnetic spectrum between federal and nonfederal users. In other words, ITS would include an office of the bureaucracy dedicated to finding ways to reallocate spectrum away from national security users and make it available for commercial purposes. Note: HR 1343 contains identical language expanding ITS and already passed unanimously in the House and is currently pending before the Senate Commerce Committee.
- Allows ITS to receive direct payments and royalties from industry, which ITS can use for its own budget and for direct payments to government employees. The bill also creates an NTIA slush fund to receive payments from industry which can be spent at the discretion of the Assistant Secretary of Commerce. In effect, NTIA and its individual employees could be paid by industry to facilitate taking spectrum away from national security users, creating an irreconcilable conflict of interest between these commercial payments on the one hand and, on the other hand, national security, homeland security, and cybersecurity.
- Incorporates language from HR 1340 (Open RAN Networks Act), which promotes a new mobile network standard that could lead to "severe security" issues.[81]

This letter has summarized serious cybersecurity and national security risks. Your immediate action is requested.

Respectfully,

National Call for Safe Technology
https://www.TheNationalCall.org
hello@thenationalcall.org

[79] https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_study_04.03.19.pdf

[80] https://www.congress.gov/bill/118th-congress/house-bill/1345.

[81] https://www.sciencedirect.com/science/article/pii/S1084804523000401