Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security	)	WC Docket No. 18-89
Threats to the Communications Supply	)	
Chain Through FCC Programs	)	
	)	

COMMENTS OF USTELECOM – THE BROADBAND ASSOCIATION

Michael D. Saperstein, Jr.

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

February 3, 2020

Table of Contents

Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security	)	WC Docket No. 18-89
Threats to the Communications Supply	)	
Chain Through FCC Programs	)	
	)	

COMMENTS OF
USTELECOM – THE BROADBAND ASSOCIATION

USTelecom – The Broadband Association (USTelecom)[1] submits these comments in response to the Federal Communications Commission's (Commission) Further Notice of Proposed Rulemaking (FNPRM) in the above-captioned proceeding. The FNPRM proposes additional measures to prevent the use of communications equipment or services from suppliers that pose a national security risk to U.S. communications networks or the communications supply chain.[2] USTelecom supports the Commission's efforts to highlight and mitigate potential security risks in the information and communications technology and services (ICTS) supply chain as a part of well-coordinated whole-of-government approach and public-private effort among multiple agencies and industry stakeholders. We offer these comments as an active and constructive partner with the federal government on these and other cybersecurity issues.

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

[2] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Report and Order, Further Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC 19-121 (rel. Nov. 26, 2019) ("Report and Order" and "FNPRM").

I. Introduction: USTelecom Promotes Leadership and Partnership with the Commission and the U.S. Government on Supply Chain Security

USTelecom commends the Commission for engaging with industry and with the federal interagency process to secure the ICTS supply chain. This opportunity for industry to provide input on the Commission's proposed initiatives is crucial to our collective efforts to implement these profoundly important new policies with precision and positive effect.

For years, USTelecom has played a prominent leadership role in developing and advancing U.S. cybersecurity policy in general and in the communications sector in particular. We helped the National Institute of Standards and Technology (NIST) develop the Cybersecurity Framework, and we led the Commission's fourth Communications Security, Reliability, and Interoperability Council's (CSRIC IV) landmark effort to implement the Cybersecurity Framework in the communications sector. USTelecom also founded, and presently co-leads with the Consumer Technology Association, the Council to Secure the Digital Economy (CSDE), a group of over a dozen large international ICTS companies dedicated to the security of our communications infrastructure and connected digital ecosystem. CSDE is recognized by this Administration as a leading industry partnership in coordinating efforts to combat botnets, to respond to cyber crises, and promote IoT security. Finally, USTelecom chairs both the Communications Sector Coordinating Council (CSCC) and the Supply Chain Risk Management Task Force (SCRM Task Force), the two principal organizations that serve as the government's industry partners for developing cybersecurity and supply chain security policies.

USTelecom is well-placed to provide constructive suggestions to guide the Commission as it considers whether and how to take further action in this proceeding. We submit these comments in partnership with the Commission and the Administration, and with our eyes wide open about the sophisticated supply chain threats that we face together. Our suggestions derive

from our belief that the foundational supply chain security regimes that are presently in their nascent stages of development must be built with solid cornerstones: Industry partnership; rigorous, discerning risk analysis; clear definitions of terms; and interagency coordination pursuant to sound and predictable processes. We urge the Commission to partner with industry leaders and other agencies to promote ICTS supply chain security.

As we have stated publicly and demonstrated through our own work, we believe deeply in formal collaborative efforts between industry and the various agencies of our federal government. These partnership efforts should feed into the Commission's consideration and implementation of any further rules it may adopt; indeed, this is the only approach that will be effective in securing the ICTS supply chain. In particular, the Commission's implementation of the Report and Order and its exploration of the FNPRM should highlight the work of the CSCC and the SCRM Task Force. The CSCC engaged meaningfully with DHS in contributing to the assessment required under Section 5(b) of Executive Order (EO) 13873, and going forward, industry – through the CSCC and other pertinent Sector Coordinating Councils – should have strong and clear roles to continue to contribute to future updates of this annual assessment, as well as future additional assessments that address other sectors. The SCRM Task Force, the only formal industry-government collaboration on supply chain security, is presently beginning to develop recommendations for legal and procedural mechanisms to govern industry's sharing with government of derogatory information regarding specific suppliers and transactions. These recommendations will address existing legal and procedural gaps that presently handicap the government's effective implementation of these developing new authorities.

USTelecom urges the Commission to leverage the expertise and institutional contributions of these partnerships. Balancing the inseparably intertwined national security and

commercial interests in the ICTS supply chain requires substantial and continual federal government coordination. It is critical for the Commission to closely coordinate all of its actions in this field across the federal government, including with the Department of Homeland Security (DHS), the Department of Commerce, and the agencies of the Intelligence Community (IC), to make its determinations about appropriate prospective restrictions and remedial measures where suspect equipment exists today.

USTelecom's previous comments in this proceeding highlighted this fundamental principle of whole-of-government coordination and industry-government partnership, and given the profound ICTS supply chain policy and security developments of the nearly two years since those comments were filed, we underscore and further elaborate on this principle here. In short, USTelecom urges the Commission to continue and enhance its participation in well-coordinated U.S. government efforts to promote a diverse, competitive market of trusted ICTS suppliers.

Additionally, we reiterate two other guiding principles that we addressed in our 2018 comments: First, that the Commission's restrictions on the use of USF funding should be prospective, taking into account existing equipment and ensuring a level playing field in the market; and second, that the Commission should confine the scope of any rule to apply only to equipment and services funded through the USF in order to stay clearly within the bounds of its legal authority. Finally, we emphasize an additional guiding principle of ensuring that the Commission's implementation of the replacement requirements in the FNPRM do not bring about "unfunded mandates." In short, USTelecom urges the Commission to take careful and sure-footed steps in this proceeding.

II. USTelecom Urges the Commission to Support Well-Coordinated U.S. Government Efforts to Promote a Diverse, Competitive Market of Trusted ICTS Suppliers

USTelecom and its members fully recognize the potential for certain suppliers to become dominant in the global ICTS market notwithstanding security concerns. The present relative paucity of U.S.-based suppliers in this market, particularly regarding Radio Access Network (RAN) hardware, is a challenge that we are acutely aware of and seeking to address, for instance through our members' support of "open RAN" initiatives.[3] Curtailing the use of questionable suppliers is only the first step in securing the ICTS supply chain; over the long term, we must also ensure that a vibrant market of trusted suppliers continues to exist and grow. We encourage the U.S. government and allies to align on security requirements which will maintain sufficient demand for a globally competitive market of trusted suppliers. Having multiple options for 5G network suppliers, for instance, significantly reduces the chance that a single state-backed dominant supplier could use its position for nefarious purposes, putting at risk national security, consumer privacy and commercial intellectual property. We strongly support efforts to increase funding via research grants to grow trusted domestic suppliers over the long term.[4]

Within the U.S. government, the Commission's activities in this proceeding are directly pertinent to this broader global effort and should be undertaken with its federal partners and with industry leaders with this long-term goal in mind. The U.S. government is presently engaged in multiple other significant efforts of various scope and maturity to promote the security of the

[3] *See, e.g.*, the work of the O-RAN Alliance to promote open and interoperable interfaces and virtualization in the RAN, *available at* https://www.o-ran.org/.

[4] *See, e.g.*, the bipartisan Utilizing Strategic Allied Telecommunications Act, which would create a $750 million research and development fund, and a $500 million program to encourage adoption of equipment from trusted vendors worldwide.

ICTS supply chain, particularly in the communications sector. The following policy activities are directly pertinent to the Commission's proceeding:

- The Commerce Department has proposed rules that would establish processes to implement its authorities under EO 13873 to evaluate and potentially prohibit, mitigate or unwind certain private commercial ICTS transactions;

- The Office of Management and Budget, the General Services Administration, and the Department of Defense are implementing the prohibitions in Section 889 of the John S. McCain National Defense Authorization Act (NDAA) of 2019 on federal procurement from Huawei and ZTE, and from entities that "use" Huawei and ZTE;

- The Federal Acquisition Security Council (FASC) is expected to issue rules regarding future "exclusion orders" for federal procurement;

- The Department of Defense is implementing its Cybersecurity Maturity Model Certification (CMMC) program for defense contractors;

- The National Telecommunications and Information Administration (NTIA) and other stakeholders are continuing a process to advance a software supply chain security and transparency (*i.e.*, a "software bill of materials"); and

- The industry-government SCRM Task Force—which, as mentioned above, USTelecom co-chairs—is presently embarking on its second year, with several work streams underway that are directly pertinent to this proceeding.

With these multiple and interrelated activities in mind, USTelecom applauds the Commission's statement supporting a "whole of government approach to supply chain security."[5] To promote the coherence of the "whole of government" approach to ICTS supply chain security and to maximize the impact of industry's real-world implementation of ICTS supply chain risk management measures, the Commission should implement its prohibitions under the Report and Order and any additional steps under the FNPRM in close coordination with these related supply chain security activities. The Commission's actions in this proceeding will affect these other processes – and vice versa. USTelecom welcomes the FNPRM's request

[5] Report and Order ¶ 73.

for comment on how specifically the Commission can ensure that its efforts in this proceeding "are consistent and in harmony with" these parallel activities,[6] and we offer the following specific recommendations.

First, the Commission has given discretion to the Public Safety and Homeland Security Bureau (PSHSB) about whether to rely on the designations of other agencies or to act unilaterally. We are encouraged that in the case of the preliminary designations of Huawei and ZTE as "covered" companies, the Commission relied on the significant public record of various agencies and Congress to make those designations. With that example in mind, we believe any future designation determinations that would cut off certain suppliers deemed to be a threat to U.S. national security should always require a similarly robust and well-documented whole-of-government coordinated determination. Unilateral determinations made by the Commission in a vacuum would be dangerous and counterproductive. For example, DHS has a dedicated ongoing effort to assess threats to the supply chain, the purpose of which is to inform U.S. policy and operational decisions. The Commission should formalize its substantive and procedural requirements for coordination with other pertinent agencies, as well as industry stakeholders, in each potential designation under this proceeding. As we suggested late last year, USTelecom urges the Commission to require PSHSB to "conduct an annual report surveying other federal entities … to determine what, if any, communications supply chain entities are designated as national security threats" and to provide recommendations to the Commission to harmonize any discrepancies between the Commission's designations and other agencies' designations.[7]

[6] FNPRM ¶ 160.

[7] Letter from Mike Saperstein, Vice President, Policy & Advocacy, USTelecom, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Nov. 15, 2019).

Second, with regard to the Commerce Department's ICTS supply chain security proceeding under EO 13873, we are pleased that the proposed rules would require the Commerce Secretary to consult with the FCC Chairman and other heads of agency in any transaction evaluation. Additionally, the proposed rules provide the FCC Chairman the authority to request in writing that the Commerce Secretary should conduct a transaction evaluation. If the Chairman of the FCC makes such a request—for instance, as a follow-up to this proceeding outside the USF context—USTelecom believes that any such request should spell out in detail the Chairman's factual and analytical reasoning for why the Chairman believes the transaction calls for a Commerce Department assessment of the risk criteria listed in those rules, and written notice should be provided to the other participant agencies listed in those rules.[8] More broadly regarding the Commission's consultative role, the Commission should establish the formal procedures by which it provides the Commerce Department and other agencies its information and expertise in implementing these rules to ensure well-coordinated and effective policy action.

Third, as noted above, Section 889 of the 2019 NDAA restricts federal procurement of equipment or services from Huawei and ZTE, and as of August 13, 2020, it will also restrict federal procurement with entities that "use" such equipment or services "as a substantial or essential component" or as "critical technology" of any system.[9] Implementation of these restrictions is directly relevant to Commission's actions in this proceeding, and vice versa. The

[8] *See* Comments of USTelecom before the Department of Commerce, Docket No. 191119-0084, RIN 0605-AA51, 10-11 (filed Jan. 10, 2020) https://www.regulations.gov/document?D=DOC-2019-0005-0046. ("To commence a transaction evaluation pursuant to a "written request" under § 7.100(b), the Secretary should grant requests for a transaction evaluation from other heads of agency or the Federal Acquisition Security Council only in response to a request similar in form and substance to the formal written notice described above through which the Secretary would exercise his own discretion to commence a transaction. The Secretary should then provide notice to the other heads of agency of his decision to grant the request.")

[9] John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong., Pub. Law 115-232, 132 Stat. 1636, § 889 (2018) ("NDAA").

Commission should therefore explain and seek comment on its plans to harmonize its actions under this proceeding with the government's implementation of these restrictions required under the NDAA. Further, under an ongoing statutory procurement proceeding that is separate from but related to the NDAA's restrictions, the FASC and individual agency heads are authorized to issue "exclusion orders" prohibiting certain suppliers from federal procurement. The FASC is expected to issue interim rules to govern this process in early 2020. Again here, the Commission should explain and seek comment on its plans to harmonize its actions under this proceeding with the rules that the FASC issues.

Fourth, the SCRM Task Force is launching an initiative to develop recommendations to govern the sharing between industry and government of critical information regarding suspect suppliers.[10] These recommendations will be directly pertinent to the Commission's designations and other future actions in this proceeding. The Commission should consider and seek public comment on any SCRM Task Force recommendations that touch on Commission authorities or activities.

III. USTelecom Urges the Commission to Take Careful and Sure-Footed Steps in this Proceeding

The supply chain security proceedings, activities, and authorities noted above are collectively—and in some cases individually—extraordinary and unprecedented. Each action taken in these arenas can potentially have far-reaching effects in the global market for ICTS. Effective implementation that maximizes positive impact and avoids negative unintended

[10] *See* Information and Communications Technology Supply Chain Risk Management Task Force, *Interim Report: Status Update on Activities and Objectives of the Task Force* (Sept. 2019) https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf.

consequences will require deep and continual engagement between the government and industry, as well as careful and sure-footed steps at every phase of implementation.

a. Avoid unintended consequences in additional Covered Entity designations.

The Commission should take great care to ensure that a future decision to designate a company as a "covered entity" does not cause negative unintended consequences. Should the Commission in the future designate additional companies as covered entities, then it should assess whether a broad blanket prohibition would have negative unintended consequences. For example, the Commission should determine whether a covered entity produces equipment or services that are innocuous with regard to network security, or whether the company is the sole source of a particular piece of equipment or device. Such assessments are particularly important to the extent the Commission implements a fund to replace equipment from covered entities. Any funding to reimburse carriers for replacement equipment will be put to best use if such replacement is only mandated where necessary for the secure operation of the communications network, not for equipment that is ancillary to network operations or poses no security concern.

b. Effective implementation of the replacement and reimbursement fund.

We begin with our most fundamental and important point on this topic. Under no circumstances should the Commission use USF monies to reimburse carriers for removing covered equipment. Instead, this funding should be provided only by a new appropriation or a separate new stream of statutorily authorized funding. Indeed, Congress is presently considering legislation, which the House of Representatives has already passed, that would establish a reimbursement program under Commission oversight.[11] No legislative proposals currently pending in Congress would use USF monies for reimbursement.

[11] Secure and Trusted Communications Networks Act of 2019, H.R. 4998, (116th Cong.) https://www.congress.gov/bill/116th-congress/house-bill/4998.

We outline our recommendations on additional questions below.

- **Should "component parts" be eligible for the replacement fund? No.**

  Replacing component parts in finished products could be tremendously challenging and complex, and therefore costly. Generally speaking, it is straightforward to replace a piece of finished of equipment produced by a covered entity such as Huawei or ZTE; moreover, to our knowledge, neither Huawei nor ZTE make sub-components of network equipment that are sold as finished products by non-covered vendors. However, if a finished product purchased from a non-covered vendor includes sub-components made by a subcontractor that is in the future determined to be a covered entity, then identifying the sub-component and replacing it would be fraught with practical complications. At the least, doing so could require the supplier to redesign the equipment to accommodate a different component. Moreover, most importantly, at present there is no indication that trusted suppliers are using sub-component parts made by Huawei, ZTE, or other entities suspected of posing national security risks. Before stepping into this complicated area, the Commission should focus the replacement fund on the national security threat it has identified: finished products made by Huawei and ZTE. Further, to the extent that the Commission seeks to determine which particular components of communications equipment should be subject to this prohibition, the Commission should use and explicitly reference the annual DHS risk and criticality assessment required under Section 5(b) of EO 13873.

  Again, application of the prohibitions to sub-component parts made by Huawei and ZTE may not create unintended consequences or compliance issues. However, to the extent the Commission may in the future expand the prohibition beyond these two companies, it should be careful to take into account any unique unintended consequences and compliance burdens associated with prohibiting use of a new entity's equipment or services. For example, a particular company may by the sole source of a particular component or piece of equipment, making replacement difficult if not impossible. Alternatively, a company might be the sole source of a low-cost consumer product, in which case the industry should be given sufficient notice and time to use other providers to deliver consumers low-cost alternatives. With this last example in mind, USTelecom believes that individual consumer devices and handsets should be excluded from the prohibitions—and also ineligible for replacement and reimbursement funding. Individual consumer devices and handsets do not create significant security risks to U.S. networks, and all carriers test them thoroughly before introduction to the market. In addition, devices are owned by the customer, and carriers cannot unilaterally force customers to give them up.

- **Should the removal and replacement fund be limited to ETCs? Yes.**

  First, ETCs are most likely to have covered equipment. Second, such funds should be used to the extent possible to directly address replacement equipment that is prohibited by the Commission. Finally, inclusion of other USF recipients, like rural health care providers and libraries, could put large administrative burdens on the

reimbursement fund without proportional benefit to national security. For example, a school or hospital's (funded by E-Rate or Rural Health Care) use of a ZTE or Huawei tablet, while potentially raising privacy concerns for individuals, does not rise to the level of the national security concerns that this proceeding seeks to address. The Commission should therefore prioritize the reimbursement fund to address national security threats to U.S. networks—that is, the removal of covered equipment in ETC networks. If there is money left over, it can then consider whether to reimburse other USF participants for removal of covered equipment.

- **Should the Commission permit new entities affected by the NDAA to become ETCs for purpose of reimbursement? No.**

  As administered by the Commission, and in the absence of legislation, noted above, the reimbursement fund should be limited only to entities that are ETCs or that become ETCs in order to participate in the Commission's USF programs. Moreover, the NDAA applies to any entity that contracts with the federal government, including non-communications sector companies such as IT companies. Allowing such a wide array of companies to be eligible for the reimbursement fund would place an unneeded burden on the fund, contrary to its purpose, and without commensurate benefit to safeguarding the security and integrity of America's communications infrastructure.[12] Again, the Commission should note that Congress is moving legislation that would establish a reimbursement program, under Commission oversight.

- **Should replacement and reimbursement funding be limited to the equipment and services covered by the NDAA? Yes.**

  The Commission should clarify the scope of the equipment and services to be replaced and how that applies to entities that are both ETCs and non-ETCs via their affiliates. Replacement and reimbursement funding should be focused on critical network equipment rather than ancillary equipment, following Congressional directives. The NDAA articulates that concept, clarifying that its prohibitions do not apply to (1) a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements, or (2) telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles. The NDAA further applies its prohibitions to vendors that use covered equipment and services that are a "substantial or essential component" of or as "critical technology" to a system. The Commission poses a similar question, asking for comment on the necessity of requiring replacement of certain equipment and services where replacement is unnecessary in order to protect national security and is a waste of public funds. We agree that replacement should be focused on critical network technology that, if compromised, would pose a national security risk. That is also why we also

[12] Report and Order ¶ 1.

recommend exclusion of devices from the replacement fund and from the general prohibition in the order itself.

- **Should the Commission require certification for replacement and reimbursement? Yes.**

  USTelecom believes self-certification is a strong mechanism for compliance and administration. An ETC that certifies it is using this funding only to replace covered equipment identified in its reimbursement application and that it is not using this funding for any other purpose creates legal liabilities for itself in the event that its statements are false. USTelecom notes that ¶ 148 of the FNPRM cites Section 254 of the Act, requiring ETCs to use their USF support only for the provision, maintenance and upgrading of facilities and services for which the support is intended. Since the Commission, in our view, absolutely should not use USF monies for this reimbursement fund, this statutory provision is inapplicable; therefore certifications pursuant to this replacement and reimbursement fund should be required independent of Section 254.

c. Focus on the prohibition and replacement of Covered Entities within USF Eligible Telecommunications Carrier (ETC) networks.

The Commission asks whether it should prohibit use of covered equipment from a Covered Entity by companies in their communications networks more broadly outside the USF setting, for instance through CALEA authority. In short, USTelecom believes that the Commission should not attempt such an expansion.

First, there is no need for the Commission to rely on CALEA. Using the USF fund as the leverage to eliminate covered equipment allows the Commission to target the parts of the market that presently use such equipment, while relying on well-established legal authority to condition the receipt of USF funds. In addition, national U.S. carriers are federal contractors and thus are already restricted under the NDAA from using Huawei and ZTE equipment in their U.S. networks. While the Order cites CALEA's section 105 as one of the statutory provisions implemented by the agency's denial of USF funding to providers using equipment from prohibited providers,[13] CALEA is not itself a grant of authority for the Commission to regulate

[13] *Id.* at ¶ 35.

carriers' supply chain decisions. The Order does not rely on CALEA Section 105 for the Commission's authority to act; it merely states that the USF-related ban advances that provision's goals.

CALEA does not and was never intended to provide the Commission authority to regulate the telecommunications supply chain. Section 105 itself merely provides that a carrier's manner of allowing government interception required by CALEA "can be activated only in accordance with a court order or other lawful authorization" and with affirmative intervention of the carrier's employees. This provision cannot be stretched to provide the Commission broad authority to regulate a carrier's supply chain decisions. In fact, Congress made clear that CALEA is not intended to authorize such regulation -- providing in no uncertain terms that CALEA "does not authorize any law enforcement agency or officer . . . to prohibit the adoption of any equipment, facility, service, or feature."[14] The Commission would thus be well advised to avoid relying on CALEA and use its solid existing USF authorities to accomplish its goals.

As discussed above, the approach available to the Commission to influence transactions outside the USF arena that is most likely to promote effective and coherent whole-of-government policy action and minimize negative unintended consequences is a formal request from the FCC Chairman to the Commerce Secretary for a transaction evaluation under the Commerce Department's proposed rules. Again, USTelecom believes that any such request should describe the Chairman's underlying reasoning for the request, and more broadly, the Commission should establish the formal procedures by which it provides the Commerce Department and other agencies its information and expertise in implementing these rules. This would be an appropriate way for the Commission to influence transactions outside the USF arena.

[14] 47 U.S.C. § 1002(b)(1)(B).

Additionally, the Commission asks whether it should expand the replacement requirements to all USF recipients rather than only in ETC networks. For the reasons discussed above, non-ETCs are not a national security priority to this replacement requirement, and should not be subject to replacement requirements nor receive reimbursement funding.

Finally, the Commission asks whether ETCs should be allowed to obtain USF support even if they currently use covered equipment and services so long as they agree to replace such equipment and services by a set deadline. USTelecom agrees that, on the condition that Congress provides separate non-USF funding for replacement and an ETC otherwise complies with the Order, then the answer is yes—ETCs should be eligible for USF support even if they currently use covered equipment and services so long as they agree to replace such equipment and services by a set deadline.

IV. Conclusion

USTelecom supports the Commission's efforts to exercise good stewardship over its USF spending and emphasizes the need for a coordinated, whole-of-government approach to determining the entities and equipment types that constitute communications supply chain risks.

Respectfully submitted,

By: _____

Michael D. Saperstein, Jr.
USTelecom Association
601 New Jersey Avenue, N.W.
Suite 600
Washington, D.C. 20001
(202) 326-7300

February 3, 2020