Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats	)	WC Docket No. 18-89
to the Communications Supply Chain Through	)	DA 20-406
FCC Programs	)	

COMMENTS OF
THE COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION
(CompTIA)

Dileep Srihari
Vice President and Senior Policy Counsel

Savannah Schaefer
Senior Director, Public Advocacy

COMPUTING TECHNOLOGY INDUSTRY
ASSOCIATION (CompTIA)
322 4th Street NE
Washington, DC 20002

May 20, 2020

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats	)	WC Docket No. 18-89
to the Communications Supply Chain Through	)	DA 20-406
FCC Programs	)	

COMMENTS OF
THE COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION

The Computing Technology Industry Association ("CompTIA"),[1] the leading association for the global information technology ("IT") industry, respectfully submits these comments in response to the Wireline Competition Bureau's Public Notice of April 13, 2020 in the above-captioned proceeding.[2]

INTRODUCTION

CompTIA appreciates the Commission's ongoing work to address supply chain security issues, including implementation of the Secure and Trusted Communications Networks Act ("Secure Networks Act").[3] In these comments, we focus primarily on Section 4(d)(1) of the Secure Networks Act, which requires the Commission to develop a list of suggested replacements or categories of replacements. The list relates to the Commission's recent

[1] CompTIA supports policies that enable the information technology industry to thrive in the global marketplace. We work to promote investment and innovation, market access, robust cybersecurity solutions, commonsense privacy policies, streamlined procurement, and a skilled IT workforce. Visit http://www.comptia.org/advocacy/ to learn more.

[2] Public Notice, *Wireline Competition Bureau Seeks Comment on the Applicability of Section 4 of the Secure and Trusted Communications Networks Act of 2019 to the Commission's Rulemaking on Protecting Against National Security Threats to the Communications Supply Chain*, DA 20-406 (rel. Apr. 13, 2020), 85 Fed. Reg. 26,653 (May 5, 2020) ("Public Notice").

[3] Pub L. No. 116-124 (Mar. 12, 2020).

prohibition on the use of Universal Service Fund support to purchase equipment or services from a company identified as posing a national security risk to communications networks.[4]

DISCUSSION

I. THE COMMISSION SHOULD DEVELOP A LIST OF CATEGORIES OF REPLACEMENTS, NOT A LIST OF REPLACEMENTS.

Section 4(d)(1) of the Secure Networks Act gives the Commission the option to create either a list of suggested "replacements" or a list of "categories of replacements." The Commission should elect to create a list of "categories of replacements" because a list of suggested "replacements" – effectively an approved product list ("APL") – would be counterproductive, contrast with the approach taken by other agencies in addressing suppliers of concern, would impair innovation, and would hurt technology neutrality.

A. Section 4(d)(1) Gives the Commission the Option to Create a List of "Categories of Replacements."

Section 4(d)(1) gives Commission the important option to develop either a list of "replacements" or a list of "categories of replacements." These two options become clear when the text of Section 4(d)(1) is properly parsed as follows:

> The Commission shall develop a list of suggested
> replacements
> of both physical and virtual communications equipment, application and management software, and services
> or
> categories of replacements
> of both physical and virtual communications equipment, application and management software and services.[5]

[4] Report and Order, Further Notice of Proposed Rulemaking, and Order, *Protecting National Security Through FCC Programs*, FCC 19-121 (Nov. 26, 2019) ("Report and Order").

[5] The "categories of replacements" option was added to Section 4(d)(1) just prior to House floor consideration. *Compare* 165 CONG. REC. H10282, 10283 (daily ed. Dec. 16, 2019) (full provision) *with* H.R. REP. NO. 116-352, at 3 (Dec. 16, 2019) (ending after the first "services").

The parsing shown above is correct because the long phrase beginning with "of both physical and virtual …" appears twice, and "[a] standard principle of statutory construction provides that identical words and phrases within the same statute should normally be given the same meaning."[6] Other readings would require breaking apart either the first or second occurrence of the long phrase, in derogation of that "standard principle."[7]

Substantively, the option to develop a list of "categories of replacements" rather than actual "replacements" is very important because a list of "replacements" would represent a form of approved product listing.[8] As the federal government has been taking various steps in recent years to address ICT suppliers of concern, Congress and agencies have generally focused on exclusion and removal processes or "deny lists," while addressing broader supply chain risk management with risk-based approaches that leverage standards, best practices, and functionally-targeted procurement programs.

B. An Approved Product List Would Be Counterproductive and Contrast with the Approach Taken by Other Agencies in Addressing Suppliers of Concern.

As a general matter, APLs are one among many tools that organizations can use to help inform procurement decisions. However, when used in an inappropriate context or not carefully

---

[6] *Powerex Corp. v. Reliant Energy Services*, 551 U.S. 224, 232 (2007); *accord* A. SCALIA & B. GARNER, READING LAW 170-173 (2012) (presumption of consistent usage).

[7] The word "suggested" could potentially be moved down one line to modify only "replacements" rather than also "categories of replacements." However, requiring the Commission to develop a binding list of categories would be a very unexpected result from a provision whose heading begins with the word "suggested." *Cf. Porter v. Nussle*, 534 U.S. 516, 527-28 (2002) (citation omitted) ("[T]he title of a statute and the heading of a section are tools available for the resolution of a doubt about the meaning of a statute"); SCALIA & GARNER, *supra* n. 6, at 221 (title-and-headings canon).

[8] The House committee report's section-by-section analysis states that the Commission is required to "develop a list of suggested replacements" without any reference to "categories of replacements. H.R. REP. NO. 116-352 at 13. However, as noted above, the "categories" option was added after the report was written. *See supra* n. 5.

maintained, APLs can lead to problematic unintended consequences and be detrimental to an organization's overall risk management process. In the Commission's case, building an APL of replacement equipment or services – even a "suggested" one – would require dedication of resources better spent on the actual replacements themselves, would misalign supply chain risk decision-making, would likely lead to over- and under-inclusion of products on the list, and would unnecessarily distort the market.

Resource constraints. An approved product list would require the Commission to conduct a rigorous, resource-intensive process to scrutinize not just the trustworthiness of suppliers – the issue at hand – but also the quality, security, and suitability of the myriad products that make up communications networks. Such an endeavor would go beyond the needs of the Commission and be outside the scope of its expertise.

APL programs are, by nature, time- and resource-intensive endeavors that require careful alignment of criteria with desired outcomes. When making a purchasing decision for communications equipment and services, organizations typically consider a multitude of factors, including but not limited to:

- the quality and cost of a particular product;
- security features and liabilities;
- how a product will integrate within its destined environment; and
- product maintenance and upgrades.

Such product-based factors are supplemented by an evaluation of the supplier itself, which would typically include not just overall trustworthiness (or national security standing) but also at least the following:

- customer service;
- financial stability and corporate governance / leadership; and
- continuity of operations.

Importantly, such evaluations are dynamic over time. For the Commission to maintain an APL, the agency would be required to continually evaluate these factors to keep its list current. However, the Commission does not have and otherwise would normally not *need* to have the same insight into a particular customer's priorities, nor the expertise to fully evaluate products or suppliers.

Vulnerabilities. APLs can create a false sense of high security, *i.e.*, that someone else has weighed all the necessary risks of a purchase. This may prevent the type of true risk-based threat mitigation that every network operator must regularly undertake. An APL creates a one-size-fits all approach for the community of purchasers that rely on it, which can negate the important process of understanding an organization's unique risks. For similar reasons, even ostensibly-appropriate APLs can be easily misapplied, with an APL designed for use in a certain context being used in a way that was not anticipated by its designer. For example, an APL designed for the purpose of replacement of communications equipment from suppliers of concern could easily morph into a list of products deemed to be equally suitable for any network environment, thus creating a security vulnerability.

APLs can also become out-of-date quickly as new models enter the market and old ones become obsolete. Reliance on an outdated list, in addition to creating distortion and other costs in the marketplace, can lead to negative security consequences. Even if updated regularly, recertifying products to achieve inclusion on the APL every time a new model is released would be arduous and expensive for both suppliers and the Commission. Such an approach could create a disincentive for the list to be a full and up-to-date representation of the options available to USF recipients.

Global repercussions. In the current environment, APLs may also carry negative geopolitical implications for the technology industry overall. While the U.S. government's national security prerogative to prevent certain suppliers from integration into domestic communications networks is widely understood, establishing a program for approving communications products writ large would create an unnecessary and harmful barrier to market entry. This would be highly detrimental to U.S. technology companies, especially if replicated abroad. Such a program would unduly limit supply options and could block U.S. suppliers from market entry in other countries. While the federal government may reasonably decide to create APLs to inform its own purchases, it should not do so on behalf of the broader marketplace, even in the context of providing subsidy funds.

Best practices. Ideally, decisions regarding particular suppliers of concern would follow risk-based approaches that might prohibit specific suppliers based on evidence of wrongdoing – a "deny list" rather than an "approve list" – but would still rely on standards, best practices, and other procedures to shape supply chain risk management overall. Other parts of the federal government have recognized this: for example, the Department of Homeland Security ("DHS") has relied heavily on partnership efforts like the ICT Supply Chain Risk Management Task Force and the Sector Coordinating Councils to develop resources to help organizations make better risk decisions themselves. This has happened even as DHS has issued Binding Operational Directives in specific instances to prevent use of equipment or services from certain suppliers that were identified as posing a threat to national security.

Likewise, rather than requiring APLs, Congress has largely focused on identifying and barring specific vendors that pose national security threats from sensitive networks. For example, Section 889 of the FY19 NDAA – which is incorporated by reference into the Secure

Networks Act – and other provisions regarding suppliers of concern have focused on *excluding* certain vendors, rather than specifying which ones should be *included*.[9] In establishing the Federal Acquisition Security Council ("FASC"), the 2018 SECURE Technology Act specifies that the FASC will establish criteria and procedures for *exclusion* and removal of sources or covered articles.[10] Even so, FASC procedures must not conflict with existing standards and guidelines and the FASC must consult with the National Institute of Standards and Technology (NIST) regarding orders that would implement NIST standards and guidelines.[11]

C. An Approved Product List Would Impair Innovation and Hurt Technology Neutrality.

The Commission has long disfavored rules that pick winners and losers among different technologies. Such policies are at the core of the agency's recent spectrum allocation practices and have been present in the Universal Service Fund structure since its inception. Even where the Commission has developed something like an approved list, such as the E-rate Eligible Services List or the process for becoming a Lifeline provider, such programs have aspired toward technology neutrality. This philosophy makes sense, because establishing a base set of rules enables innovation to take place – for example, the plethora of unimagined unlicensed wireless technologies such as Wi-Fi, Bluetooth, Zigbee, NFC, and many more that the Commission's technology-neutral Part 15 rules have permitted to thrive.

---

[9] John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 889, Pub. L. No. 115-232, 132 Stat. 1636, 1917 (2018) ("FY19 NDAA"); Secure Networks Act § 2(c)(3) (relying on FY19 NDAA § 889); *see also* National Defense Authorization Act for Fiscal Year 2018 § 1634, Pub. L. No. 115-91, 131 Stat. 1283, 1740-41 (2017) (excluding Kaspersky Lab).

[10] *See* 41 U.S.C. §§ 1323(c)(1)(A)-(B) (enacted by the SECURE Technology Act § 202, Pub. L. No. 115-390, 132 Stat. 5173, 5181 (Dec. 21, 2018)) ("To reduce supply chain risk," the FASC is empowered to recommend exclusion or removal orders).

[11] *Id.* § 1323(c)(1)(D).

Approving certain companies or products could significantly interfere with this principle. For example, the inclusion of some well-established market participants on an initial APL could discourage smaller vendors or resellers from participating in the program. In some cases, smaller vendors may be more accustomed to working with the small and rural carriers that are the primary focus of the Section 4 program, and in developing and deploying solutions to which larger vendors may be unaccustomed. Furthermore, network function virtualization ("NFV") has the potential to provide an immense number of new entrants to the communications marketplace. Even a "suggested" list from the Commission – one which would likely heavily influence USF recipients' purchases – would at best limit small and medium-sized communications providers' access to those new technologies and products, or at worst could foreclose the entry of those new suppliers and technologies altogether. *See also* section II-A below.

Ultimately, Section 4(d)(1) directs the Commission to build a list as a resource for USF recipients faced with rip-and-replace obligations and to provide clarity to the marketplace regarding what kinds of purchases will be supported by the USF program going forward. With that in mind, the Commission should focus its efforts not on a resource-intensive evaluation of every potential product and service that makes up a communications network – which would likely lead to over- and under-inclusion – but rather on the types of products that the Commission is most concerned with USF recipients transitioning as part of the rip-and-replace process. For these reasons, the Commission should not build a list of specific replacements, but should instead identify categories of equipment and services that USF recipients should be focused on replacing under the Secure Networks Act.

II. THE LIST OF CATEGORIES SHOULD BE BROAD AND TECHNOLOGY-NEUTRAL.

In assembling the list of categories of replacements, the Commission should be inclusive and permit both hardware and software solutions, both for statutory reasons and because of emerging technology trends. However, the Commission should not impose any limits based on security or architectural frameworks, nor should it prevent up-to-date equipment from being included on the list.

A. The Categories Should Be Inclusive and Permit Both Hardware and Software Solutions.

In order to promote competition, innovation, and technology neutrality (*see* section I-C above), the list of categories of replacements should be as broad as possible. It should be expansive and high-level enough to incorporate most if not all relevant elements of a network. This would include, for example:

- Elements used in any segment of a provider's network, including access networks, transport, edge, core, ISP DMZ LANs, etc.;[12]
- Traditional network infrastructure hardware appliances such as routers, switches, base stations, baseband units, DSLAMs, etc.;
- Software or service-based replacements for any of these functions, in keeping with Section 4(d)(1)(B)'s clear mandate of technology neutrality along with current trends toward network function virtualization (NFV);[13]

[12] Newer technologies may contribute to different network topologies than older ones, and the Commission should be accommodative of different approaches. For example, 5G networks may require more infrastructure closer to the edge of networks rather than in the core.

[13] Examples of 4G virtualized network functions include: Radio Network Controllers – XnodeB; Gateways; Content Delivery Networks; MME – Mobility Management Entity; HSS – Home Subscriber Server; PCRF – Policy and Charging Rules Function; SMSC – Short Message Service Center; OCS – Online Charging System; ePDG – enhanced Packet Data Gateway; SGW – Serving Gateway; PGW – Packet Gateway; PCEF – Policy Control Enforcement Function; ANDSF – Access Network Discovery and Selection Function; MRF – Media Resource Function; MGCF – Media Gateway Controller Function; AAA – Authentication, Authorization,

- Commodity off-the-shelf (COTS) hardware being used to replace dedicated network hardware appliances if such COTS hardware is accompanied by NFV software, such as an x86-based server paired with appropriate software.[14]

Even a broad, high-level list of categories would provide helpful guidance to the marketplace regarding implementation. It would give carriers and suppliers a sense of the types of equipment and services for which the Commission intends to provide replacement funding, and which types would not be eligible. The Commission should categorically exclude, for example, any equipment from a covered company that has been designated pursuant to the Secure Networks Act and in this proceeding.

B. Limits Based Upon Specific Security or Architectural Standards or Frameworks Should Not be Imposed.

To date, the Commission has largely and appropriately refrained from mandating particular cybersecurity or other security standards for particular telecommunications equipment. This is entirely appropriate, because national security, supply chain security, and cybersecurity threats are all best handled through risk-based frameworks. *See* section I-B above. For example,

---

Accounting; CSCF – Call Session Control Function; OSS – Operation Support Systems; BSS – Business Support Systems; TAS – Telco Applications Server.

Examples of 5G network function elements include: AUSF – Authentication Server Function; AMF – Access and Mobility Management Function; NEF – Network Exposure Function; NRF - Network Repository Function; NSSF – Network Slice Selection Function; N3IWF – Non 3GPP Interworking Function; PCF – Policy Control Function; SMF – Session Management Function; UDM – Unified Data Management; UPF – User Plane Function; UDR – User Data Repository; UDSF – Unstructured Data Storage Function; NWDA – Network Data Analytics Function; EIR – Equipment Identity Register; SMSF – Short Message Service Function; BSF – Billing Support Function; SEPP – Security Edge Protection Proxy; AF – Application Function; CHF – Charging Function; NSMF – Network Slicing Management Function. *See* 3GPP, *System architecture for the 5G System*, 3GPP TS 23.501 v.16.4.0 (Mar. 2020), https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/23501-g40.zip.

[14] Failure to include COTS hardware in the program could potentially give a significant financial advantage to traditional network infrastructure hardware appliances. This would violate section 4(d)(2)(B), which requires that the list be "technology neutral."

the NIST Cybersecurity Framework, the DHS ICT Supply Chain Task Force, and the Commission's own Communications Security, Reliability, and Interoperability Council ("CSRIC"), have all promoted risk-based approaches to security.

Risk-based frameworks facilitate shared responsibility for security across the ICT ecosystem, pushing the ***users*** of telecommunications equipment and services to consider not just which products and services they buy, but how they are integrated into a particular environment and actually used. The Secure Networks Act is explicitly consistent with this principle, as it requires the recipients of grant funding – the users – to "*consult and consider* the standards, guidelines, and best practices set forth in the cybersecurity framework developed by the National Institute of Standards and Technology."[15] With this important principle established by Congress, it should suffice here for the Commission to say that products from covered companies will be categorically excluded from the Section 4(d)(1) list, and the Commission need not and should not go further.

In a similar vein, the Commission should not limit its list to technologies based on virtualized radio access networks, including O-RAN or any similar architecture. To be sure, these architectures offer great promise and many CompTIA members are actively engaged in their development. However, the statutory requirement of technology neutrality in section 4(d)(1)(B) – which sensibly codifies the Commission's longstanding practice and allows NFV-based and O-RAN-based solutions to compete for grant dollars – also prohibits the agency from leveraging funding in *favor* of particular technologies or architectures. Attempts to do so through the rulemaking process could introduce unforeseen practical or legal complications into a grant program that Congress intended the Commission to implement rapidly.

[15] Secure Networks Act § 4(d)(4)(B)(ii) (emphasis added).

C. Products and Services Using Up-to-Date Technologies Should Not Be Categorically Excluded.

The Commission should not limit the categories of replacements to equipment or services that would be an exact or "like-kind" replacement for what is being removed. As the agency knows, some of the affected carriers are likely using 3G or even 2G equipment. It would be a highly imprudent use of limited federal resources to require that such carriers replace their gear with equipment that is obsolete. Moreover, while modern gear may be backward-compatible with 3G devices, it may no longer be realistically possible to purchase a new base station that does not also include more modern protocols. Indeed, it may be difficult to even obtain such gear on the used market. In extreme cases, vendors may also have stopped supporting such older gear, which could result in security vulnerabilities if a legacy product were suddenly incorporated into a network today.

Importantly, the Commission is not under any legal obligation to prevent replacement of covered equipment with updated technology. The Secure Networks Act contains no such provision; in fact, Congress considered but eventually declined to include such a requirement.[16] While the House committee report urged the Commission to "preclude network upgrades" that go beyond the replacement of covered services, it also included a major caveat that better anticipates the market reality: "the Committee expects there to be a transition from 3G to 4G or even 5G-ready equipment in instances where equipment being replaced was initially deployed several years ago."[17] In any event, such "committee report language unconnected to the text of

[16] The first version of the bill introduced in September 2019 included the following in section 4(c)(2): "A recipient of a reimbursement under the Program may not use reimbursement funds to … (C) make network upgrades that go beyond the replacement of covered communications or services, as determined by the Commission." H.R. 4459 (116th Cong.) When the bill was re-introduced in November 2019, the provision was dropped. *See* H.R. 4998 (116th Cong.)

[17] H.R. REP. 116-352 at 13.

an enacted statute has no binding legal import," and it would be "contrary to law" for the Commission to act based on a belief that it did.[18] This is especially true where, as here, the legislative history also shows that Congress declined a proposal to include a similar provision in the statutory text.

To be sure, the statute includes explicit measures to reduce waste, fraud, and abuse.[19] However, forcing carriers to replace networks with legacy components would be wasteful in the long term and would countermand universal service goals. The Commission has experience addressing "gold-plating" concerns in other contexts, such as the digital television transition and the implementation of ATSC 3.0. CompTIA is confident that similar principles can be applied here as the agency reviews grant applications, rather than imposing any artificial ex ante restrictions.

III. CONGRESS MUST APPROPRIATE FUNDING FOR THE PROGRAM.

In the Public Notice, the Commission seeks comment on its reading that the Secure Networks Act "appears to require an express appropriation from Congress" while noting that the program "must be separate from any Federal universal service program …."[20] This reading is undoubtedly correct. The Commission cannot divert USF funding for this program, and it must seek an appropriation from Congress.

---

[18] *Northwest Environmental Defense Center v. Bonneville Power Administration*, 477 F.3d 668, 682 (9th Cir. 2007).

[19] Secure Networks Act § 4(e).

[20] Public Notice ¶ 9.

CONCLUSION

The Commission should use the flexibility afforded by Section 4(d)(1) of the Secure Networks Act to create a list of "categories of replacements" rather than a list of "replacements." Moreover, that list of categories should be broad and technology-neutral, and should avoid unnecessary limits. CompTIA greatly appreciates the Commission's work in this proceeding, and we look forward to continued engagement on these issues.

Sincerely,

/s/ Dileep Srihari

Dileep Srihari
Vice President and Senior Policy Counsel

Savannah Schaefer
Senior Director, Public Advocacy

COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION (CompTIA)
322 4th Street NE
Washington, DC 20002

May 20, 2020