Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

COMMENTS OF
THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Cinnamon Rogers
Senior Vice President, Government Affairs

Dileep Srihari
Senior Policy Counsel and Director, Government Affairs

K.C. Swanson
Director, Global Policy

Savannah Schaefer
Policy Counsel, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Road
Suite 200
Arlington, VA 22201
(703) 907-7700

June 1, 2018

EXECUTIVE SUMMARY

The Federal Communications Commission faces an extraordinary situation. Growing national security concerns about certain suppliers of communications products, long discussed among the national security community, have now exploded into public view. Actions regarding those suppliers are being considered – or have already been taken – by Congress and by officials at the highest levels of the federal government, including the President. And in the brief period since the Commission adopted the Notice of Proposed Rulemaking, it has become clear that this proceeding is now being carefully watched both at home and abroad. Therefore, as detailed in these comments, the Telecommunications Industry Association ("TIA") supports the Commission's proposal to prevent the use of federal Universal Service Fund dollars to procure or obtain equipment or services produced or provided by any company posing a national security threat.

The Commission faces a significant challenge, but also has a unique opportunity. Although the Notice is narrowly focused on the disbursement of universal service support, any steps the Commission takes here will have ramifications beyond that context. Its actions will set an example for other federal agencies, advance the discussion among policymakers in Congress and the executive branch, and guide the actions of other regulators around the world. In this rapidly-evolving environment, the Commission is right to recognize that it has an important but targeted and specific role to play, and that its actions must further the ongoing national and international conversation about how best to address these issues.

This proceeding is the first on-the-record opportunity for all stakeholders, including the information and communications technology ("ICT") industry, to share their views on how to balance (1) the need for government action to mitigate the risk of state-sponsored cyberespionage or malicious disruption with (2) the impact such action will have on trusted suppliers and an extremely complex global supply chain. In these comments, TIA, on behalf of its membership comprising hundreds of global manufacturers and vendors of ICT equipment and services, describes the immediate challenge facing the Commission and makes recommendations to guide the Commission, as well as Congress and the executive branch, toward long-term, durable solutions. The Commission's actions now should be taken with long-term considerations in mind and with awareness of the broader processes underway in industry and government on these issues.

The Case for Action

Government intervention in the marketplace to mandate, favor, disfavor, or prohibit the use of products from a particular supplier is an extraordinary action, particularly for an agency whose mission is to promote competition. If not done carefully, under well-defined conditions, and for clear, articulable reasons, such action could stifle innovation, discourage competition, and lead to significant legal challenges. And when foreign suppliers are involved – as is the case here – any steps to intervene could also have significant, negative, and long-term repercussions for U.S. companies trying to compete in the global ICT marketplace.

Nevertheless, the high threshold for taking targeted action has been satisfied for the companies specifically named in the Notice. There is substantial evidence that state actors,

notably China and Russia, have supported extensive and damaging cyberespionage efforts in the United States. The federal government has increasingly focused on the potential risks associated with products from specific suppliers in those countries that are believed to have ties with those governments. Actions have been taken, beginning with quiet phone calls to major U.S. service providers at least as far back as 2010 and gradually expanding to the specific by-name statutory prohibitions on procurement by certain federal agencies that were enacted last year. Legislation now moving through Congress would prohibit all federal procurement from specific suppliers of concern.

Against that backdrop, it is appropriate to take targeted action to prevent the use of federal USF dollars to procure or obtain products from those suppliers. Cybersecurity is a shared responsibility across the ecosystem, and given the pervasiveness and importance of USF-funded networks, the Commission has an important responsibility to safeguard a program it directly oversees. Meanwhile, any actions beyond the USF context raise more complex questions, and should be deferred to a Further Notice of Proposed Rulemaking.

Specific Suppliers vs. General Supply Chain Management

This proceeding should focus on *specific suppliers of concern*, rather than attempting to address supply chain risk management more broadly. Supply chain risk management is extraordinarily complex and works best through consensus-based, industry-led processes. Industry-driven standard-setting efforts such as the Factor Analysis of Information Risk (FAIR) Methodology, Common Criteria for Information Technology Security Evaluation, and Open Group Trusted Technology Forum are just some examples of efforts designed to promote supply chain security. Public-private partnerships coordinated by the Department of Homeland Security, including the Government and Sector Coordinating Councils and the Information Sharing Analysis Centers and Organizations, also play important roles. Additionally, the National Institute of Standards and Technology ("NIST") recently updated the highly-acclaimed NIST Cybersecurity Framework to address supply chain security risk management. The recommendations of the Commission's own Communications Security, Reliability, and Interoperability Council ("CSRIC") on supply chain security are another important resource developed through industry leadership.

However, on the whole, these tools do not address, nor were they intended to address, defending against state actors' strategic exploitation of specific suppliers that are potentially beholden to them. Likewise, product testing is not effective in this context. Of course, testing can be a very useful means of detecting inadvertent security vulnerabilities, either in a single product or in an enterprise network. Indeed, the ICT industry engages in vigorous efforts to test and verify products, while network penetration testing has become a well-established practice. However, it remains very challenging to detect whether a particular communications technology product has been deliberately and covertly compromised, especially by a state-sponsored actor.

Focusing on specific suppliers that raise national security concerns, rather than supply chain management generally, is the most immediate and surgical approach to protect our nation's infrastructure and also acknowledges that ICT supply chains are truly global. Given this reality, blanket country-of-origin prohibitions would significantly disrupt longstanding and vital supply

chains for trusted suppliers and therefore should be scrupulously avoided. Such broad prohibitions would also harm global trade without yielding appreciable security benefits.

In addition, focusing on certain types of *components* from those suppliers of concern would be the most precise approach to materially advance national security goals. To that end, the following guiding principles are important: (i) *differentiation* to recognize the variance in threats posed by different components (*e.g.*, a cable or plastic housing versus a central processing unit); (ii) *clear application* so that any component-focused restriction is easy to understand and apply; (iii) *consistency* across the government to avoid compliance challenges; and (iv) *administrative flexibility in implementation* for manufacturers who take different approaches to their supply chains. These comments outline a definition for "logic-enabled" components with the goal of furthering the national discussion on this issue. Finally, any restrictions on services should be narrowly tailored to avoid inadvertent problems such as interfering with the equipment decommissioning process.

Defining and Limiting the Commission's Role

Sections 201(b) and 254 of the Communications Act provide the Commission well-settled discretion over the universal service program, and promoting national security is indisputably an important element of providing high-quality services to all Americans. *However*, as the Commission cautiously opens the door to a new form of national security-based regulation, it is vitally important to articulate limiting principles at the outset. Such limiting principles can be discerned from national security-related provisions of the Communications Act and from the agency's own precedents, all of which defer specific national security determinations to the President or to executive branch agencies with appropriate expertise.

In practice, this means the Commission should not independently determine which specific suppliers should be subject to any prohibition adopted here. Such determinations rely on assessments of a particular foreign government's laws and a specific company's governance structure, often based on classified intelligence information. The Commission lacks relevant expertise on these matters. Furthermore, independent determinations made by each agency would lead to an inconsistent patchwork of restrictions across the government and potential legal challenges. Specific action by the President or by agencies with appropriate national security expertise, as well as statutory language from Congress, should govern such determinations.

Implementation Issues

For practical reasons, the Commission should create and publish a list of prohibited suppliers for use by USF recipients and by industry. The list should include specific companies prohibited by name by the President, by executive agencies, or by statute from selling to any civilian federal agency due to national security reasons, including subsidiaries and affiliates of those companies. USF recipients should be required to provide an attestation that they have not spent any funds on covered products or services from a prohibited company. Importantly, if the Commission imposes any restriction based on components, then manufacturers will also need to provide such attestations. The procedures should provide flexibility for manufacturers of varying sizes with different approaches to supply chain management, for example, by including

the option to remove *all* components from a prohibited supplier, rather than just logic-enabled components.

Specificity and clarity will be of utmost importance, both to provide certainty to the marketplace and to signal to the international community that the Commission is acting in a principled manner. The Commission's list of prohibited suppliers, and any definitions it establishes regarding restricted components and services, must be capable of being applied by USF recipients, by non-lawyers working across the ICT manufacturing industry, and by the agency itself. To that end, *draft text of a rule applying the principles described above is provided in an Appendix to these comments* for the Commission's consideration. TIA welcomes feedback from other stakeholders on this proposed text.

Weighing the Costs and Benefits

If action is narrowly tailored as described in these comments, the benefits will outweigh the costs. The Commission is well-acquainted with the need to weigh costs and benefits in the universal service context. There are clear benefits to action here, including greater confidence in the global ICT marketplace, higher quality and greater equality of service for USF recipients, potential reduction of costs from security breaches, and increased consumer confidence that sensitive personal information will not be compromised by a foreign state actor.

While removing a supplier from the market is never optimal, when it comes to national security, there is less room for tradeoffs. Fortunately, there is a *robust and competitive marketplace for equipment* that includes a number of trusted suppliers. As described in these comments, the specific suppliers named in the Notice appear to have a very small share of the U.S. market. Numerous TIA member companies sell the various types of equipment upon which USF-funded service providers rely. In fact, in all four USF programs, available suppliers include large, sophisticated equipment manufacturers that presently compete for market share, as well as enterprising start-ups that are developing new products and services to compete with these established suppliers.

Towards A Long-Term Approach

The Commission has recognized that it cannot and should not address this problem alone. With Congress and the executive branch actively engaged in this area, the agency must remain cognizant of ongoing work elsewhere to address these issues. A holistic approach is consistent with established guidelines for the protection of critical infrastructure. Specific actions by other agencies – such as the Department of Commerce's denial order to one Chinese supplier resulting from export control violations – may have direct and immediate impacts on the Commission's own goals.

Ultimately, a long-term and durable approach is needed to address these challenges beyond the Commission's reach. To facilitate this, an interagency process should be established that would be more flexible and effective than naming individual companies in legislation. The interagency process should include the Department of Homeland Security as the Sector Specific

Agency for the IT and communications sectors, with input from the Intelligence Community, the Commerce and Defense Departments, and other agencies with relevant expertise.

Determinations regarding particular suppliers should be made only after careful investigation of all available evidence, and due process should be provided to ensure that trusted suppliers are not inadvertently snared in the net. These comments include factors for decision-makers to use, including *nation-specific criteria* such as a country's history of state-backed cyberespionage or its legal environment, *company-specific criteria* such as evidence of illegal activity or corporate governance structure, and potentially *product-specific criteria* based on the relevance of particular products to security within a network.

Global Cooperation

No single country can address the threats from potentially malicious actors or high-risk suppliers by itself. Fortunately, the United States has engaged in cybersecurity-related dialogues with the European Union, Japan, Australia, India, as well as China, among others. Several countries are now closely following developments in the United States regarding the companies named in the Notice, and some have already taken action or issued advisories. The national conversation on these issues will quickly have international ramifications, and everything the United States does must be considered with that reality in mind.

TIA will continue to actively participate in that conversation at home and abroad, including discussions with and among our member companies who are the manufacturers and suppliers of the world's ICT products. Our member companies are on the front lines of the global challenge to ensure that ICT products are both secure and reliable, and we therefore have a vital stake in the outcome of this proceeding. We look forward to working with the Commission and with the rest of the government to continue advancing the discourse about these very important issues.

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

COMMENTS OF
THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association ("TIA")[1] respectfully submits these comments in the above-captioned proceeding.[2] As both an advocacy organization and a standards-setting body, TIA represents hundreds of global manufacturers and vendors of information and communications technology ("ICT") equipment and services that are supplied to the owners and operators of communications networks, enabling operations across all segments of the economy.[3] Our member companies design, produce, and sell equipment and services in countries around the world that leverage modern global supply chains, and each company has a vital stake in the outcome of the Commission's work in this proceeding.

[1] TIA is the leading trade association for the information and communications technology ("ICT") industry, representing companies that manufacture or supply the products and services used in global communications across all technology platforms. TIA represents its members on the full range of policy issues affecting the ICT industry and forges consensus on voluntary, industry-based standards.

[2] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC 18-42 (rel. Apr. 18, 2018), 83 Fed. Reg. 19,196 (May 2, 2018) ("Notice").

[3] These comments represent the views of the TIA Public Policy Committee. While some companies mentioned in the Notice are members of TIA, specifically Huawei Technologies Company ("Huawei") and ZTE Corporation ("ZTE"), these companies do not have access to the Public Policy Committee or to any of its internal communications or deliberations, and so did not influence these comments.

INTRODUCTION

TIA supports the Commission's efforts to promote the security of the nation's communications networks. As the Commission notes, threats posed by certain communications equipment providers have long been a matter of concern to the executive branch and to Congress.[4] The Commission has a targeted and important role to address those concerns and has appropriately focused its initial efforts in this proceeding on federal funds distributed through the Universal Service Fund ("USF").

Government intervention in the marketplace to mandate, favor, disfavor, or prohibit the use of products from a particular ICT vendor is an extraordinary action. It is not one that TIA takes lightly, nor should the Commission. If not done carefully, under well-defined conditions, and for very clear, articulable reasons, such an action could stifle innovation, discourage competition, and give rise to significant legal challenges. Moreover, when foreign vendors are involved – as is the case here – it could also result in significant, negative, and long-term repercussions for U.S. companies and the global ICT marketplace.

Nevertheless, in these specific circumstances, the threshold for action has been satisfied. The Commission is seeking here to address a unique situation in which certain ICT vendors have already been identified as posing security threats by Congress or executive branch agencies possessing appropriate expertise and access to intelligence information. Even so, while the Commission may act expeditiously to address the issue at hand – and all of the legal analysis and proposals in these comments would facilitate that outcome – the agency should still proceed with an eye to the long-term future as well.

[4] Notice ¶ 1.

As the Commission also recognizes, these are complex issues that span across not only the federal government but also throughout the global ICT marketplace. However, this is the first on-the-record proceeding at *any* federal agency to address these issues. Therefore, these comments are intended to inform not just the Commission's work in this proceeding, but the work of Congress and other executive branch agencies as well. Although the proposals here can be implemented by the Commission immediately on its own, the agency's actions should take place within a broader set of processes and actions coordinated across the federal government. We make proposals below for how those processes and actions could be structured.

Section I of these comments supports the Commission's conclusion that USF funding should not support communications technology suppliers deemed to pose a threat to national security. Promoting the security of USF-funded networks is critical for national security. We describe the concerns raised, and actions taken, by Congress and other agencies across the U.S. government, and by foreign governments, regarding the specific companies named in the Notice. However, any actions beyond USF restrictions should be considered in a Further Notice of Proposed Rulemaking.

Section II explains that while the Commission has the legal authority to adopt its proposed rule, that authority should be subject to limiting principles and predicated on national security determinations made outside the Commission. However, once such determinations have been made regarding a particular supplier – as has happened here – a restriction on USF funds becomes a permissible and appropriate means for implementation.

Section III explains why the Commission's actions should be focused on specific suppliers of concern rather than cybersecurity supply chain risk management in general. For example, product testing is not an appropriate mechanism to address the concerns raised here,

despite some suggestions to the contrary. The Commission should also avoid overbroad supply chain restrictions based on country-of-origin, and should narrowly tailor its actions due to the potential global repercussions. Such tailoring may include prohibitions on certain types of components from specific suppliers of concern, while also more clearly targeting certain types of communications products versus the blanket prohibition tentatively proposed in the Notice.

Section IV addresses implementation details, beginning with the Commission publishing a list of prohibited suppliers. The list should derive from determinations made by Congress or appropriate processes that include federal security agencies, and should operate in a clear fashion based on easy-to-implement criteria. However, the Commission should not make its own national security determinations regarding any particular supplier, as it lacks the expertise to do so and would set a bad precedent for other regulatory agencies across the government. Nor should the Commission codify the names of particular companies into the Code of Federal Regulations. But the Commission should establish an attestation procedure applicable to USF recipients that will in turn apply to their upstream suppliers.

Section V addresses the costs and benefits of the Commission's proposed rule. If narrowly tailored, a rule addressing security concerns would improve customer confidence in the global ICT marketplace and provide significant public interest benefits to users of USF-supported networks and services. Importantly, a narrowly-tailored rule should not impact the competitive marketplace for equipment available to USF recipients.

Section VI explains that although the proposals here can be implemented by the Commission immediately on its own, the agency's actions should be informed by a long-term view that would ultimately require actions across the federal government. We encourage the Commission to coordinate with other government actors, and we outline a future interagency

process by which it could do so, including listing a set of criteria for possible use by national security decisionmakers when evaluating particular suppliers of concern. We also address the need for global approaches to deal with these issues over the long term.

Finally, the complexity and importance of these issues gives rise to a significant need for specificity and clarity. For that reason, we provide the text of a proposed rule in an Appendix for the Commission's consideration that embodies the principles and recommendations set forth in these comments.

DISCUSSION

I. UNIVERSAL SERVICE FUNDS SHOULD NOT SUPPORT PURCHASES OF PRODUCTS FROM SUPPLIERS DEEMED TO POSE A THREAT TO NATIONAL SECURITY.

The Commission has a unique responsibility and ability to ensure that the billions of dollars it makes available to schools, libraries, rural healthcare providers, and broadband providers that serve millions of Americans are not used in a way that would undermine national security. As described below, there are widely acknowledged threats to networks from specific suppliers identified as posing those types of risks. As a steward of funds collected from American ratepayers intended to support American consumers and critical institutions in communities across the country, the Commission has an obligation to ensure that USF funds are not available to purchase products or services from those suppliers. To do otherwise would be inconsistent with the Commission's statutory obligation to ensure that USF support is distributed in a manner consistent with the public interest.[5]

While government intervention in the marketplace must be carefully calibrated to ensure consistency with the agency's expertise and statutory authority, once the Commission is

[5] 47 U.S.C. § 254(c)(1)(D).

presented with clear evidence of a national security risk, it is on solid ground to adopt a targeted policy of funding restrictions to address those risks. (*See* Section II below.) As described below, there is now substantial evidence that state actors, notably China and Russia, have supported cyber espionage in the United States. As a result, Congress and the executive branch have increasingly raised and pursued concerns related to specific suppliers based in those countries, including by taking informal actions, initiating formal proceedings, and even adopting targeted statutory language. However, any actions the Commission might consider taking beyond the USF context should be deferred to a Further Notice of Proposed Rulemaking where they can be considered in greater depth.

A. Promoting the Security of USF-Funded Communications Networks is Critical for National Security.

Every year, consumers in the United States pay billions of dollars into universal service programs, to support the goal of ensuring that all Americans have access to essential communications services. In 2017 alone, the Universal Service Administrative Corporation ("USAC") distributed nearly $9 billion in USF support.[6] During the past six years, since the Commission began to focus its universal service programs on broadband, over $50 billion has been spent to connect Americans to modern communications infrastructure.

Today, universal service programs subsidize networks and services in every state, territory, and tribal region in the United States, providing access to many of the nation's most vulnerable consumers. Through the E-rate program, billions of dollars have supported high-speed connectivity to, and within, thousands of schools and libraries to support digital learning in

[6] *See* Universal Service Administrative Company, 2017 Annual Report, https://www.usac.org/_res/documents/about/pdf/annual-reports/usac-annual-report-2017.pdf ("USAC 2017 Annual Report").

every corner of the country. Hundreds of millions of Rural Healthcare Program dollars have been invested in networks relied on by rural healthcare providers offering essential medical and telemedicine services for rural communities. Billions more have been invested in fixed and mobile broadband networks in the most remote and hard to reach communities in America, places that would not have connectivity but for support from the Commission's Connect America Fund ("CAF"). Finally, countless Americans are able to connect with friends and family and to seek emergency assistance from the Commission's Lifeline program serving low-income consumers. Through at least one of these four programs, virtually every community in America benefits from connectivity provided by USF dollars. Meanwhile, USF-funded networks are interconnected with the rest of the vast communications infrastructure that allow Americans to connect with anyone, anywhere, at any time.

Given the pervasiveness and importance of USF-funded networks, the Commission has a critical responsibility to take steps to protect them from national security threats posed by certain suppliers. Students and teachers using E-rate funded services have a right to expect that their networks are secure. Healthcare providers – who are experiencing a rapid increase in cybersecurity attacks at levels far greater than other industries[7] – should not be exposed to even more threats simply because they rely on USF-subsidized broadband connections. According to

[7] *See* Ladi Adefala, *Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries*, CSO, Mar. 6, 2018, https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html; *see also* Heather Landi, *Report: Ransomware Attacks Against Healthcare Orgs Increased 89 Percent in 2017*, HEALTHCARE INFORMATICS INSTITUTE, Jan. 8, 2018, https://www.healthcare-informatics.com/news-item/cybersecurity/report-ransomware-attacks-against-healthcare-orgs-increased-89-percent-2017 (citing a report finding that the number of reported major IT/hacking events attributed to ransomware by health care institutions increased by 89 percent from 2016 to 2017).

one study, healthcare is the industry most frequently targeted by cybersecurity attacks, with 164 threats detected per 1,000 host devices; education is a close second with 145 detections per 1,000 host devices.[8] And rural businesses and homes that rely on USF support for their broadband connectivity should not be subject to higher risk of cyber intrusions because of policies that permit service providers to use equipment that puts their customers at risk. Even in those cases where consumers have limited options for broadband connectivity – made possible by USF support – those service providers nonetheless have multiple options available to them to deploy such networks without relying on technology from bad actors. (*See* Section V.C below.)

Cybersecurity is a shared responsibility across the ecosystem – including efforts by the ICT industry (*see* Section III.A below) – and USF-supported networks indiscriminately interconnect with global commercial networks. While the Chairman is right to acknowledge that the Commission "doesn't have the authority or capacity to solve this problem alone,"[9] in unanimously adopting the Notice, the Commission recognized the critical need for the agency to do its part. In shepherding the universal service programs, which directly or indirectly impact nearly every person in the United States, the Commission has a duty to ensure to the best of its ability that funds are being spent responsibly in the public interest, and that networks and services paid for by the American public are procured with security in mind.

[8] *See* Jeff Goldman, *Healthcare Industry Suffers the Most Cyber Attacks*, eSECURITY PLANET, June 9, 2017, https://www.esecurityplanet.com/network-security/healthcare-industry-hit-most-frequently-by-cyber-attacks.html.

[9] Notice, Statement of Chairman Ajit Pai.

B. Government Intervention in the Marketplace is an Extraordinary Action that Requires a Thoughtful Approach, But the Threshold for Action Regarding the Specific Suppliers Identified in the Notice Has Been Satisfied.

The Commission's actions in this proceeding are likely to set a global precedent that, if not implemented carefully by the Commission and by foreign regulators, could potentially raise the cost of doing business for U.S. communications technology vendors both at home and abroad. Removing any competitor from the marketplace is therefore a major step, not least because the Commission's usual task is to *promote* competition in the telecommunications industry.[10] It is a step that could result in specific retaliation by certain foreign governments against U.S. companies. Thus, any regulatory intervention in the marketplace should not be taken lightly, and must be tailored for a specific purpose and to address a specific harm.

To that end, the government has widely acknowledged threats posed by certain state-backed and state-controlled suppliers. As the Chairman noted, "U.S. government officials have expressed concern about the national security threats posed by certain foreign communications equipment providers in the communications supply chain" for many years now.[11] Specifically, as the FBI Director discussed in his testimony to the Senate Select Committee on Intelligence earlier this year, the U.S. government is becoming increasingly aware of "the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks," including "the capacity to

[10] As the Senate Commerce Committee explained in the report accompanying its version of the Telecommunications Act of 1996: "Reducing regulation of the telecommunications industry will spur the development of new technologies and increase investment in these industries, which will create jobs and greater choices for consumers. The United States telecommunications industry is competitive worldwide. By reducing regulation and barriers to competition, the bill will help ensure the future growth of these industries domestically and internationally." S. Rep. 104-23, at 9-10 (1995).

[11] Notice, Statement of Chairman Ajit Pai.

maliciously modify or steal information" and "conduct undetected espionage."[12] According to the Director of the National Security Agency, "this is a challenge that … is only going to increase, not lessen, over time for us."[13]

As described below, for more than a decade, national security experts and policymakers across the federal government have flagged concerns regarding specific threats posed by the suppliers identified in the Notice. Based on this intelligence, Congress and executive agencies with security expertise have started taking overt action to address those concerns. For its part, the Commission has recently been urged by members of Congress to address the threats posed by these suppliers.[14]

1. The United States and Allied Governments Have Identified Security Concerns Regarding Those Suppliers.

There is now substantial public evidence that state actors, notably China and Russia, have supported extensive and damaging cyberespionage efforts in the United States. For example, in 2013 the cybersecurity firm Mandiant released a report detailing extensive Chinese commercial

[12] Hearing before the Senate Select Committee on Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community*, 115th Cong. (Feb. 13, 2018) ("Senate Intel Feb. 13 Hearing") (statement of Christopher Wray, Director, FBI), https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-hearing-1, at 02:06:50 – 02:08:00.

[13] *Id.* (statement of Admiral Michael Rogers, Director, NSA), https://www.intelligence.senate.gov/hearings/openhearing-worldwide-threats-hearing-1, at 02:08:06 – 02:08:13.

[14] Letter from 18 U.S. Senators to Ajit Pai, Chairman, FCC (Dec. 20, 2017), https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0323/DOC-349859A2.pdf (expressing concern over reports of use of Huawei equipment by a major U.S. service provider, noting that "[Pai] and other commissioners would benefit from Intelligence Community briefings on the threat Huawei and other Chinese technologies pose").

cyber theft by actors associated with the People's Liberation Army.[15] More recently, in March 2018, the Office of the U.S. Trade Representative ("USTR") said that "evidence indicates that China continues its policy and practice, spanning more than a decade, of conducting and supporting cyber-enabled theft and intrusions into the commercial networks of U.S. companies."[16] On April 16, the Department of Homeland Security, the FBI, and the government of the United Kingdom issued a joint technical alert that highlighted recent Russian state-sponsored cyber-hacking of U.S. network devices.[17]

The U.S. government has therefore increasingly focused on the potential risks associated with ICT products from specific technology vendors based in those countries. Notably, U.S. concerns have focused on certain ICT companies from China and Russia that are believed to have ties with governments known to have supported malicious cyber activity. As a result, there is now a heightened awareness of the potential risk posed by these firms.

Specifically, various government entities have raised concerns regarding Huawei and ZTE's ability to (1) access information transmitted across U.S. networks or (2) influence the operation of U.S. networks, concerns that are heightened by the opaque structures of these companies and the nature of potential ties between those companies and the Chinese government. In 2012, the House Intelligence Committee noted that "to the extent these

---

[15] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, at 3-4 (2013), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[16] Office of the U.S. Trade Representative, *Findings of the Investigation into China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*, at 171 (Mar. 22, 2018), https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF ("USTR China Findings").

[17] U.S. Computer Emergency Readiness Team, *Alert (TA18-106A), Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices*, Apr. 16, 2018, https://www.us-cert.gov/ncas/alerts/TA18-106A ("US-CERT April 2018 Alert").

companies are influenced by the state, or provide Chinese intelligence services access to telecommunications networks, the opportunity exists for further economic and foreign espionage by a foreign nation-state already known to be a major perpetrator of cyber espionage."[18] According to the same report, "it appears that under Chinese law, ZTE and Huawei would be obligated to cooperate with any request by the Chinese government to use their systems or access them for malicious purposes under the guise of state security."[19] More recently, a leaked National Security Council presentation noted that the FBI continues to "update its compendium of activities and risks associated with Huawei and ZTE."[20]

Similar concerns have been expressed about Kaspersky Lab. The Department of Homeland Security stated that it was "concerned about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks."[21] The agency explained that "[t]he risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to

---

[18] House Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, at iv (2012), https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf

[19] *Id.* at 3. The Committee went so far as to state that "[c]ompanies around the United States have experienced odd or alerting incidents using Huawei or ZTE equipment," while alluding to classified information that provided significantly more cause for concern. *Id.* at 10.

[20] Unknown National Security Council author, *Secure 5G: The Eisenhower National Highway System for the Information Age*, leaked Jan. 28, 2018, https://www.axios.com/trump-team-debates-nationalizing-5g-network-f1e92a49-60f2-4e3e-acd4-f3eb03d910ff.html.

[21] Press Release, Department of Homeland Security, *DHS Statement on the Issuance of Binding Operations Directive 17-01*, Sept. 13, 2017, https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01.

compromise federal information and information systems directly implicates U.S. national security."[22]

These concerns are shared by foreign governments. For instance, in February 2018, Australia's Department of Home Affairs said it would conduct a national security assessment of Huawei in response to concerns about possible "threats and vulnerabilities" related to 5G.[23] Australia passed legislation in 2017 granting the government power to direct carriers to protect networks from national security risks. Earlier, Huawei had not been allowed to bid as a supplier for Australia's national broadband network in 2012. Australia also recently decided to fund an undersea connecting cable to the Solomon Islands itself, instead of allowing Huawei to serve as contractor.[24]

In Canada, members of the opposition party in March 2018 urged the federal government to reconsider allowing Huawei to sell telecom equipment, after three former national security officials cited worries about espionage.[25] Finally, the head of a major South Korean carrier, SK

---

[22] *Id.*

[23] Michael Walsh & Xiaoning Mo, *Security Alarm Sounded Over Chinese Company Huawei's Possible Involvement in Australia's 5G Network*, Australian Broadcasting Corporation, Mar. 11, 2018, http://www.abc.net.au/news/2018-03-11/security-concerns-over-chinese-firm-huawei-5g-technology/9522894.

[24] Dan Strumpf, Rob Taylor, & Paul Vieira, *Who's Afraid of Huawei? Security Worries Spread Beyond the U.S.: Concerns about Chinese telecom giant, World No. 1 in Wireless Equipment, Sprout in Canada, Australia and South Korea*, WALL ST. J., Mar. 20, 2018, https://www.wsj.com/articles/whos-afraid-of-huawei-security-worries-spread-beyond-the-u-s-1521561391.

[25] Robert Fife & Steven Chase, *Federal Government Won't Block Huawei's Business in Canada*, THE GLOBE AND MAIL, Mar. 19, 2018, https://www.theglobeandmail.com/politics/article-federal-government-wont-block-huaweis-business-in-canada/.

Telecom, recently voiced doubt about whether Huawei should serve as a supplier for its 5G network, saying Huawei is "a concern."[26]

Regarding ZTE, on April 16, 2018, the United Kingdom's National Cyber Security Centre, part of the Government Communications Headquarters intelligence agency, advised Britain's telecom operators not to buy from ZTE, saying "the national security risks arising from the use of ZTE equipment or services within the context of the existing UK telecommunications infrastructure cannot be mitigated."[27]

2. Congress and Executive Agencies with Security Expertise Have Taken Actions to Address Concerns with Those Suppliers.

Several concrete actions have now been taken by the U.S. government to impose restrictions upon the specific suppliers named in the Notice.[28] Importantly, these actions have typically been taken either by Congress or by executive branch agencies with access to appropriate national security expertise. The actions have taken various forms, including statutory restrictions, agency directives, prohibitions on corporate transactions, and even public or private pressure on service providers to avoid transactions with certain suppliers of concern.

---

[26] *See id.*

[27] National Cyber Security Center, *ZTE: NCSC advice to select telecommunications operators with national security concerns*, Apr. 16, 2018, https://www.ncsc.gov.uk/news/zte-ncsc-advice-select-telecommunications-operators-national-security-concerns-0. The UK government has taken notably extraordinary steps, the effectiveness of which is unclear, to ensure the security of the Huawei equipment in its communications infrastructure. *See, e.g.*, Paul Sandle & Brenda Goh, *Parliamentarians say Huawei-BT deal exposes flawed security controls*, REUTERS, June 7, 2013, https://uk.reuters.com/article/uk-britain-telecoms-huawei/parliamentarians-say-huawei-bt-deal-exposes-flawed-security-controls-idUKBRE9550RP20130607.

[28] The U.S. government also has taken action against these companies for non-security reasons that may nonetheless be relevant. *See infra* Section VI.A.

Statutory restrictions on procurement by federal agencies. In several cases, Congress has acted directly through enactment of statutory text, or implicitly through report language, to prohibit or discourage federal agencies from procuring equipment from specific suppliers of concern:

- **May 2011: FY 2012 National Defense Authorization Act ("NDAA") Committee Report details security concerns regarding Huawei and ZTE equipment.** The report from the House Armed Services Committee noted: "[g]iven the potential ties between the Chinese Government and malicious actors within China, the committee is alarmed that two state-owned Chinese firms, Huawei and ZTE, have been included on the Department of Agriculture's list of safe and approved telecommunications equipment providers for the U.S. broadband expansion program. … [T]he committee is concerned about the potential threat this may pose to national security as well as to Department of Defense data."[29]

- **February 2012: Spectrum Act prohibits 'barred' entities from participating in certain activities under FCC authority.** Section 6004 of the 2012 Spectrum Act prohibits any entity or person "who has been, for reasons of national security, barred by any agency of the Federal Government from bidding on a contract, participating in an auction, or receiving a grant" from receiving FirstNet and state implementation funds or participating in a spectrum auction.[30] This provision has been generally regarded as being intended to prohibit Huawei or ZTE from participating in FirstNet.

- **March 2013: FY 2013 Commerce, Justice, Science and Related Agencies Appropriations Act bars certain agencies from purchasing IT systems from China-subsidized entities.** Section 516(b) bars the Departments of Commerce and Justice, NASA, and the National Science Foundation from purchasing IT systems "produced, manufactured or assembled" by entities "owned, directed, or subsidized by the People's Republic of China" unless the purchase is "in the national interest of the United States."[31] Moreover, Section 516(a) requires that agencies must consult with the FBI or another appropriate federal entity to assess the risk of cyberespionage or sabotage before considering purchasing any such systems.[32]

---

[29] H.R. Rep. No. 112-78, at 198 (2011).

[30] Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96, title VI, § 6004, 126 Stat. 156, 205 (2012) (codified at 47 U.S.C. § 1404) ("2012 Spectrum Act").

[31] Commerce, Justice, Science, and Related Agencies Appropriations Act, 2013, Pub. L. No. 113-6, div. B, § 516(b), 127 Stat. 198, 274 (2013) ("CJS Appropriations Act 2013").

[32] *Id.* at § 516(a), 127 Stat. at 273-74.

- **December 2017: FY 2018 NDAA bars Kaspersky from all federal procurement and bars Huawei and ZTE by name from DoD nuclear and homeland security contracts.** Section 1634 prohibits all federal agencies from using any "hardware, software, or services developed or provided, in whole or in part," by Kaspersky Lab.[33] Section 1656 bars the Department of Defense from "procur[ing] or obtain[ing], or extend[ing] or renew[ing] a contract" with Huawei or ZTE for "any equipment, system, or service" that forms a substantial component of any nuclear deterrence or homeland security mission.[34] Section 888 further empowers the Defense Secretary to "terminate existing contracts or prohibit the award of contracts for the procurement of goods or services for the Department of Defense" from any "Chinese commercial entities" that "materially support the illicit activities on the part of North Korea."[35]

- **May 2018: FY 2019 NDAA (House version) would prohibit all federal procurement from Huawei and ZTE.** Section 880 of the FY 2019 NDAA (H.R. 5515), as passed by the House of Representatives on May 24, 2018, incorporates a version of the Defending Government Communications Act (H.R. 4747 / S. 2391) that would prohibit all federal procurement from Huawei or ZTE. The House bill would also require the Director of National Intelligence to develop a report outlining the national security risks of Huawei and ZTE technology, and require that an unclassified version of the report be made available to U.S. allies.[36]

Administrative restrictions on procurement. In several cases, administrative agencies have prohibited certain procurements by Huawei, ZTE, or Kaspersky Lab:

- **Sept. 2011: Department of Commerce bars Huawei from participating in FirstNet.** Huawei was initially invited to test its equipment for a nationwide public-safety broadband network in April 2011, but the Department prohibited it from participating.[37]

---

[33] National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, div. A, § 1634, 131 Stat. 1283, 1739 (Dec. 12, 2017) ("FY18 NDAA").

[34] *Id.* at § 1656, 131 Stat. at 1762.

[35] *Id.* at § 888, 131 Stat. at 1507.

[36] National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong., div. A, § 880 (as reported in House on May 15, 2018) ("H.R. 5515"), *available at* https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515rh.pdf; *see also* Defending Government Communications Act, H.R. 4747, 115th Cong. (2018), *available at* https://www.congress.gov/115/bills/hr4747/BILLS-115hr4747ih.pdf; S. 2391, 115th Cong. (2018) (Senate companion to H.R. 4747).

[37] *See* Eli Lake, *U.S. Blocks China Telecom Bid to Build Wireless Network Over Spying Concerns*, DAILY BEAST, Oct. 11, 2011, https://www.thedailybeast.com/us-blocks-china-telecom-bid-to-build-wireless-network-over-spying-concerns; Michael Kan, *Huawei told by US*

- **Sept. 2017: Department of Homeland Security bars Kaspersky from all federal government systems.** DHS issued a Binding Operational Directive that required all federal agencies to remove Kaspersky products from their systems within 90 days.[38] DHS stated that it was "concerned about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks." As DHS explained, "[t]he risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security."[39] Notably, while the Department of Defense is outside the jurisdiction of DHS, it stated that it too planned to "follow the intent of the directive."[40]

- **May 2018: Department of Defense orders retail stores on military bases to stop selling products made by Huawei and ZTE**. The ban is worldwide and based on the potential security threat the Pentagon believes the phones from these companies may pose.[41]

Discouraging commercial use. On occasion, U.S. government officials have advised the private sector to avoid using equipment from Huawei and ZTE. This has included targeted

---

Commerce Department they are a 'security concern', COMPUTERWORLD UK, Oct. 14, 2011, https://www.computerworlduk.com/it-vendors/huawei-told-by-us-commerce-department-they-are-a-security-concern-3310940.

[38] Letter from Elaine C. Duke, Acting Secretary, Department of Homeland Security, to all Federal Executive Branch Departments and Agencies, Binding Operational Directive BOD-17-01 (Sept. 13, 2017) ("Binding Operational Directive BOD-17-01"), https://cyber.dhs.gov/assets/report/bod-17-01.pdf.

[39] Press Release, Department of Homeland Security, DHS Statement on the Issuance of Binding Operational Directive 17-01 (Sept. 13, 2017), https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01.

[40] Joseph Marks, *Pentagon to Scrub Kaspersky from Defense Systems Following DHS Ban*, NEXTGOV, Oct. 23, 2017, https://www.nextgov.com/cybersecurity/2017/10/pentagon-scrub-kaspersky-defense-systems-following-dhs-ban/141978/.

[41] *See, e.g.*, Hamza Shaban, *Pentagon tells U.S. military basis to stop selling ZTE, Huawei phones*, WASH. POST, May 2, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/05/02/pentagon-tells-u-s-military-bases-to-stop-selling-zte-huawei-phones/.

outreach to certain service providers, as well as more general and public statements of concern in recent months:

- **Nov. 2010: Secretary of Commerce calls Sprint to express concern over potential use of Huawei or ZTE.** Sprint dropped plans to consider Huawei or ZTE for a contract worth billions of dollars "largely because of national security concerns in Washington." Commerce Secretary Gary Locke called Sprint to "discuss concerns about awarding [] work to a Chinese firm."[42]

- **Jan. 2018: AT&T and Verizon drop deals to market Huawei's Mate 10, reportedly in response to political pressure.** Reports indicated that political pressure may have been a factor in these decisions.[43] The Mate 10 will now be sold in the United States only through open channels.

- **Feb. 2018: Top U.S. Intelligence Chief Leaders recommend not using Huawei equipment.** The heads of the CIA, FBI, NSA, as well as the Director of National Intelligence, the Defense Intelligence Agency Director, and the National Geospatial Intelligence Agency Director, all recently testified at a U.S. Senate Select Committee on Intelligence hearing on worldwide threats that they would advise Americans against using Huawei products or services.[44]

Prohibitions of corporate acquisition transactions. On at least one occasion, the Committee on Foreign Investment in the United States ("CFIUS") has played a significant role in blocking transactions where concerns about Huawei have been a factor:

- **Feb. 2011: CFIUS intervenes with the Futurewei-3Leaf acquisition, and Huawei unwinds deal.** In 2010, Futurewei, Huawei's U.S. subsidiary, purchased assets from 3Leaf, a small US server technology firm. The DoD directed CFIUS staff to invite Huawei to file deal information after the fact. On February 11, 2011, CFIUS informed Huawei of its intent to recommend to the President that the Administration require the deal to be reversed, and Huawei unwound the deal.[45]

---

[42] Joann S. Lubin & Shayndi Raice, *Security Fears Kill Chinese Bid in U.S.*, WALL ST. J., Nov. 5, 2010, https://www.wsj.com/articles/SB10001424052748704353504575596611547810220.

[43] Stephen Shankland, *Verizon-Huawei pact reportedly hit by political pressure*, CNET, Jan. 9, 2018, https://www.cnet.com/news/verizon-huawei-mate-10-pro-political-pressure-ces/

[44] Sara Salinas, *Six top US intelligence chiefs caution against buying Huawei phones*, CNBC, Feb. 13, 2018, https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html; Senate Intel Feb. 13 Hearing, *supra* n.12.

[45] Shayndi Raice, *Huawei Set Back on Deal in U.S.*, WALL ST. J., Feb. 15, 2011, https://www.wsj.com/articles/SB10001424052748703703804576144892603923096.

C. Actions Beyond USF Restrictions Should be Considered in a Further Notice of Proposed Rulemaking.

While the facts above provide ample justification for the Commission to restrict USF funding, the Notice also briefly seeks comment on whether the agency should take additional steps beyond the scope of the USF program, including targeting non-USF-funded equipment or services from companies that might pose the same or similar threats to U.S. communications networks.[46] It is logical that if equipment or services from certain companies is deemed to pose a sufficient threat to require action in the USF context, such equipment or services would also pose a similar threat in other contexts as well.

Nevertheless, for its immediate next steps, the Commission should proceed with caution, beginning in the area where it is on its strongest legal footing, and deferring any further action outside the scope of USF at this time. As discussed in Section II below, while the Commission has clear legal authority to condition the distribution of USF support to companies who do not include technology or services from specifically identified risks, the agency should not on its own make unilateral national security determinations. Thus, limiting its actions here to USF based on national security determinations made by other expert federal agencies and Congress is the appropriate first-step action at this time.

Having said that, the Commission may wish to seek further comment on any additional steps the Commission should take as part of a Further Notice of Proposed Rulemaking ("FNPRM") that considers building off the limited initial action focused on USF. For example, extending restrictions beyond the USF context would likely require a much more detailed examination of the Commission's legal authority beyond the analysis contemplated by the

[46] Notice ¶ 31.

Notice. While the Notice does briefly ask commenters to address the scope and extent of its legal authority to take broader actions,[47] the Commission would be far better served procedurally by working through those issues in an FNPRM.

Moreover, any action by the Commission in this proceeding – whether limited to the USF context or not – will unfold against a remarkably fluid and dynamic backdrop that includes significant high-level attention from the Administration and from Congress. On May 24, 2018, the House of Representatives passed the FY19 National Defense Authorization Act, which as described above includes a section based on the proposed Defending U.S. Government Communications Act (H.R. 4747 / Rep. Conaway and S. 2391 / Sen. Cotton) that would extend prohibitions on Huawei and ZTE equipment or services to *all* U.S. agencies.[48] Meanwhile, it has been widely reported that the President is considering issuing an executive order that will

[47] *Id.*

[48] *See supra* n.36. During floor debate, the House approved an amendment to this bill that named three additional Chinese video surveillance companies. *See* 164 Cong. Rec. H4610 (daily ed. May 23, 2018), https://www.congress.gov/crec/2018/05/23/CREC-2018-05-23.pdf (text of Amendment. No. 17, adding Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company); *id.* at H4656 (statement of Rep. Hartzler). Another approved amendment targeting funding for state and local governments extended the prohibitions to grant and loan funding. *See id.* at H4610 (text of Amendment No. 18); *id.* at H4655 (statement of Rep. McCaul) (the original version of the bill "does not apply to State and local governments, who often rely on Federal grant dollars and play a major role in the protection of our Nations' security, and that is why I have offered this amendment. My amendment simply extends the prohibition on purchasing ZTE and Huawei products and services to Federal grant money and loans to better safeguard State and local communications networks.").

specifically target equipment and services from Huawei and ZTE.[49] And since May 14, 2018, the President has indicated that he is personally focused on ZTE for geopolitical and economic reasons,[50] has apparently negotiated a deal that would mitigate the effect of other regulatory actions,[51] and is now encountering "fierce bipartisan opposition" from Congress.[52]

Against this rapidly-evolving backdrop, the Commission would be wise to take a limited but important and well-considered step that leverages its unquestioned legal authority over USF funding while deferring national security judgments to agencies or processes in the executive branch with appropriate expertise. By doing so, the Commission would set an example for other federal agencies, as well as for state and local governments that may be grappling with these

---

[49] *See, e.g.*, John D. McKinnon, *U.S. Weighs Curbs on Chinese Telecom Firms Over National-Security Concerns*, WALL ST. J., May 2, 2018, https://www.wsj.com/articles/u-s-weighs-curbs-on-chinese-telecom-firms-over-national-security-concerns-1525279627; Ana Swanson & Cecilia Kang, *White House Considers Barring Chinese Telecom Sales as Tensions Mount*, N.Y. TIMES, May 2, 2018, https://www.nytimes.com/2018/05/02/us/politics/trump-china-telecoms-restrictions.html.

[50] President Donald J. Trump (@realDonaldTrump), Twitter (May 13, 2018, 8:01 AM), https://twitter.com/realDonaldTrump/status/995680316458262533 ("President Xi of China, and I, are working together to give massive Chinese phone company, ZTE, a way to get back into business, fast. Too many jobs in China lost. Commerce Department has been instructed to get it done!").

[51] Ana Swanson, *Trump Administration Plans to Revive ZTE, Prompting Backlash*, N.Y. TIMES, May 25, 2018 ("The Trump administration told lawmakers it had reached a deal that would keep the Chinese telecom firm ZTE alive[.]"); https://www.nytimes.com/2018/05/25/us/politics/trump-trade-zte.html; President Donald J. Trump (@realDonaldTrump), Twitter (May 25, 2018, 4:07 PM), https://twitter.com/realDonaldTrump/status/1000151354701213696 ("... Obama Administration let phone company ZTE flourish with no security checks. I closed it down then let it reopen with high level security guarantees, change of management and board, must purchase U.S. parts and pay a $1.3 Billion fine ...").

[52] Damian Paletta, *Trump says he'll spare Chinese telecom ZTE from collapse, defying lawmakers*, WASH. POST, May 25, 2018, https://www.washingtonpost.com/business/economy/congress-threatens-to-block-deal-between-white-house-china-to-save-telecom-giant-zte/2018/05/25/1db326ba-604a-11e8-9ee3-49d6d4814c4c_story.html

issues, for every private-sector owner and operator of network infrastructure, and potentially even for Congress itself as it considers how best to establish a national framework for addressing these issues in a coordinated fashion. In short, the Commission is not acting in a vacuum, and it will serve national objectives best by acting in an expeditious but also deliberate and procedurally sound manner that provides the rest of the government – and the ICT industry – with an opportunity to respond to its first steps.

II. THE COMMISSION HAS LEGAL AUTHORITY TO RESTRICT UNIVERSAL SERVICE SUPPORT, BUT SHOULD IDENTIFY LIMITING PRINCIPLES REGARDING ITS NATIONAL SECURITY AUTHORITY.

TIA agrees with the Commission that "the promotion of national security is consistent with the public interest,"[53] and that the Commission can therefore promote national security interests through its USF oversight responsibilities. However, this basic logic could be extended too far without a sufficient limiting principle. The solution lies in addressing how and by whom "national security" determinations are made. For that, the Commission should look to Section 1 of the Communications Act, to other provisions of the Act that address how and *by whom* national security determinations are made, and to its own history. These considerations both inform and place important limits on the Commission's legal authority in this area.

A. Sections 201 and 254(b) of the Communications Act Permit Restricting USF Support to Promote National Security.

Commission precedent, supported by the courts, makes clear that the agency is on solid legal ground to place conditions on the use of USF support – in this case, a condition that USF not be used on products from suppliers identified as posing national security risks. The Notice correctly identifies Sections 201(b) and 254 of the Act as providing ample legal authority for the

[53] Notice ¶ 35.

proposed rule.[54] Section 201(b) establishes the Commission's authority to promulgate "such rules and regulations as may be necessary in the public interest to carry out the provisions of this Act."[55] Section 254 states that USF recipients "shall use that support only for the provision, maintenance, and upgrading of facilities and services for which the support is intended."[56] As the expert agency tasked with meeting the statute's universal service directives, the Commission is permitted to determine that certain requirements must be met in order for a USF recipient to use the support in a manner for which such support is intended – in this case in a manner that ensures the protection of national security interests.

In 2011, the Commission adopted its landmark *USF Transformation Order* which conditioned the receipt of high-cost USF support on the deployment of networks capable of delivering broadband and in fact offering broadband service, even though the supported service remained voice telephony.[57] The Commission determined that it had a "'mandatory duty' to adopt universal service policies that advance the principles outlined in section 254(b)," and that it had "the authority to 'create some inducement' to ensure that those principles are achieved."[58] Among those are principles "necessary and appropriate for the protection of the public interest, convenience, and necessity. . . ."[59]

---

[54] *Id.* ¶¶ 35-36.

[55] 47 U.S.C. § 201(b).

[56] *Id.* § 254(e).

[57] *Connect America Fund*, Report and Order and Further Notice of Proposed Rulemaking, 26 FCC Rcd 17663, 17684-76 ¶¶ 61-65 (2011) ("*USF Transformation Order*").

[58] *Id.* at 17686 ¶ 64.

[59] 47 U.S.C. § 254(b)(7).

The 10th Circuit upheld the order, finding that "nothing in the statute limits the FCC's authority to place conditions . . . on the use of USF funds."[60] The Court determined that "it is reasonable to conclude that Congress left a gap to be filled by the FCC, *i.e.*, for the FCC to determine and specify precisely how USF funds may or must be used."[61] The court concluded further that it "is consistent both with § 254(c)(1)'s express grant of authority to the FCC to periodically redefine 'universal service' and § 254(b)'s express charge to the FCC to 'base policies for the preservation and advancement of universal services on' a specific set of controlling principles outlined by Congress."[62]

In this situation, the Commission has determined that it is in the public interest to ensure that USF dollars are not permitted to be spent on technology or services provided by companies that pose a national security risk. For the reasons described above,[63] TIA agrees that adopting such a condition is in the public interest. The Commission is therefore justified in determining that such a condition would advance the principles outlined in Section 254(b).

The Notice also inquires whether adopting the proposed rule would be equivalent to establishing a new definition of the "evolving level of telecommunications services" that are supported by USF mechanisms under Section 254(c)(1).[64] In TIA's view, these are not equivalent concepts. However, conditioning the support as proposed is clearly in the public interest and consistent with the statute's directive to the FCC to ensure its universal policies

---

[60] *Direct Communs. Cedar Valley, LLC v. FCC (In re FCC 11-161)*, 753 F.3d 1015, 1046 (10th Cir. 2014).

[61] *Id.*

[62] *Id*. at 1047.

[63] *See supra* Section I.

[64] Notice ¶ 36.

evolve along with changes in the communications marketplace. The introduction of increased cybersecurity risk is one the most prevalent aspects of the evolution of modern networks, and the Commission is right to ensure its USF policies keep up.

B. National Security Provisions of the Communications Act and Relevant Precedents Make Clear that the Commission's Actions Should be Based Upon Determinations Made by Expert Security Agencies or Statutory Requirements from Congress.

While the *USF Transformation Order* and its review by the 10th Circuit establish the Commission's authority to condition the receipt of USF support, invoking national security involves other important considerations that limit the reach of the Commission's authority. In the 2011 order, the Commission conditioned support on the offering of broadband-capable networks based on its expert determination that requiring broadband deployment was necessary to meet the principles of Section 254(b). A determination about the importance of broadband, particularly on the heels of the release of the National Broadband Plan, was easily within the wheelhouse of the Commission's expertise.

In contrast, while Section 1 of the Communications Act specifies that one of the reasons for the Commission's creation is "for the purpose of national defense,"[65] the Commission has rarely (if ever) relied upon its own independent determinations of which specific practices – or entities – would negatively impact the "national defense." Accordingly, in this proceeding, the Commission should be careful to avoid making national security judgments of its own. Instead, both precedent and statutory text show that the Commission's efforts to further national defense have relied upon determinations made by Congress, by the President, or by executive branch

[65] 47 U.S.C. § 151.

agencies with appropriate staffing and expertise who are presumed to act in the President's name.

For example, in 1958 the Commission acted on an expedited basis to modify certain frequency allocations at the request of the Office of Defense Mobilization ("ODM").[66] The Commission cited ODM's representations that the changes were "required either because of vital national defense considerations or are desirable changes incident thereto," as well as ODM's statements about the changes being necessary "due to the international political climate and the advent of the 'space age.'"[67] The D.C. Circuit upheld the Commission's actions against a treaty-based challenge, finding that "the Commission *pursuant to the exercise of the prerogative of the Executive* correctly conformed its Rules to accommodate the national defense requirements."[68] The court observed that "[n]ational trust and responsibility must be reposed somewhere and in this situation … they are centered in the President with all his vast power. He is the Commander in Chief."[69]

Likewise, communications-related directives from Congress regarding national security issues have typically invoked the expertise of the President, or by extension executive branch agencies acting in his name. Virtually every provision of the Communications Act or the NTIA Organization Act relating to national defense requires relevant determinations to be made by the

---

[66] *Amendment of Parts 2, 4, 7, 8. 9. 10, 11,12, 16 and 41 of the Commission's Rules and Regulations to reallocate certain frequency bands above 25 [MHz], now designated for exclusive Amateur or other non-Government use, to Government services on a shared or exclusive basis, and conversely to reallocate to non-Government use certain bands now designated for Government use*, Memorandum Opinion and Order, FCC 58-379, 23 Fed. Reg. 2,676, 2,677 (Apr. 23, 1958), https://www.gpo.gov/fdsys/pkg/FR-1958-04-23/pdf/FR-1958-04-23.pdf.

[67] *Id.* at 2,677 ¶ 2.

[68] *Bendix Aviation v. FCC*, 272 F.2d 533, 538 (D.C. Cir. 1959) (emphasis added).

[69] *Id.* at 540.

President or by Congress.[70] While Section 6004 of the 2012 Spectrum Act is somewhat broader, it still does not repose national security determinations in the Commission, instead prohibiting any entity "who has been, for reasons of national security, barred by *any agency of the Federal Government*" from participation in certain spectrum auctions or participation in FirstNet.[71]

Thus, the Commission must look to national security determinations made by Congress or by an appropriate U.S. government agency or body regarding a certain supplier. Based on such determinations, the Commission may then take reasonable action to prevent USF funding from being spent on products from that supplier. Preventing funds from being spent on products from a supplier determined to pose a risk to national security easily qualifies as an "appropriate" action to protect the public interest. In short, once Congress or appropriate executive agencies have determined that state-sponsored cyberespionage is taking place, and also determined that products from specific suppliers associated with those governments pose a heightened national security risk, the Commission may prevent the use of federal funds on such products.

As we have demonstrated in Section I.B above, a sufficient record of action by Congress and executive agencies now exists to justify Commission action regarding the companies specifically mentioned in the Notice. Despite this, the issue of legal authority is not merely an academic one. In this proceeding, the Commission is exercising its infrequently-used authority

---

[70] *See, e.g.*, 47 U.S.C. § 302a(c) (certain wireless devices are exempt from the Commission's interference regulations if developed "under United States Government criteria … taking into account the unique needs of national defense and security"); *id.* § 303(c) (President's authority to make national security determinations regarding radio licenses owned by foreign governments); *id.* § 308(a) (emergency license applications permitted only in a declared emergency proclaimed by the President or declared by Congress); *id.* § 606 (President may invoke communications war powers "if *he* finds it necessary for the national defense and security") (emphasis added); *see also id.* §§ 924(b)(1), (b)(2)(A) (President may determine whether certain frequency reassignments would jeopardize national defense interests).

[71] 2012 Spectrum Act § 6004, 47 U.S.C. § 1404 (emphasis added).

"to promote the national defense" while opening the door to a new type of rulemaking with potentially far-reaching implications for the global ICT marketplace. Therefore, establishing well-defined limiting principles at the outset is important to provide certainty to the broader ecosystem and avoid difficulties in the future.

III. DECISIONS TO RESTRICT USF SUPPORT DUE TO NATIONAL SECURITY CONCERNS SHOULD BE NARROWLY TAILORED TO ADDRESS SPECIFIC SUPPLIERS OF CONCERN, NOT GLOBAL SUPPLY CHAIN RISK MANAGEMENT GENERALLY.

As described above, the Commission's actions in this area should be carefully informed and limited by national security determinations made by Congress or by agencies with appropriate expertise. Once such determinations have been made, it remains important to delineate an appropriate scope and focus for the Commission's own actions to further national security goals. As the agency moves forward in this proceeding, its decisions must balance practical considerations, effectiveness in promoting security goals, the reality of the global ICT supply chain, and the significant repercussions its actions will likely have around the world. The best way for the agency to balance these factors is by focusing on specific suppliers rather than global supply chains.

A. Supply Chain Risk Management Is Best Addressed Through Public-Private Partnerships and Consensus-Based Industry-Driven Standards.

As TIA understands it, this Notice does not seek to address cybersecurity risk management *generally*, which necessitates a consensus-based, industry driven approach. Rather, we believe this Notice seeks to address the *discrete* question of how to revise the Commission's procurement policies to remain supportive of national security, based on the trustworthiness (or lack thereof) of certain suppliers. Once an appropriate determination has been made that a certain supplier's involvement in the nation's ICT supply chain poses a credible threat to national

security, the Commission may determine that it is in the public interest to prevent that supplier's equipment from being deployed in networks supported by the universal service programs.[72] Such targeted action by the Commission should complement, rather than supplant or disrupt, ongoing efforts to develop and refine approaches to supply chain risk management more broadly.

As a general matter, supply chain risk management is a complex process. In a global marketplace with dynamic sourcing practices and an ever-evolving threat landscape, each supplier of telecommunications products – like each enterprise that uses those products – must, on an ongoing basis, make holistic assessments of the risks faced by its ecosystem and make informed decisions about what risks it is willing to accept. This complex undertaking has advanced significantly – and continues to do so – through government-facilitated multi-stakeholder collaboration and through industry standards-setting processes. TIA itself has been a leader in these efforts in various fora, championing policies to facilitate effective approaches to

[72] TIA disagrees with the assertion by the Rural Wireless Association ("RWA") that the Commission is proposing to abandon the longstanding partnership model on which current cybersecurity risk management is founded. *See* Letter from Caressa D. Bennet & Erin P. Fitzgerald, Rural Wireless Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89, at 1 (filed Apr. 9, 2018) ("RWA Ex Parte"). TIA has long been a participant in these efforts and we continue to view this work, in agreement with RWA, as the critical foundation to understanding and addressing supply chain security risk management overall. As discussed herein, if tailored appropriately, consistent with the Commission's articulated intention to "take targeted action to ensure that USF funds are not used in a way that undermines or poses a threat to our national security," Notice ¶ 12, the current proceeding should in no way encroach on that which is best left to the purview of the partnership model.

supply chain and cybersecurity risk management through strong collaboration between public and private sectors, across industries, and within the international community.[73]

Multistakeholder collaboration. Multistakeholder collaboration takes various forms, including public-private partnerships. The partnership model, as articulated in guiding documents such as the Defense Industrial Base ("DIB"),[74] Executive Orders 13636 and 13800,[75]

[73] *See, e.g.*, Comments of the Telecommunications Industry Association, *Developing a Framework To Improve Critical Infrastructure Cybersecurity*, NIST Docket No. 130208119-3119-01 (filed Apr. 8, 2013), https://www.tiaonline.org/wp-content/uploads/2018/02/TIA_Comments_NIST_Cybersecurity_Framework_040813.pdf; Comments of the Telecommunications Industry Association, *Defense Federal Acquisition Regulation Supplement: Requirements Relating to Supply Chain Risk (DFARS Case 2012-D050)* (filed Jan. 17, 2014), https://www.regulations.gov/contentStreamer?documentId=DARS-2013-0052-0005&attachmentNumber=1&contentType=pdf; Comments of the Telecommunications Industry Association, *FCC's Public Safety and Homeland Security Bureau Requests Comment on CSRIC IV Cybersecurity Risk Management and Assurance Recommendations*, PS Docket No. 15-68 (filed May 29, 2015), https://ecfsapi.fcc.gov/file/60001076156.pdf; Comments of the Telecommunications Industry Association, *Promoting Stakeholder Action Against Botnets and Other Automated Threats*, NTIA Docket No. 170602536-7536-01 (filed July 28, 2017), https://www.ntia.doc.gov/files/ntia/publications/tia_comments_on_ntia_botnet_reduction_rfc.pdf ; Comments of the Telecommunications Industry Association, *Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity*, NIST Docket No. 130208119-3119-01 (filed Apr. 10, 2017), https://www.tiaonline.org/wp-content/uploads/2018/02/TIA-Comments-on-NIST-Framework-Update-4-10-2017.pdf; Comments of the Telecommunications Industry Association, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Draft 2* (filed Jan. 19, 2018), https://www.tiaonline.org/wp-content/uploads/2018/02/TIA-Comments-on-CSF-V1.1-Draft-2_.pdf. TIA has also engaged in CSRIC, in NTIA multistakeholder processes such as "IoT Updatability and Patching," and in the Communications and Information Technology Sector Coordinating Councils (CSCC and ITSCC).

[74] Department of Defense, *Defense Industrial Base, Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan*, May 2007, https://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf.

[75] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, Feb. 12, 2013, 78 Fed. Reg. 11,737 (Feb. 19, 2013), https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf; Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017, 82 Fed. Reg. 22,391 (May 16, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

and Presidential Policy Directive 21 ("PPD-21"),[76] enables the United States to coordinate between federal agencies, across industry sectors, and among a variety of actors in between.[77] Such partnership is exemplified in the work of entities like the Government and Sector Coordinating Councils, which define joint policy priorities and provide recommendations on issues related to critical infrastructure security;[78] the Information Sharing Analysis Centers and Organizations (ISACs and ISAOs), which provide all-hazard threat and mitigation information to asset owners and operators;[79] as well as open and transparent processes like the one recently led by the Departments of Commerce and Homeland Security to develop the "Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats."[80]

The success of the multistakeholder collaboration model is illustrated most vividly through the development and use of the "Framework for Improving Critical Infrastructure Cybersecurity" ("Cybersecurity Framework") under the auspices of the National Institute for

---

[76] Directive on Critical Infrastructure Security and Resilience, Presidential Policy Directive/PPD-21, 2013 DAILY COMP. PRES. DOC. 91 (Feb. 12, 2013), https://www.gpo.gov/fdsys/pkg/DCPD-201300092/pdf/DCPD-201300092.pdf ("PPD-21"); *see also* Interagency Security Committee, *Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper*, Feb. 2015, https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf;

[77] *See also infra* Section VI.A (further describing the relevance of PPD-21).

[78] *See* IT Sector Coordinating Council, http://www.it-scc.org; Communications Sector Coordinating Council, https://www.comms-scc.org.

[79] National Council of ISACs, https://www.nationalisacs.org.

[80] Secretary of Commerce and Secretary of Homeland Security, *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other, Automated, Distributed Threats, Transmitted by the Secretary of Commerce and the Secretary of Homeland Security*, May 22, 2018, https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf ("Botnet Report").

Standards and Technology ("NIST"). Since 2013, the NIST Cybersecurity Framework has emerged as a voluntary, internationally accessible toolkit for entities of all kinds to comprehensively identify and address cybersecurity risks in general. The most recent update to the NIST Cybersecurity Framework, in Version 1.1, includes new sections aimed specifically at supply chain risk management.[81] Meanwhile, the Commission's own Communications Security, Reliability, and Interoperability Council ("CSRIC") has convened various industry-led working groups to examine cybersecurity risk management in general and supply chain issues in particular, producing resources that are of enduring value to the IT and communications sectors. As an illustrative example, the CSRIC V Working Group 6 issued a report in March 2016 that urged suppliers to apply the NIST Cybersecurity Framework to themselves, including a table of best practices.[82]

Industry standards. Many entities also use non-profit models like the Factor Analysis of Information Risk (FAIR) methodology to measure, manage, and report on information risk or standards from bodies like the International Standards Organization ("ISO"). The Common Criteria for Information Technology Security Evaluation ("Common Criteria") and its

---

[81] *See* National Institute for Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, pub. Apr. 16, 2018, https://www.nist.gov/sites/default/files/documents/2018/05/14/framework_v1.1_with_markup.pdf. The new version includes an expanded Section 3.3 titled *Communicating Cybersecurity Requirements with Stakeholders* to help "users better understand Cyber Supply Chain Risk Management (SCRM)," a new Section 3.4 titled *Buying Decisions* that "highlights use of the Framework in understanding risk associated with commercial off-the-shelf products and services," as well as additional SCRM criteria incorporated in the Implementation Tiers and a SCRM category added to the Framework Core.

[82] *See* Communications Security, Reliability, and Interoperability Council V, Working Group 6, *Secure Hardware and Software: Security-By-Design Working Group 6 – Final Report: Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network*, at 12-17 (Mar. 2016), https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_FINAL_%20wAppendix_0316.pdf.

companion Common Methodology for Information Technology Security Evaluation, for example, are a suite of ISO/IEC standards that provide a technical framework for producers of IT products to specify their security functional and assurance requirements, enable vendors to communicate the security attributes of their products, and testing laboratories to evaluate those products to ensure consistency with a vendor's claims.[83] Such a process provides assurance that the process of specification, implementation, and evaluation of a computer security product has been conducted in a rigorous, standard, and repeatable manner at a level that is commensurate with the target environment for use.

Similarly, the Open Group Trusted Technology Forum ("Open Group TTF") is a global supply chain integrity program that certifies technology providers to help assure against maliciously tainted and counterfeit components and products throughout the commercial off the shelf ("COTS") ICT product life cycle, encompassing the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal.[84] Time and again, public and private experts from across sectors and disciplines have found that industry's expertise and operational experience uniquely qualify it to lead the way toward defending against malicious cyber

[83] *See* The Common Criteria, *Common Criteria*, https://www.commoncriteriaportal.org.

[84] *See* The Open Group, *The Open Group Trusted Technology Forum*, http://www.opengroup.org/getinvolved/forums/trusted.

threats,[85] noting that any policy approaches to cybersecurity risk management must enable coordination across stakeholders in the ecosystem.[86]

Inapplicability to this situation. In TIA's experience, the public-private partnerships and industry standards described above have become a valuable set of risk assessment procedures that are improving supply chain security significantly. Indeed, stakeholders in the ICT industry have already implemented, or are currently implementing, these procedures. To be sure, some of these procedures are relevant to the issues discussed in the Notice, including items regarding assessments of governance (for the compromised supplier) or regarding the removal of certain suppliers from the supply chain (for all others). But on the whole, these various tools do not address – and were not intended to address – defenses against state actors' strategic exploitation of specific suppliers that are potentially beholden to them. The government can and must bring its unique resources and intelligence information to bear on those problems; such resources and

[85] *See, e.g.*, PPD-21, *supra* n.76 (explaining that "[c]ritical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient"); *see also* Communications Sector Coordinating Council, Industry Technical White Paper, July 17, 2017, https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf; Satellite Industry Association (SIA), Global VSAT Forum (GVF), & EMEA Satellite Operators Association (ESOA), Joint Statement on the Satellite Industry's Commitment to Cybersecurity and a Secure Supply Chain, May 2018, at 2, https://gvf.org/images/pdf/SIAGVFESOAcybersecMay2018.pdf (stating that "many industry-led efforts have proven effective at developing cybersecurity best practices and sharing valuable information").

[86] *See, e.g.*, Botnet Report, *supra* n.80, at 5; *see also* NTIA Multistakeholder Working Group on Incentives, Barriers, and Adoption, Incentives and Barriers to Adoption of IoT Update Capabilities, Nov. 2017, at 2, https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_incentives_nov2.pdf ("[a]ddressing these challenges and concerns requires a multi-stakeholder process, involving industry, consumers, and governments to align and collaborate").

information are much more difficult to leverage through industry standards or public-private partnership models.

Ultimately, the discussion above of just a few of the robust tools and processes already in place highlights that the Commission's proposed actions in this proceeding are appropriately focused on certain specific suppliers deemed to pose a national security risk, rather than supply chain risk management in general. Broader goals regarding supply chain risk management will continue to be most effectively addressed by multistakeholder-produced resources and industry-driven standards setting processes such as those described above.

B. Product Testing is Not a Viable Mechanism to Address the Concerns Raised in the Notice.

The Rural Wireless Association has urged the Commission to focus its efforts on creating a "standards and testing based system,"[87] rather than "imposing a 'country of origin' prohibitory regime"[88] or a "ban on specific vendors via a USF eligibility disqualification."[89] Of course, TIA does not understand the Commission to be proposing a country of origin ban; we oppose such a ban. (*See* Section III.D below.) Rather, the Commission is proposing to ban specific suppliers that have been identified by Congress or by other expert agencies as posing a national security risk.

Nevertheless, the Commission seeks comment on "testing regimes, showings, or steps" that it should consider "in addition or as an alternative" to restricting USF support.[90] To be sure, a rigorous assurance regime in product design, manufacturing, testing, and support is an

[87] RWA Ex Parte, *supra* n.72, at 1.

[88] *Id.*

[89] *Id.* at 5.

[90] Notice ¶ 31.

important element of ensuring that products are secure. The ICT industry is engaged in continuous and extensive work to improve the security of communications technology products, including through product testing and standards development. (*See* Section III.A above.)

That said, product testing is not presently a viable mechanism for addressing the specific concern most directly raised by the Notice, namely, the threat of state-sponsored cyberespionage or malicious network disruption arising from products made by suppliers closely connected with those state actors. Understanding why this is so requires a brief exploration of possible threat vectors. In short, the Commission's concern seems most targeted at addressing the risk of *deliberately compromised* products – those that have been intentionally altered by a state-sponsored actor to enable future exploitation – rather than those products that are merely *vulnerable* to a future attack due to inherent weaknesses in design or implementation.

Deliberately compromised products. It is very challenging to construct a testing regime to detect whether a communications technology product has been deliberately and covertly compromised. As one analysis of the issue explains:

> In an ideal world, corrupted designs would be detected, regardless of their source. However, the sheer complexity of modern chips greatly impedes such detection. While *extensive* – but not *exhaustive* – testing is performed during the design and manufacturing process, the goal of this testing is to confirm that a chip is behaving as expected. The testing procedures are very good at identifying accidental design flaws, but are poorly suited to ferreting out intentionally hidden malicious circuitry.
>
> Consider the following example: suppose that a company outsources the design for a block of the chip that is supposed to add the number six to any input. During testing, if 20 is provided to this block, the block outputs 26. When 127 is provided, the block outputs 133. One hundred thousand more inputs are provided, and in every case, the result comes back correct. This block will be deemed to have passed functional testing. But the block could have a hidden circuit triggered by an input with value 126,321,204. When that input – and that input alone – arrives, an attack is launched. Because testing

> can't possibly be *exhaustive*, this input will never be encountered until it is provided months later by an attacker.[91]

While the passage above describes a hardware attack, the challenge is similar for software: a hidden backdoor might only enable access to a router at a very specific time – perhaps only a few days or even minutes of every year – and in response to a very specific input sequence, rendering detection through testing virtually impossible.[92]

Even assuming that a testing lab is given complete access to a product's chip or circuit designs (hardware) and source code (software) – neither of which is commercially possible in many cases due to trade, intellectual property, or other concerns – it would still be extremely difficult to detect a deliberate covert attack. For example, detection of compromised software would require detailed forensic examination of a product's source code to verify that there are no

[91] John D. Villasenor, *Ensuring Hardware Cybersecurity*, ISSUES IN TECHNOLOGY INNOVATION, at 5 (Brookings, Wash. D.C.), May 2011 (emphasis added), https://www.brookings.edu/wp-content/uploads/2016/06/05_hardware_cybersecurity.pdf

[92] A recently-discovered security breach at the Multi-State Lottery Association ("MUSL") – the organizer of the Powerball and Hot Lotto games – is instructive. Using only 21 lines of code, MUSL's information-security director, Eddie Tipton, rigged the outcome of the national Hot Lotto game for over a decade, but only under certain conditions that would occur no more than three times per year. *See* Reid Forgrave, *The Man Who Cracked The Lottery*, N.Y. TIMES MAGAZINE, May 3, 2018, https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-iowa-lottery-fraud-mystery.html.

exploits.[93] Even then, a backdoor could be overlooked, since any code inserted by a sophisticated state-sponsored actor would likely be cleverly hidden rather than appearing as an obvious extra subroutine with no apparent legitimate purpose.[94] Detection of hardware exploits would potentially require circuit analysis and a much more sophisticated level of engineering expertise.

Matching solutions to risks. While testing is not well-suited to mitigating the risk of deliberately compromised products, other risk management options are available. For example, applying the CSRIC V Working Group 6 best practices listed above (*see* Section III.A *supra*), a blanket prohibition on products from certain identified suppliers – such as that under consideration by the Commission here – can be viewed as a top-level "identification" of risk.

---

[93] *See, e.g.*, Stu Woo, *Are Huawei and ZTE a Real Cybersecurity Threat?*, WALL ST. J., May 29, 2018, https://www.wsj.com/articles/are-huawei-and-zte-a-real-cybersecurity-threat-1527611521 ("Not only do the electronics run on software with possibly millions of lines of code, but it is frequently updated by the manufacturer remotely … [t]hat makes it nearly impossible for a wireless carrier or a government to detect whether there is a 'back door' that could allow the manufacturer to remotely switch off a tower's electronics, or send data to somewhere it shouldn't go."). The article posits that it would be "much more difficult" for an equipment manufacturer to conduct espionage, as opposed to shutting down a device completely, since "[m]ost *wireless* carriers use sophisticated software that can automatically detect anomalous behavior, such as equipment that sends data to unexpected places." *Id.* (emphasis added). However, state-sponsored actors could potentially evade such countermeasures by disguising the retransmission of any intercepted data, perhaps by embedding it within other innocuous data. Meanwhile, some smaller and/or wireline broadband carriers would likely not have such "sophisticated software" countermeasures in place.

[94] *Id.* ("'When you're dealing with millions of lines of code, there's always going to be a vulnerability,' says Darien Huss, a researcher at Sunnyvale, Calif.-based cybersecurity firm Proofpoint Inc. 'A piece of code could look legitimate, but it could be a back door. There are a lot of ways to hide it.'"); *see also* Gus Fritschie & Evan Teitelman, *Backdooring the Lottery and Other Security Tales from Gaming* (Powerpoint presentation), SeNet International Corp., July 30, 2017, at 39, https://www.senet-int.com/s/Backdooring-the-Lottery.ppt (visited May 13, 2018). In describing their work on the MUSL lottery case, *supra* n.92, Fritschie and Teitelman note that the compromised random number generator (RNG) code had been certified by a major testing lab, after the lab had performed an audit of the source code.

Appropriate mitigation methods can then be implemented by downstream suppliers to protect against any legitimate risks associated with various products from that supplier.

Proper role for testing. Product testing can be a very useful means of detecting inadvertent security *vulnerabilities*, either in a single product or in an enterprise network. Penetration testing has become a well-established practice for government and commercial networks alike, and many vendors now offer such testing and/or tools for organizations to conduct their own tests.[95] The ICT industry actively engages in its own rigorous testing and certification regimes to reduce or eliminate inadvertent security vulnerabilities to the greatest extent possible.

However, as described above, testing is not the proper approach to address the supplier-specific national security concerns raised in the Notice. Nor should the Commission expand the scope of its action by imposing testing mandates to address various product vulnerabilities, particularly when these issues have largely evolved in other forums including public-private partnerships and consensus-based industry standards. (*See* Section III.A *supra*.) Finally, the Commission does not have the appropriate expertise to mandate and monitor compliance with any particular cybersecurity product testing regime.

[95] *See, e.g.*, Intertek, *Cyber Security Services*, http://www.intertek.com/cybersecurity/ (visited May 22, 2018); Rapid7, *Products*, https://www.rapid7.com/products/ (visited May 22, 2018); Nettitude, *Penetration Testing*, https://www.nettitude.com/uk/penetration-testing/ (visited May 22, 2018); Kroll, *Penetration Testing Services*, https://www.kroll.com/en-us/what-we-do/cyber-security/prepare-and-prevent/penetration-testing (visited May 22, 2018); KPMG, *Penetration testing and Cyber-security defence*, https://home.kpmg.com/ro/en/home/services/advisory/consulting/cyber-security/penetration-testing-cyber-security-defence.html (visited May 22, 2018).

C. The Commission's Actions Should Remain Narrowly Tailored to Avoid Disruption to Broader U.S. International Trade Interests.

TIA strongly believes that open markets that enable export growth are essential for the continued dynamism of the U.S. telecom sector. For this reason, the Commission must act with deliberation on any measure – such as that contemplated here – that would have the effect of reducing market access by foreign suppliers. It is vitally important for the United States government, or any agency thereof, to explain clearly that any restrictive actions it may take would be based solely on a narrow national security justification and unrelated to broader trading concerns.

This is especially relevant as U.S.-China trade tensions have escalated sharply, with the United States preparing to implement tariffs on a number of Chinese goods,[96] including items used in telecommunications equipment,[97] and potentially imposing restrictions on Chinese

[96] Office of the United States Trade Representative, *Notice of Determination and Request for Public Comment Concerning Proposed Determination of Action Pursuant to Section 301: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation*, 83 Fed. Reg. 14,906 (Apr. 6, 2018), https://www.gpo.gov/fdsys/pkg/FR-2018-04-06/pdf/2018-07119.pdf (includes list of approx. 1,300 products subject to tariffs) ("USTR Section 301 Draft Tariff List").

[97] Telecommunications Industry Association, *[Response to] Request for Public Comment From the Office of the U.S. Trade Representative Concerning Proposed Determination of Action Pursuant to Section 301: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation*, Docket No. USTR-2018-0005, at 2-3 (filed May 11, 2018), https://www.regulations.gov/document?D=USTR-2018-0005-2554 ("TIA May 2018 Section 301 Comments") (listing seven examples of products used in communications equipment that are included on the draft products list, such as capacitors, resistors, diodes, fuses, cable assemblies, hard disk drives and non-magnetic drives, monitoring and testing equipment, and liquid crystal displays).

technology investment.[98] Moreover, given the current scrutiny of Chinese telecommunications suppliers in markets outside the U.S., it is likely that actions undertaken by the Commission could set a precedent in other countries. As described in Section I.B.1 *supra*, questions about possible security concerns involving Huawei have also recently been raised in the United Kingdom, Canada, South Korea, and Australia. It would be particularly beneficial at this point if the Commission led by example, acting in a manner that is clearly and unequivocally grounded upon legitimate national security concerns rather than upon any national industrial policy.

This is important because other nations – China in particular – have issued regulations under the guise of improving cybersecurity that are protectionist and discriminate against U.S. and other non-Chinese suppliers. Chinese President Xi Jinping has voiced wariness of what he describes as foreign control of core technologies[99] and has called openly for China to speed the pace of innovation and accelerate the replacement of foreign goods with "Chinese-made,

[98] President Donald J. Trump, Memorandum on Actions by the United States Related to the Section 301 Investigation of China's Laws, Policies, Practices, or Actions Related to Technology Transfer, Intellectual Property, and Innovation, § 3, 2018 DAILY COMP. PRES. DOC. 180 (Mar. 22, 2018), https://www.gpo.gov/fdsys/pkg/DCPD-201800180/pdf/DCPD-201800180.pdf ("The Secretary of the Treasury … shall propose executive branch action … to address concerns about investment in the United States directed or facilitated by China in industries or technologies deemed important to the United States.").

[99] President Xi Jinping, Speech at the Working Session on Cyber Security and Information Industry (Apr. 19, 2016), http://www.cac.gov.cn/2016-04/25/c_1118731366.htm （一个互联网企业即便规模再大、市值再高，如果核心元器件严重依赖外国，供应链的"命门"掌握在别人手里，那就好比在别人的墙基上砌房子，再大再漂亮也可能经不起风雨，甚至会不堪一击。"Even if an Internet company is great in scale and has a high market value, if the core components rely heavily on foreign countries, the 'Gate of Life' [roughly translated, 'essence'] of the supply chain is held in the hands of others. It is like building a house on someone else's wall. It may not be able to withstand wind and rain, and will be vulnerable.").

indigenous, controllable" technology products into its critical infrastructure.[100] Accordingly, any measures ostensibly designed to address security should be viewed through the prism of China's national industrial policies.

For example, Beijing plans to expand a security ranking system – the Cybersecurity Classified Protection Scheme – from government to commercial markets. For the past decade, Chinese government and state enterprise networks deemed "sensitive" have been required to use only products with Chinese domestic IP.[101] But over the past two years, Beijing has announced that it will extend the ranking system to the commercial insurance industry,[102] civil aviation,[103] and a wide swath of other fast-growing commercial sectors, including cloud computing, mobile internet, the Internet of Things, industrial controls, and big data.[104] The growth of the security

---

[100] President Xi Jinping, Address Before the Communist Party of China's Central Committee (Oct. 9, 2016), http://www.cac.gov.cn/2016-10/09/c_1119682237.htm ("我们要 ... 大力发展核心技术.要 ... 加快推进国产自主可控替代计划" – translation: "We'll … strive to develop core technologies. We'll … accelerate the development of a replacement plan for Chinese-made, indigenous, controllable products.").

[101] PRC Ministry of Public Security, *Information Security Multi-Level Protection Training Manual (Second Edition*), Aug. 2007 (Annex 4, 14 requires "developers and manufacturers of such products in systems [be] invested or owned by Chinese citizens, legal persons or the state, and have independent legal person qualification in China, and the core technology and key components of products have independent Chinese or 'indigenous' intellectual property rights"); *see also* American Chamber of Commerce in the People's Republic of China ("AmCham-China"), *American Business in China: 2010 White Paper*, at 226 (2010), *at* https://www.amchamchina.org/policy-advocacy/white-paper/2010-american-business-in-china-white-paper (explaining that these policies were originally applied to government and state-owned enterprise networks).

[102] China Insurance Regulatory Commission, *Supervision Rules on Insurance Institutions Adopting Digitalized Operations* (draft), Apr. 2016.

[103] Civil Aviation Administration of China (CAAC), *Interim Provisions on Administration of Network Information Security in Civil Aviation*, Feb. 2016.

[104] General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China (AQSIQ), *Information Security Technology - Implementation Guide for Cybersecurity Classified Protection*, Nov. 2016.

ranking system represents the vast expansion of an approach that is premised on excluding foreign ICT equipment from many Chinese information networks.

China has also issued several policies requiring security tests of ICT products that create the potential for IP disclosures. For example, in 2017, Beijing issued draft cybersecurity standards that require suppliers of mobile Internet and IoT services provide access to source code.[105] This followed the release of a proposed procurement ranking system for semiconductors in the fall of 2016; under those rules, companies accrue more security points by providing details about their IP.[106] And a 2017 policy requires that routers, switches and other equipment be tested for compliance with unspecified national standards before they can be approved for commercial sale.[107] Moreover, the labs tasked with testing will be accredited by agencies including the Ministry of Public Security, China's chief law enforcement authority, raising the prospect that proprietary information could be disclosed in ways that are disadvantageous to foreign companies.

China's expanding testing regime has raised significant concerns among U.S. and foreign ICT vendors, given the extent of IP appropriation previously carried out at the direction of the Chinese government. As the USTR recently stated:

> For over a decade, the Chinese government has conducted and supported cyber intrusions into U.S. commercial networks targeting confidential business information held by U.S.

---

[105] People's Republic of China ("PRC"), National Information Security Standardization Technical Committee ("TC260"), *Baseline for Cybersecurity Classified Protection: Special Security Requirements for Mobile Interconnection (Draft); Baseline for Cybersecurity Classified Protection: Special Security Requirements for Internet of Things (Draft)*, Jan. 2017.

[106] TC260, *Security Controllable Level Evaluation Index of Information Technology Products for CPUs*, Oct. 2016. Similar documents apply to application software, such as suites of office products, and to operating systems.

[107] Cyberspace Administration of China, *Catalogue of Network(Cyber)-Critical Equipment and Cybersecurity-Specific Products, Batch 1*, June 2017.

> firms. Through these cyber intrusions, China's government has gained unauthorized access to a wide range of commercially-valuable business information, including trade secrets, technical data, negotiating positions, and sensitive and proprietary internal communications.[108]

TIA has submitted comments to USTR outlining concerns that multiple Chinese policies issued under the guise of security are discriminatory and have a protectionist impact.[109] As a principle, we have consistently advocated against governments advancing unreasonably expansive security policies that would have an inhibiting effect on global trade. Thus, in this proceeding we urge the Commission to communicate that its actions are limited to targeting national security concerns related to a discrete group of suppliers with the goal of maintaining the integrity of the USF program.

D. The Commission Should Refrain from Country-of-Origin Prohibitions.

Both U.S. and foreign communications equipment vendors sell products into the domestic ICT marketplace, and both categories of vendors rely heavily on global supply chains.[110] Indeed, global supply chains that have been built out over decades are critical to the health and competitive standing of the U.S. ICT industry. Thus, any actions by the Commission must account for the critical role of these supply chains in ensuring that the U.S. communications technology market is adequately supplied. The Commission should therefore refrain from broad

---

[108] USTR China Findings, *supra* n.16, at 153.

[109] Statement of K.C. Swanson, Director, Global Policy, TIA, Before the Office of the U.S. Trade Representative Hearing on Investigation under Section 301 of the Trade Act of 1974, Sept. 28, 2017, https://www.tiaonline.org/wp-content/uploads/2018/02/20170928-TIA-Section-301-Comments-to-USTR.pdf.

[110] Government Accountability Office, *GAO-17-688R, State Department Telecommunications: Information on Vendors and Cyber-Threat Nations*, at 4, July 27, 2017 (*see* Figure 1: Possible Manufacturing Locations of Typical Network Components) ("2017 GAO State Department Report"), https://www.gao.gov/assets/690/686197.pdf.

geographic prohibitions and seek to minimize any potential supply chain disruptions to the extent possible. Instead, a constructive approach to considering network security must involve assessing the trustworthiness of *specific suppliers* in countries of concern.

RWA has recently raised concerns that the proposed rule would implement an "ineffective 'country of origin' prohibitory regime."[111] However, TIA does not understand the Commission to be proposing a broad ban on suppliers located in any given nation. Instead, TIA shares Nokia's belief that "the Commission's approach has less to do with country of origin as a basis of risk assessment and more to do with supplier trustworthiness. Therefore, the risk of an overly broad application of the rules is minimal."[112]

However, to avoid creating the impression that the Commission's actions might have more generalized geographic implications, the agency must precisely articulate the scope of its proposal. This is a meaningful commercial consideration, since many leading non-Chinese telecommunication equipment suppliers source components from and maintain production facilities in China, among other countries. Indeed, a recent GAO report concluded that "China [is] the largest importer and exporter of IT hardware globally."[113] Any broader product ban related to geography could have a deleterious effect on these companies, affecting long-established, trusted suppliers of commercial telecommunications infrastructure.

To consider a relevant example, on April 30, 2018, USTR established a draft list of items imported from China on which it proposes to place a 25 percent tariff.[114] The action was

---

[111] RWA Ex Parte, *supra* n.72, at 1.

[112] Letter from Brian Hendricks & Jeffrey Marks, Nokia, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89, at 2 (filed Apr. 9, 2018) ("Nokia Ex Parte").

[113] 2017 GAO State Department Report, *supra* n.110, at 3.

[114] USTR Section 301 Draft Tariff List, *supra* n.96, 83 Fed. Reg. at 14,907.

positioned as a punitive trade remedy after USTR's investigation found that China had engaged in forced technology transfer and other unfair actions,[115] thus subjecting it to enforcement under Section 301 of the Trade Act of 1974.[116] Yet, because many Chinese items are used in advanced technology manufacturing that takes place on U.S. soil, the imposition of duties on Chinese components would in fact have the counter-productive effect of raising costs for U.S. manufacturers of ICT equipment.[117] Though the intent is to punish Chinese firms, the result would be to undermine U.S. competitiveness in leading-edge telecom production.

In short, there is a significant risk that whether motivated by trade or security, any blunt actions by any part of the U.S. government to target broad geographies may have unintended consequences. For that reason, the Commission should avoid a scenario in which a well-intentioned policy might cause substantial collateral damage to global trade without yielding appreciable security benefits. While protecting American networks is of great importance, that objective may be pursued – and in fact, is most effectively pursued – in a manner consistent with a risk-based approach to cybersecurity. To that end, an appropriate strategy would be to focus on particular suppliers and even on particular products within their portfolios – *i.e.*, using a scalpel rather than a hatchet. A path toward such a more targeted and thoughtful approach to specific restrictions is described below.

---

[115] *Id.* at 14,907 ("China uses foreign ownership restrictions, such as joint venture requirements and foreign equity limitations, and various administrative review and licensing processes, to require or pressure technology transfer from U.S. companies.").

[116] Pub. L. No. 93-618, § 301 (1975), 19 U.S.C. § 2411.

[117] TIA May 2018 Section 301 Comments, *supra* n.97, at 2-4 (describing how tariffs on ICT components from China will hurt advanced U.S. technology manufacturing).

E. The Commission Should Carefully Consider Any Potential Restrictions on Components.

The Commission's proposed rule would apply to "equipment or services" from prohibited companies,[118] but the Notice also suggests a components-based approach by asking "which components or services are most prone to supply chain vulnerabilities."[119] TIA agrees that imposing restrictions on certain types of components could materially contribute to advancing the security goals the Commission is pursuing. Security issues related to components have also received recent attention in Congress, although specific legislative proposals remain in flux and could potentially create implementation challenges. The Commission should therefore proceed carefully in this area based upon the principles described below.

1. Restrictions Should Account for Different Types of Components, Be User-Friendly and Consistent Across the Government, and Provide Manufacturers with Implementation Flexibility.

As the Commission considers security challenges related to components from suppliers of concern, it should keep several important principles in mind:

- *Differentiation.* Different types of components have different impacts on security. The potential security impact of a network interface card or a CPU is quite different from that of a plastic housing or a screw, or even from that of low-level electronic components like capacitors, resistors, or op-amps.

- *Clear application.* Any restriction that differentiates between types of components should be both carefully designed and easy to understand and apply. Importantly, the definition should be easily understandable by engineers and contracting officers without requiring significant consultation of attorneys or extensive implementation guidance from the Commission.

- *Consistency.* Restrictions should be consistent across the government to the greatest extent possible. Inconsistent definitions across agencies – or from an approach adopted by Congress – about which components are covered would create a compliance nightmare.

[118] Notice, App. A (proposing to add 47 C.F.R. § 54.9).

[119] *Id.* ¶ 15.

- *Administrative flexibility in implementation.* Each manufacturer must be given flexibility to determine how it will implement any restrictions. As described below, some manufacturers will benefit from the flexibility offered by a targeted restriction on logic-enabled components, while others will elect to adopt a zero-percent approach to any components from a prohibited supplier.

Recognition of and adherence to these facts and principles from the outset will help avoid a scattershot approach that raises costs unnecessarily without producing meaningful security benefits.

Differentiation. Banning every component from a prohibited supplier would not advance any material security purpose. For example, restrictions on components such as glass or plastic, or even low-level and low-cost electronics like resistors or capacitors, would not have any effect on the ability of a malicious actor to remotely intercept or disrupt communications by virtue of such components being included in any piece of network equipment. Ultimately, the intent of the prohibition is to ensure security, not to punish particular companies. A complete restriction would be overbroad with potentially negative repercussions for U.S. industry overseas, and may also be inconsistent with emerging approaches under consideration in Congress.

To be sure, manufacturers would likely not deliberately choose to source *any* components from a supplier prohibited by the Commission. However, some manufacturers – especially smaller or startup ICT companies, but also larger companies – may buy off-the-shelf components like screws or plastic connectors without establishing any meaningful contractual relationship with the upstream supplier. In these circumstances, it would be very difficult to guarantee that no upstream supplier used any part from a prohibited company, no matter how minor. Efforts to provide such guarantees would be very costly at a minimum and could disrupt innovation, and in some cases obtaining such guarantees may be nearly impossible.

Clear application. Constructing a workable definition that appropriately targets "smart" components may be more challenging than it appears, as some recent attempts suggest. For example, the initial version of the House FY19 National Defense Authorization Act proposed a lengthy definition for "intelligent components" with six sub-clauses, including "any component or device that performs a communication function."[120] That clause could have easily encompassed fiber-optic or copper cabling and physical antennas, *i.e.*, components through which data undoubtedly travels, but which do not reasonably pose a security threat. A more recent version contains a somewhat improved but difficult-to-parse definition, with intelligent components being those that could "route or redirect data traffic or visibility into any data or packets that [certain covered] equipment, system, or service transmits or manipulates,"[121] and some reliance upon cross-references to other definitions.

These well-meaning attempts highlight two issues. *First*, the definition must take care to exclude low-level electrical and electronic components that pose no meaningful threat. A definition focused on "integrated circuits" or "semiconductors" might inadvertently capture analog components such as op-amps, the output (power) stage of a transmitting radio, or a power supply regulator, none of which pose a meaningful threat of enabling remote interception or disruption. *Second*, to be of any practical use, the definition must be reasonably clear and easily understandable by engineers in the field – including those working at small manufacturers

[120] House Armed Services Committee, FY19 National Defense Authorization Bill, Chairman's Mark, § 866(b)(4)(E)(v), May 2018, *available at* https://docs.house.gov/meetings/AS/AS00/20180509/108275/BILLS-115HR5515ih.pdf

[121] H.R. 5515, *supra* n.36, § 880(b)(5)(E)(iii). The definition is actually part of a carve-out for *non*-intelligent components – those that "*cannot* route or redirect data traffic," etc. – with intelligent components being defined by negative implication.

seeking to buy off-the-shelf components – without resort to lawyers or extensive consultation of Commission guidance documents.

Consistency. Applying multiple definitions of what constitutes an intelligent component could create a serious administrative challenge for any company – or any engineer or purchasing official at a small startup manufacturer – that is trying to comply with different requirements. Lawyers may be needed to identify which restrictions apply in which purchasing contexts, *e.g.*, different component restrictions for USF customers vs. other federal customers. While it may be possible in some circumstances to construct a "most-restrictive" definition that combines elements from Congress or various agencies, this would be a massive administrative burden that would hurt innovation. Nevertheless, the Commission may be well-positioned through this proceeding to establish a definition that could be relied upon by other agencies and potentially by Congress itself.

Administrative flexibility in implementation. Some large manufacturers likely do much or all of their sourcing via contracts that facilitate sophisticated tracking of upstream suppliers. These manufacturers may find it easier to simply certify that their supply chains contain *no* components from a prohibited supplier, rather than logic-enabled components. Electing such a voluntary blanket "zero-percent content" option would potentially avoid the need for the manufacturer to educate its upstream suppliers regarding any technical definition the Commission may adopt regarding logic-enabled components, particularly if the definition is complex. This "zero-percent content" requirement would likely be enforced via contractual requirements with every upstream supplier in a manufacturer's supply chain. Any rules adopted should therefore allow for this possibility.

2. Restrictions Should Focus on Logic-Enabled Components and Products.

Although the Commission must continue to closely monitor developments on components-related issues throughout the government, as the first agency to consider these issues in an open proceeding, the Commission may be well-situated to advance the dialogue. To that end, TIA proposes in the Appendix a rule that is consistent with the principles above. At the outset, we recognize that these are challenging issues, and our proposal is therefore provisional. We look forward to engaging with the Commission and reviewing any proposals from other commenters on this issue.

Definition. TIA's proposed restriction would focus on *logic-enabled components*, which would be "those components containing or implementing logical functions and that are capable of generating or modifying the information content of digital data." In turn, any "equipment" that contains such components would be prohibited, while end products that do not contain any such components would be unaffected. Additionally, it may be helpful to provide examples in the rule text: "this includes network controller chips, CPUs, and functional circuit boards such as network or graphics cards, but does not include analog circuits or components such as op-amps, power supply regulators, cabling or antennas unless those components themselves contain a covered component."

Regardless, the Commission should avoid qualitative definitions of targeted components that would be difficult to apply. For example, the Notice considers the possibility of limiting restrictions on *equipment* or *systems* "the compromise or failure of which could disrupt the confidentiality, availability, or integrity of a network,"[122] while leading proposals in Congress would target entities that use prohibited equipment or services "as a substantial or essential

[122] Notice ¶ 15.

component of any system, or as critical technology as part of any system." Such consequences-based or value-judgment restrictions, while appealing in theory, would be much more challenging when applied to *components*. They could require smaller manufacturers – and their upstream suppliers – to conduct costly and wholly unnecessary risk-based assessments for every off-the-shelf screw or plastic connector.

End products. The Commission need not prohibit USF funding from being used on "*any* equipment" from a covered company.[123] Similar to components, some end products pose little or no security risk on their own account, including fiber optic cables, physical antennas, or device enclosures. Thus, if the Commission decides to place restrictions on components, then the current proposed rule for end products may be unnecessarily overbroad, especially given that the Commission's actions will be scrutinized as a global precedent and could result in reciprocal prohibitions on U.S. manufacturers. Therefore, the limits on hardware end products should be explicitly tied to whether those products contain a logic-enabled component.

Zero-percent option. The Commission should provide manufacturers with flexibility by creating a "zero-percent content" option for any party providing an attestation under the rule. (*See* Section IV.D *infra*.) Parties may either (1) attest to non-reliance upon any covered components, or (2) attest to non-reliance upon *any* components from a covered company. Including the zero-percent reliance option in the rule would potentially help forestall legal challenges or lawsuits from covered companies who believe that their non-intelligent components have been unduly caught up alongside prohibitions of logic-enabled components.

Software. TIA recognizes that issues regarding software prohibitions may present a different set of challenges than hardware, and we look forward to reviewing any proposals from

[123] *Id.* App. A (proposing to add 47 C.F.R. § 54.9).

other commenters on this issue. In some regards, software poses a more difficult-to-manage threat than hardware, as it is difficult to say with certainty that any piece of software would not pose a security vulnerability. For example, Kaspersky Lab produces anti-virus software that has been alleged to permit cyberespionage, quite remote from its advertised function. And unlike hardware, software updates are difficult to trace while hardware parts lists can more easily be traced through the supply chain. Pending review of proposals from other commenters, TIA's preliminary conclusion is that given the Commission's focus on Kaspersky Lab in the Notice, software could also be addressed as part of a restriction on components. Any software or firmware from any prohibited supplier could simply be deemed to be a "logic-enabled component."

F. Restrictions on Services Should Be Narrowly Tailored.

The Commission should consider tailoring the scope of covered services to avoid inadvertent problems related to decommissioning or end-of-life support that USF recipients may potentially need to obtain from prohibited companies. A broad prohibition on services could also potentially create problems in scenarios whereby non-prohibited ICT companies may need to temporarily operate prohibited equipment during a transition period. It could also affect participation in various types of innocuous, shared-services agreements for supported services with a covered company, perhaps in a foreign country or as part of an international body. The prohibition could be narrowed, for example, to actual communications services, *i.e.*, telecommunications services or information services, but TIA looks forward to reviewing submissions from other commenters regarding the implications of prohibitions on services.

IV. THE COMMISSION SHOULD PUBLISH A LIST OF PROHIBITED SUPPLIERS.

For the time being, the Commission should maintain and publish its own list of prohibited suppliers. This could be done through the issuance of occasional public notices and/or through a list maintained on the Commission's website. However, the Commission's list should explicitly derive from determinations made by agencies with appropriate national security expertise, or by Congress. As described below, this approach would recognize that the Commission does not have appropriate expertise to make supplier-specific national security determinations on its own, and that such independent determinations could result in an inconsistent patchwork of restrictions by different agencies across the government.

Regardless, the Commission should avoid hard-coding the names of any specific companies or products into the Code of Federal Regulations. And as part of ensuring compliance with its rules, the Commission may require that operators or suppliers provide an attestation that they do not use any equipment or services from the prohibited companies in their own products or services. In the future, these implementation details could potentially change if Congress or the President establishes a systemic whole-of-government approach to identification of prohibited suppliers, including designation of a lead agency and/or creation of an interagency process. (*See* Section VI below.) But for now – and as the Commission itself recognizes – its present task is to identify, apply, and ultimately translate a disparate set of national security assessments sometimes made in other contexts into a workable set of procedures and a list of prohibited suppliers.[124]

[124] *See id.* ¶¶ 19-25.

A. The Commission's List of Prohibited Suppliers Should Derive from Determinations Made by Expert Security Agencies or Statutory Requirements from Congress.

In identifying which actions by other federal entities should trigger the inclusion of a covered company, the Commission should select criteria that permit the Commission and interested parties to easily determine which companies are affected, while avoiding being unnecessarily overbroad. The Commission should also consider not only short-term circumstances, but the eventual establishment of a long-term whole-of-government approach. With those principles in mind, TIA proposes that the following companies should be covered by the Commission's rule:

- Any company that is prohibited by name in any federal statute from selling one or more covered communications technology products to one or more civilian federal agencies for national security reasons;

- Any company that is prohibited by name in any publicly-released finding, directive, order, or similar action issued by the President, the Department of Homeland Security, or any other federal national security agency from selling one or more covered communications technology products to one or more civilian federal agencies for national security reasons;

- Any company that is prohibited by name as the result of a federal interagency review process established either by statute or by executive order from selling one or more covered communications technology products to one or more civilian federal agencies for national security reasons; or

- Any company that is a subsidiary, affiliate, or successor-in-interest of any company mentioned above.

Explanations for the use of particular terms or concepts in the proposal above are provided below. The text above is also incorporated in TIA's proposed rule text (*see* Appendix).

Prohibited by name. The process of identifying covered companies should be made as simple as possible for the Commission and for its stakeholders. Under one of the Notice's

proposed approaches,[125] complex logical inferences could potentially be required to determine whether a particular supplier has been effectively prohibited by operation of a particular statute. Requiring that a company be prohibited by name greatly simplifies the Commission's task. There is also little risk of under-inclusion, considering that all three companies mentioned in the Notice have already been specifically named by Congress and/or by specific agency actions, as described above.

Civilian federal agencies. The Department of Defense often imposes a higher bar for procurement of certain products.[126] Companies should not be prohibited solely because they have been unable to meet the threshold for procurement by DoD.

National security reasons. To prevent inadvertent inclusion of companies who may be prohibited from selling to particular agencies for commercial or other reasons, the national security condition should be explicitly specified. On occasion, congressional statutes naming particular companies may not explicitly identify the reason for naming a particular company.[127] However, other tools of statutory interpretation – context, findings, or legislative history – would typically supply the necessary justification without the need for careful discernment of congressional intent by the Commission.

Publicly-released. Some executive branch agencies may elect to impose confidential restrictions on particular suppliers for their own reasons. However, such confidential restrictions are unworkable here given that the participation of USF recipients and private-sector entities will be required to implement the prohibitions.

---

[125] *See id.* ¶ 20.

[126] *See, e.g.*, Defense Federal Acquisition Regulation Supplement: Requirements Relating to Supply Chain Risk (DFARS Case 2012-D050), 80 Fed. Reg. 67,244 (Oct. 30, 2015).

[127] *See, e.g.*, FY18 NDAA, *supra* n.33, at § 1656(c)(3)(a), 131 Stat. at 1762.

Action by President, DHS, or other federal national security agency. To avoid an inconsistent patchwork of regulation and ensure that national security determinations are being made appropriately, any executive branch trigger should be limited to determinations made by the President or by agencies with appropriate national security expertise. For example, a unilateral decision by the U.S. Department of Education to ban all products from a particular supplier should not immediately become binding across the federal government or on USF recipients.

Interagency review process. The Commission should adopt a forward-looking approach – and avoid the need for a future rulemaking – by anticipating the establishment of a future interagency process that is empowered to make national security determinations on behalf of the entire (non-military) federal government. We describe such a process in Section VI.B *infra*.

Subsidiary, affiliate, or successor-in-interest. In the Notice, the Commission asks whether it should prohibit subsidiaries, parents, and/or affiliates of prohibited companies, and if so, how those terms might be defined.[128] TIA supports a rule that would extend prohibitions to subsidiaries (51%), affiliates (25% or 10%), or successors-in-interest of prohibited companies.[129] Importantly, while TIA does not understand the Commission to be proposing a country-of-origin prohibition, care should be taken to avoid inadvertently impacting joint ventures.

Effect on companies named in the Notice. As described in Section I.C.2 *supra*, all three companies named in the Notice would be covered by the proposed rule above. Huawei and ZTE have been prohibited by Congress from selling products to one or more civilian agencies,[130] and

[128] Notice ¶ 25.

[129] *See id.*

[130] *See* FY18 NDAA, *supra* n.33, at § 1656(b)(1), 131 Stat. at 1762.

Kaspersky Lab has been prohibited by a DHS Binding Operational Directive from selling to any federal agencies.[131]

Indefinite duration. Assuming the Commission adopts the approach above, it may safely assume that companies should remain on the list "indefinitely until the relevant agency or Congress has affirmatively reversed course," without the need for a three-year expiration period.[132] While inclusion on the list by virtue of congressional or executive agency action will likely result in some attempts by companies to reverse those designations, a scheduled sunset period imposed by the Commission will almost certainly produce that result. This would likely draw the Commission into making substantive national security determinations that the agency is not well-suited to make, as explained below.

B. The Commission Should Not Make Its Own National Security Determinations.

TIA does not understand the Commission to be proposing that the agency would make its own national security determinations regarding any particular supplier. As described in Section II.B above, doing so would be inconsistent with precedent and would remove an important limiting principle on the Commission's legal authority in national security matters. Nevertheless, since the Commission has inquired about "alternatives" – including citing proposals that would potentially have the agency make such determinations directly – we provide additional reasons below why the Commission should refrain from doing so.[133]

[131] Binding Operational Directive BOD-17-01, *supra* n.38.

[132] Notice ¶ 20.

[133] *See id.* ¶ 20 & n.37.

1. The Commission is Not Well Positioned to Perform National Security Evaluations of Particular Suppliers.

As the Commission has implicitly recognized, it is not well-suited to make independent assessments regarding national security. Assessing whether products from a particular ICT supplier pose a heightened risk can sometimes involve complex technical assessments, as clearly demonstrated by the computer engineering analysis contained in the April 2018 joint alert regarding the targeting of network infrastructure by Russian state-sponsored cyber actors.[134] Organizations such as US-CERT at the Department of Homeland Security, or various intelligence agencies, are much better positioned to make such determinations.

Even when evaluating non-technical factors such as the legal environment in a particular foreign country or a particular vendor's corporate governance structure, national security assessments should still be made by intelligence officials equipped to consider evidence in the appropriate geopolitical context. This is consistent with longstanding practice: as far back as 1941, the Commission resisted efforts in Congress to give the agency legal authority to police subversive activities, "largely on the ground that the Commission was unprepared to make investigations into [such] activities, and did not wish to undertake them."[135] A judge's later commentary on that situation applies equally here: "[n]othing appears which would suggest that the Commission is equipped today to pass upon such matters."[136] Thus, for both practical

---

[134] US-CERT April 2018 Alert, *supra* n.17.

[135] *Borrow v. FCC*, 285 F.2d 666, 671 (D.C. Cir. 1960) (Washington, C.J., dissenting). In this case, a D.C. Circuit panel majority upheld a Commission regulation prohibiting the grant of radio licenses to any self-identified member of the Communist Party. The core holding would likely be invalid today, and the majority opinion reads as a product of its times, while the dissent's logic seems more durable.

[136] *Id.*

reasons as well as the need for limiting legal principles discussed in Section II.B *supra*, the Commission should rely on determinations made by Congress or by expert agencies.

2. Independent Determinations by the Commission Would Set a Precedent that Could Lead to a Patchwork of Different Lists and Restrictions Imposed by Various Regulators.

As the first independent regulatory agency – perhaps even the first non-security agency – to consider these issues, the Commission is plowing new ground. Its actions will likely shape the steps that other agencies across the federal government will take, as well as future actions by state and local governments, the private sector, and foreign governments. The Commission therefore has an important responsibility to ensure that national security determinations regarding particular suppliers will not be made in a patchwork manner across the federal government.

As discussed in greater detail in Section VI.B *infra*, deferring to determinations made by Congress, the President, or national security agencies will promote substantively and procedurally sound decision-making that avoids inconsistent results across agencies. Moreover, Congress can eventually move beyond targeting specific companies by name in legislation once a robust interagency process has been established. In contrast, allowing different agencies to deliver mixed messages regarding the viability of using equipment from a particular supplier on national security grounds could be highly damaging to consumer confidence, to the government, and to the standing of other ICT companies in the global marketplace.

C. The Commission Should Not Insert Company Names into the Code of Federal Regulations.

The Commission is currently focused on a small number of specific companies, and it would be appropriate to name them in public notices and on the Commission's website. However, any approach based on naming those companies in the rule text itself would limit the

Commission's ability to respond rapidly and flexibly to future changes in the marketplace, including potential attempts at deliberate circumvention. For example, the Commission should not need to go through a notice-and-comment rulemaking every time another problematic situation arises. While providing some amount of due process for a targeted company is important, that process need not consist of a notice-and-comment rulemaking at the Commission. Assuming that the Commission bases its designations solely upon actions or processes by other agencies with appropriate expertise (or by Congress) as recommended above, then aggrieved parties can seek relief through those channels.

To be sure, Congress has recently chosen to name specific companies in legislation, but it has limited itself to annual appropriations bills and situations related directly to federal procurement.[137] However, these bills have not yet been tested in court and could potentially be the subject of a legal challenge, especially if ever expanded beyond the limited government procurement context.[138] Regardless of congressional action, any action by a regulatory agency to restrict a single company by name in a rule is an extremely rare practice in the modern regulatory

[137] *See, e.g.*, CJS Appropriations Act 2013, *supra* n.31, at § 516(b), 127 Stat. at 274 (procurement by the Departments of Commerce and Justice, NASA, and the National Science Foundation from companies connected to China); FY18 NDAA, *supra* n.33, at § 1634, 131 Stat. at 1739 (federal procurement from Kaspersky Lab); *id.* at § 1656, 131 Stat. at 1762 (Department of Defense procurement from Huawei or ZTE).

[138] Indeed, such legislation evokes analogous (even if inapplicable) bill-of-attainder concerns, especially if any non-security rationales are involved and perceived to be punitive in nature. *See generally* Kenneth R. Thomas, *Bills of Attainder: The Constitutional Implications of Congress Legislating Narrowly*, CONGRESSIONAL RESEARCH SERVICE, Aug. 26, 2014, https://fas.org/sgp/crs/misc/R40826.pdf.

era except for possible situations regarding certain monopolies. The Commission should not go down this path.[139]

D. The Commission Should Establish an Attestation System to Ensure Compliance.

In the Notice, the Commission seeks comment regarding how it should enforce its proposed rule.[140] Once the Commission publishes a list of prohibited suppliers as described above, it should require recipients of universal service support to provide an attestation that they have not spent any funds on covered products or services from any covered company. The attestation could be required as a condition of applying for and receiving universal service support, or upon request by USAC.

Manufacturer role. Assuming the Commission imposes restrictions on logic-enabled components in addition to end products (*see* Section III.F *supra*), manufacturers who sell into the USF marketplace will likely have an important role to play in ensuring compliance. USF recipients should in turn be able to rely upon attestations they have obtained from their suppliers. Suppliers would be able to rely upon attestations from their upstream suppliers, and so on. Particularly for large manufacturers, such attestations would likely evolve into contract conditions, with each supplier responsible for recursively providing assurance regarding its upstream suppliers.

Product groups. To the extent that manufacturer attestations are required as to components, manufacturers should have the option of attesting to the non-reliance of a single

[139] Recent events demonstrate that attempts by Congress to name specific companies in statutes can be highly visible in the press – sometimes intentionally – with greater visibility to foreign governments and potentially to their citizens. These actions could therefore provoke greater retaliation against U.S. companies and companies from allied nations, and potentially interfere with U.S. trade policy determinations that should be made separately from the security context.

[140] Notice ¶ 26.

product upon prohibited products or services, or of multiple products, or even of all products supplied by that manufacturer. Such flexibility would likely promote efficiency for a manufacturer that ensures compliance across its entire product line, and may avoid the need for repeated interactions between operator and vendor for each different subclass of product.

White labeling. In the Notice, the Commission asks how it should treat "white labeling," in which "a covered company may provide equipment or services to a third-party entity for sale under that third party's brand."[141] To address such cases, the rules should prohibit attestation of white-labeled products. Instead, attestation must be obtained by the original manufacturer. In practice, the white-label vendor would likely assist the customer in obtaining such attestation.

Zero-percent option. As noted in Section III.E.2 *supra*, some suppliers may prefer to attest to zero percent content from a covered company, rather than only logic-enabled components. To account for this, the rules should explicitly provide an option for any entity providing an attestation to use the zero percent option. Although some manufacturers might choose for zero percent attestation anyway, formally establishing a zero percent option in the rules could provide those suppliers with a defense against potential lawsuits from covered companies who believe their non-logic-enabled products have been inappropriately caught up alongside a ban of their covered products.

V. THE BENEFITS OF COMMISSION ACTION WILL OUTWEIGH THE COSTS IF APPROPRIATELY TAILORED.

The benefits will significantly outweigh the costs if the Commission's actions in this proceeding are appropriately tailored and implemented as recommended in these comments. In the universal service context, the Commission has long been cognizant of the importance of

[141] *Id.* ¶ 25.

balancing the costs and benefits of its policy choices.[142] Congress declared in 1996 that the definition of universal service would consistently evolve along with technology advances in the communications marketplace. Indeed, the Commission is required to "take into account advances in telecommunications and information technologies and services" as it balances the costs and benefits of difficult policy choices necessary to achieve universal service objectives.[143]

There is a persistent yet unavoidable tension between the advantages and disadvantages of any decision the Commission might make with respect to universal service. Indeed, the Commission must routinely assess the benefits of increased total spending against the costs of contributions from ratepayers, evaluate the extent of regulatory burdens on USF recipients, and decide on the relative support levels provided to individual USF programs. For example, while there would be clear benefits from connecting every home in America with a 1 Gbps broadband connection, the Commission has determined that the cost of doing so and the impact on ratepayers outweigh the potential benefit of subsidizing that level of connectivity. In that example, there are tradeoffs that can be made – the Commission can subsidize connectivity to ensure all Americans have access to broadband, but at lower supported speeds that still meet basic universal service objectives without an exorbitant price tag.

If the Commission's proposal here is adopted, ensuring that USF funds do not undermine national security would become an additional factor for the agency to consider. Consistent with that approach, the Notice prudently observes that any action taken will likely carry its own

---

[142] *See, e.g.*, *Universal Service Contribution Methodology*, Further Notice of Proposed Rulemaking, 27 FCC Rcd 5357, 5489 ¶ 387 (2012); *Modernizing the E-rate Program for Schools and Libraries*, Second Report and Order and Order on Reconsideration, 29 FCC Rcd 15538, 15586 ¶ 117 (2014); *Promoting Telehealth in Rural America*, Notice of Proposed Rulemaking and Order, 32 FCC Rcd 10631, 10639 ¶ 16 (2017).

[143] 47 U.S.C § 254 (c).

benefits as well as countervailing costs, and it seeks comment on both sides of that equation.[144] To be sure, the Commission should candidly acknowledge that prohibiting a specific supplier from participating in any segment of the U.S. communications technology market is an extraordinary regulatory action that potentially bears *some* costs. Moreover, while the Commission rightly asks about potential costs to "USF recipients, the Fund, end users, consumers, the public safety and law enforcement community, the Commission, or other Federal agencies,"[145] there could also be some costs to innovation and certainly to the rest of the ICT industry if the Commission's actions are not narrowly tailored.

When it comes to national security, there is less room – and perhaps no room – for trade-offs. If the Commission is presented with hard facts from its national security partners that there are well-documented national security risks associated with a particular technology or company, there may be no alternatives available other than prohibiting the use of USF dollars to support the further deployment of such technology.[146] The analysis then turns to whether there are competing policy objectives, such as the availability of universal broadband connectivity in every community, that could not be achieved if eligible USF recipients were unable to use products from suppliers deemed to pose a national security risk.

If the only way that millions of Americans could be connected to broadband was through products from suppliers that pose a national security risk, then the Commission would be faced with an extremely difficult choice. Fortunately, that is not the case, as described below. Moreover, there are affirmative benefits to addressing security concerns, including promoting

[144] *See generally* Notice ¶¶ 33-35.

[145] *Id.* ¶ 33.

[146] For example, as explained in Section III.B *supra*, product testing is not a viable alternative.

confidence in the global ICT marketplace and potentially reducing the costs of security breaches. Therefore, the dual benefits of securing USF-supported networks and ensuring robust connectivity in rural communities and within the nation's schools, libraries and healthcare clinics can both be achieved.

A. Addressing Security Concerns Will Improve Confidence in the Global ICT Marketplace.

Cyberespionage is a serious and growing problem. In addition to state-sponsored espionage, hidden back doors can allow other bad actors to steal intellectual property from American entrepreneurs and innovators or even worse to use such access to launch targeted cyberattacks targeting critical infrastructure. A report released earlier this year by the White House Council of Economic Advisors titled "The Cost of Malicious Cyber Activity to the U.S. Economy" summarized the costs well:

> Malicious cyber activity directed at private and public entities manifests as denial of service attacks, data and property destruction, business disruption (sometimes for the purpose of collecting ransoms) and theft of proprietary data, intellectual property, and sensitive financial and strategic information. Damages from cyberattacks and cyber theft may spill over from the initial target to economically linked firms, thereby magnifying the damage to the economy."[147]

It is commonly acknowledged that state-sponsored actors conducting malicious cyber activity are very technically skilled. Nation-states engage in the theft of IP and sensitive financial information, but they are also capable of engaging in the offensive destruction of data relied upon by businesses and governments. These risks are growing, and if they are not sufficiently addressed then consumers and businesses will be reluctant to use broadband networks for

[147] Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy*, Feb. 2018, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf ("*CEA Economic Impact Report*").

important activities, which is precisely the opposite of the Commission's universal service objectives.

Addressing concerns regarding particular suppliers, if handled in a transparent way, should promote global confidence in ICT vendors in an era of rising threats. The concerns related to the specific companies described in the Notice relate in part to the legal environments in their home countries and/or opacity regarding their corporate governance structures and independence from their governments. If the United States puts companies on notice that their actions have consequences, then those companies and others will be properly incentivized to change behaviors. While access to USF support is a small factor in a broader global discussion about how to address cybersecurity issues, restricting access to the multi-billion-dollar USF market is an important step that can set an example for other federal agencies and international players. Further, if a transparent path is provided for companies of concern to regain access to the marketplace, this could potentially spur positive changes in the domestic legal environments or governance structures of those companies, improving outcomes for everyone.

B. Promoting Secure Communications Will Provide Significant Public Interest and Economic Benefits to U.S. Consumers, Businesses, and Community Anchor Institutions that Utilize USF-Supported Networks and Services.

Any action to ensure the security of communications networks and services – provided that it is taken along the lines described above – will undoubtedly yield a range of significant public interest benefits for all stakeholders, some of which may even be quantifiable. Benefits would include the following:

Promoting quality and equality of service. Actions to promote national security in the USF context would further the principles of both *quality* and *equality*. As explained in the Notice, "one of the Commission's central missions" under Section 1 is to "make 'available … to

all the people of the United States … a rapid, efficient, Nation-wide, and world-wide wire and communication service with adequate facilities at reasonable charges.'"[148] Meanwhile, Section 254(b)(1) requires that policies regarding the preservation and advancement of universal service be based on the principle that "[q]uality services should be available at just, reasonable, and affordable rates"[149] and Section 254(b)(3) requires that consumers in rural areas should have access to communications services that are "reasonably comparable to those services provided in urban areas."[150]

In these very specific circumstances, the Commission may reasonably conclude that limiting the use of technology from certain vendors deemed to pose a heightened national security risk is an appropriate element of providing a *quality* communications service. As noted above, the U.S. government has highlighted the need to improve cybersecurity and to better defend commercial communications networks against state-sponsored malicious cyber actors. Meanwhile, the two largest national wireless carriers have recently abandoned their use of equipment from certain vendors.[151] Thus, restrictions on USF funding would further the principle that individuals and business benefitting from subsidies in rural areas should have access to services that are "reasonably comparable" to services in urban areas, *i.e.* having the

[148] Notice ¶ 10 (quoting Communications Act of 1934 § 1 [47 U.S.C. § 151]).

[149] 47 U.S.C. § 254(b)(1).

[150] *Id.* § 254(b)(3).

[151] Stu Woo & Betsy Morris, *AT&T Backs Off Deal to Sell Smartphones from China's Huawei*, WALL ST. J., Jan. 8, 2018, https://www.wsj.com/articles/at-t-backs-off-deal-to-sell-smartphones-from-chinas-huawei-1515443153; Scott Moritz, Mark Gurman & Todd Shields, *Verizon Drops Plan to Sell Phones From China's Huawei, Sources Say*, BLOOMBERG, Jan. 29, 2018, https://www.bloomberg.com/news/articles/2018-01-30/verizon-is-said-to-drop-plans-to-sell-phones-from-china-s-huawei.

option of obtaining service from unsubsidized major national providers that do not use such equipment.

Reducing costs of breaches and protection. Enhanced security via the ecosystem-wide elimination of known threats would go far toward sparing U.S. businesses the economic costs associated with breaches and online distributed threats. It would also likely mitigate the costs that U.S. businesses must incur on an individual basis for routine security protection. In the present context, those cost savings may be most pertinent to community anchor institutions and others that utilize USF-supported networks and services, but they would inevitably flow to all other consumers, businesses, and government and public entities with which they are interconnected. Indeed, a White House Report estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.[152] Even if restricting support to cyber threats via USF spending is a limited act, it will help reduce the mounting costs associated with malicious cyber intrusions.

Consumer confidence. Equally important are the intangible benefits of enhanced security. Individual consumers may be reluctant to use certain commercial networks – either completely or just for certain purposes they deem individually sensitive such as banking and e-commerce – if the perception exists that certain service providers have been compromised through the use of certain equipment. Rightly or wrongly, this perception could ultimately harm broadband deployment, consumer adoption, and/or drive some rural consumers to incur additional costs to combat perceived weaknesses in the security of their ISP.

[152] CEA Economic Impact Report at 1.

For that reason, various government and industry stakeholders – including the Commission itself[153] – have long recognized that improving security preserves confidence among consumers and the private sector generally, which in turn promotes adoption of and innovation with advanced services.[154] Indeed, that concept underlies the recent report from the Secretaries of Commerce and Homeland Security regarding enhanced resilience against botnets and other automated, distributed threats.[155] The inextricable connection between enhancing security and preserving consumer confidence is a key driver behind the efforts of TIA members and others to ensure that their own security practices are up-to-date and adequate.

Ultimately, by taking specific action in this proceeding to address security concerns, the Commission will further the principles of ensuring quality and reasonably comparable service to all Americans, improving the security of some of the nation's most vulnerable networks such as

---

[153] *See, e.g., Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*, 2015 Broadband Progress Report and Notice of Inquiry on Immediate Action to Accelerate Deployment, 30 FCC Rcd 1375, 1438 ¶ 104 (2015) (noting correlation between non-adoption of broadband and security and privacy concerns); Julius Genachowski, Chairman, FCC, Prepared Remarks on Cybersecurity, Meeting of CSRIC, Washington, D.C., Mar. 22, 2012, at 2 ("Privacy and security are complementary – both are essential to consumer confidence in the Internet and to adoption of broadband."), https://docs.fcc.gov/public/attachments/DOC-313161A1.pdf.

[154] *See, e.g.*, RSA, 2017 Consumer Cybersecurity Confidence Index, https://www.rsa.com/content/dam/pdfs/5-2017/rsa-consumerconfidenceindex-ebook.pdf; Department of Commerce, Cybersecurity, Innovation and the Internet Economy, 75 Fed. Reg. 44,216 (2010); Federal Trade Commission, *Internet of things, Privacy & Security in a Connected World (FTC Staff Report)*, Jan. 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (noting how industry stakeholders have expressed concern to FTC staff that "perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption").

[155] *See generally* Botnet Report, *supra* n.80.

those in under-resourced hospitals and schools, and buttressing the consumer confidence needed to promote robust broadband adoption.

C. USF Recipients Will Continue to Benefit from a Competitive Marketplace for Equipment that Includes a Number of Trusted Suppliers.

To the extent there is concern about the proposed rule disrupting the marketplace in a way that would increase equipment and service costs, TIA is confident that USF recipients will continue to benefit from a competitive marketplace for equipment that includes a number of trusted suppliers. TIA has a unique insight into this issue.

Suppliers of concern. While Huawei and to a lesser extent ZTE have a significant market share in the global economy,[156] Huawei products reportedly make up *less than one percent* of the equipment in American cellular and landline networks today.[157] Of course, it is unclear how much USF support is used to purchase equipment from any of the companies identified in the Notice, or how many USF recipients rely on equipment from such vendors. TIA is unaware of a source to determine those figures. With that said, the level of spending is assuredly very low in comparison to the total level of USF spending. Still, for small companies who have invested in

---

[156] *See, e.g.*, Teresa Mastrangelo, *Global Market Share Report: DSL Port Shipments – 2017 & 4Q 2017*, BroadbandTrends, Feb. 18, 2018, at 5 (showing Huawei and ZTE having a combined 48% of global DSL port shipments), https://docs.wixstatic.com/ugd/d2dfa1_2ee8c67d883a48aebae238739b90c7e0.pdf; *but see* BroadbandTrends, *2015 & 4Q15 Market Share Report Summary-DSL*, Mar. 17, 2016, at 2 (showing that the top DSL vendors in the North American market were Nokia, ADTRAN, and Calix, even as Huawei and/or ZTE were among the top three vendors in the rest of the world), https://broadbandtrends.files.wordpress.com/2016/03/bbt_2015dslmktshare_161010_toc.pdf.

[157] Drew FitzGerald & Stu Woo, *In U.S. Brawl with Huawei, an Unlikely Loser: Rural Cable Firms*, WALL ST. J., Mar. 27, 2018, https://www.wsj.com/articles/caught-between-two-superpowers-the-small-town-cable-guy-1522152000 (referencing information from research firm Dell'Oro Group); *see also* U.S. House of Representatives Committee on Energy and Commerce Majority Staff, Memorandum on Hearing entitled "Telecommunications, Global Competitiveness, and National Security," May 14, 2018, at 2 & n.7 https://docs.house.gov/meetings/IF/IF16/20180516/108301/HHRG-115-IF16-20180516-SD002-U2.pdf (citing the *Wall Street Journal* article).

Huawei or ZTE equipment or seek to do so in the future to meet their universal service deployment obligations, there is a cost if such equipment is no longer available for purchase. The question is whether the benefits of restricting access to such equipment is outweighed by the benefits, and the answer is clearly yes given the alternatives in the market that can achieve all of the capabilities of the potentially restricted equipment.

Based on the robust capabilities of many companies within TIA's membership alone, we are confident that no current recipient of USF support in any of the Commission's universal service programs would be stuck without multiple options to deploy the networks and services they have committed to providing as a recipient of USF. In all four USF programs, available suppliers include large, sophisticated equipment manufacturers that presently compete for market share, as well as enterprising start-ups that are developing new products and services to compete with these established suppliers. Following the implementation of the proposed rule, USF recipients would continue to have access to a sufficiently robust and competitive marketplace providing choices among trusted suppliers. The potential removal of one or two suspect suppliers from this dynamic market will not appreciably alter this reality.

High-cost programs. Approximately half of all universal service spending is provided to carriers through the Commission's high-cost program, which includes the Connect America Fund and the Mobility Fund.[158] These programs fund the deployment of fixed and mobile broadband networks in high-cost areas. Recipients of such funding must certify compliance with minimum deployment and capacity requirements, but are not required to identify the specific components or technology suppliers used in meeting such requirements. However, numerous

[158] *See* USAC 2017 Annual Report, *supra* n.6 (approx. $4.7 billion spent on high cost programs and approx. $4.1 billion spent on other three programs combined).

TIA members actively supply companies who are recipients of high-cost support to build the networks required to meet their deployment obligations.

With respect to the deployment of fixed and wireless broadband networks, ADTRAN, Calix, Cisco, CommScope, Ericsson, Juniper, Nokia, and other telecom suppliers are capable of providing full design, implementation, and installation services along with the broadband access electronics and equipment required for fixed and mobile broadband buildouts. These companies are the leading providers of broadband access equipment and services in the United States for high-cost USF projects. On the wireless side, numerous companies, from large equipment providers like Cisco, Ericsson, Nokia, and Samsung, to newer entrants like SpiderCloud, Tarana, Phazor, Mimosa, Ceragon, Radwin, Siklu, and Aviat, are investing heavily in this space.[159] Global data supports the view that the marketplace is populated by a wide range of trusted suppliers, many of whom have provided equipment to companies participating in the high-cost USF program for years.[160]

---

[159] *See, e.g.*, Research and Markets, *Small Cells: Market Shares, Strategies, and Forecasts, Worldwide 2018-2024*, Jan. 2018 (noting that the total value of the small cell market is $12.5 billion in 2017, up from $10.35 billion in 2016, with a projected increase to $58.7 billion by 2024), https://www.researchandmarkets.com/research/gnsslw/worldwide_small.

[160] *See generally* IHS Markit, *Router and Switch Vendor Leadership, Service Provider Survey Excerpts* (2017), https://www.juniper.net/assets/us/en/local/pdf/analyst-reports/2000686-en.pdf; *IDC's Worldwide Quarterly Ethernet Switch and Router Trackers Show Modest, Continued Growth for Fourth Quarter and Full Year 2017*, International Data Corporation, Mar. 5, 2018, https://www.idc.com/getdoc.jsp?containerId=prUS43603718; *Global Small Cell Market 2018 - Airvana, Alcatel-Lucent, Cisco, Ericsson, Huawei, NEC, Nextivity, Nokia*, SBWIRE, Feb. 23, 2018, http://www.sbwire.com/press-releases/global-small-cell-market-2018-airvana-alcatel-lucent-937797.htm; *Worldwide Small Cells Market 2018-2024: Driving Forces & Critical Issues - Markets to Reach $58.7 Billion*, PRNEWSWIRE, Mar. 6, 2018, https://www.prnewswire.com/news-releases/worldwide-small-cells-market-2018-2024-driving-forces--critical-issues---markets-to-reach-587-billion-300608952.html.

Equipment. TIA is not aware of any relevant products from Huawei or ZTE that are not also manufactured by numerous other suppliers, nor of any requirements that are not fully addressed by other suppliers. For example, a comparison of the major equipment categories marketed by Huawei to carriers, against similar offerings from other suppliers, shows that all such equipment can be found elsewhere from numerous TIA member companies alone.[161] Below is a list of the main types of equipment used in the deployment of broadband networks, all of which are provided by numerous companies within TIA's membership (and much of which would not fall within the definition of "logic-enabled" components that TIA proposes herein):

Aggregation

- Digital subscriber line access multiplexers (DSLAMs)
- Broadband access MSAN/MSAPs (Multi-service access nodes / platforms)
  - Chassis
  - MSAP electronics
  - Optical splitters
  - Vectoring modules (VDSL2)
  - Site/aggregation routers
- Cable modem termination systems (CMTSs)[162]

---

[161] *Compare* Huawei, *Carriers / Products*, http://carrier.huawei.com/en/products (visited May 28, 2018), *with* ADTRAN, *Products by Categories*, https://portal.adtran.com/web/page/portal/Adtran/wp_product_category_landing (visited May 28, 2018), Cisco, *Service Provider Products, Solutions, and Services*, https://www.cisco.com/c/en/us/solutions/service-provider/sp-products-solutions-services.html (visited May 28, 2018), Ericsson, *Ericsson Networks Products*, https://www.ericsson.com/ourportfolio/networks-products (visited May 28, 2018), Fujitsu, *Network / Products*, http://www.fujitsu.com/us/products/network/products/ (visited May 28, 2018), Juniper Networks, *Products & Services*, https://www.juniper.net/us/en/products-services/ (visited May 28, 2018), Nokia, *Networks / Products and solutions*, https://networks.nokia.com/portfolio (visited May 28, 2018), Ribbon Communications (formerly GENBAND), *Service Provider Products*, https://ribboncommunications.com/products/service-provider-products (visited May 28, 2018), Samsung Networks, *Products: The World of Mobile Technology*, https://www.samsung.com/global/business/networks/products/ (visited May 28, 2018), and Tellabs, *Tellabs Products*, https://www.tellabs.com/products/ (visited May 28, 2018).

[162] *See, e.g.*, Dade Hayes, *Cisco, Arris and Casa roll out dueling network tech announcements*, FIERCECABLE, May 30, 2017, https://www.fiercecable.com/cable/top-cable-broadband-vendors-tout-new-ways-to-quench-data-thirst.

Distribution

- DSL Broadband Access Retrofit Bundles (kits to upgrade existing remote cabinets)
    - Vectoring cards (electronic circuit packs)
    - Splitter shelves
    - Cables and accessories
- Distribution frames – optical, copper, coax, etc.
- Outside plant cabinets – pole-mounted, pad-mounted, stake-mounted
- Loop shortening cabinets
- DOCSIS access hubs
- Optical distribution networks (ODNs)
- Passive optical networks (PONs)
- Optical line terminals (OLTs)

IP Networking

- Routers and switches
- Broadband network gateways (BNGs)
- Optical network terminals (ONTs)
- PON line cards
- Cable and DSL modems

Fiber Optics

- Cabling
- Small form-factor pluggable transceivers (SFPs)
- Jumpers, attenuators
- Splicers
- Terminal closures

Power Plant and Heat Exchangers

- DC power plants
- Power wires and connectors
- Heat exchangers

Wireless (not otherwise captured above)

- Towers
- Base stations
- Small cells, picocells, metrocells, etc.
- Radio modules
- Antennas
- Access controllers
- RF cabling and connectivity

E-rate. In addition to the deployment of broadband networks to schools and libraries which are built and managed with equipment provided by the companies listed above, the E-rate program also supports inside wiring and Wi-Fi connectivity within schools. Unlike the other USF programs, USAC makes available a detailed list of the types of equipment requested by schools and libraries through the E-rate program, including the manufacturers of such equipment requested by applicants. Publicly available data identifies the following types of equipment, in addition to various services, that are requested by E-rate applicants:[163]

- Antennas, connectors, and related components
- Wireless controllers
- Wireless access points
- Switches and routers
- Cabling
- UPS/Battery back-up
- Air cards
- Racks
- Caching

The list of companies providing such services is extremely robust, including the following manufacturers: ADTRAN, Aerohive, Alcatel-Lucent (now Nokia), Apple, American Power Conversion, Avaya, Belkin, Berk-Tek, Brocade Communications Systems (now Broadcom), Cisco, CommScope, Corning, D-Link, Dell, Extreme Networks, Hitachi, HPE/Aruba, Juniper Networks, Leviton, Meraki, Netgear, Ortronics, Panduit, Ruckus Wireless (now Arris Group), SMC Networks, Sonicwall, Superior Essex, Tripplite, Ubiquiti, and Xirrus – to name a few.

[163] *See* E-rate Open Competitive Bidding: Services Requested (FCC Form 470 and Related Information) (dataset containing information about the services requested within each FCC Form 470, including the service type, function, and manufacturer, and related information from the E-rate Productivity Center (EPC)), https://opendata.usac.org/E-rate/E-rate-Open-Competitive-Bidding-Services-Requested/39tn-hjzv/data.

Based on the capabilities within TIA's membership alone, it is clear that there are sufficient options available to fixed and mobile broadband providers in order for such companies to meet their universal service obligations.[164] The benefits of ensuring they do so in a secure manner thus clearly outweigh the harms of removing certain companies from the marketplace.

VI. TIA SUPPORTS A BROAD APPROACH TO PROTECTING THE INTEGRITY OF U.S. NETWORKS.

TIA appreciates the Commission's intention to act promptly. National security concerns have been raised regarding certain suppliers, and certainty for USF recipients should be provided as soon as possible to address these threats and promote network deployment. With these principles in mind, all of the legal arguments and practical approaches put forth in these comments – from the need to rely on determinations by Congress and expert agencies to the manner in which such determinations are translated into workable restrictions by the Commission – can be implemented swiftly and without immediate involvement by any other agency.

Nevertheless, the Commission itself has recognized that it cannot and should not address these issues by itself. Rather, this proceeding forms a starting point for what is likely to become a more systemic effort across the federal government to address risks from suppliers deemed to pose a higher risk of facilitating malicious interference in the network or state-sponsored cyberespionage.[165] As such, any decisions the Commission makes now should be forward-

---

[164] *See supra* n.161; *see also* TIA, *Members of the Telecommunications Industry Association*, https://www.tiaonline.org/about/our-members/ (visited May 28, 2018).

[165] *See* Sen. Tom Cotton & Chairman Ajit Pai, *Hostile powers like Russia and China threaten US communications networks – enough*, FOX NEWS, Apr. 16, 2018, http://www.foxnews.com/opinion/2018/04/16/hostile-powers-like-russia-and-china-threaten-us-communications-networks-enough.html.

looking, while also addressing the immediate issues at hand. In particular, the Commission should commit to continued coordination with other federal agencies and Congress to ensure that federal policy evolves in a uniform manner.[166] Below, we describe some key principles that should govern that process.

A. Any Immediate Action Regarding USF Restrictions and the Specific Suppliers Named in the Notice Should Derive from and Further Complement a Whole of Government Approach.

As this proceeding explores the Commission's role in addressing the threat of untrusted suppliers in USF-funded communications networks, the Commission should remain cognizant of ongoing work in other branches of the federal government to address these and related issues. As described in Section I.B above, various agencies have been active in overseeing conduct of the companies specified in the Notice, both inside and outside the security context. Recognition of and respect for ongoing efforts by other agencies also will ensure continued enforcement of existing laws, which TIA fully supports.

A holistic approach here also is consistent with established guidelines and structure regarding the protection of critical infrastructure. Since 2013, Presidential Policy Directive 21 (PPD-21) has outlined the mechanism by which the federal government builds trusted partnerships with industry to "advance a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure."[167] In addition to naming the Communications and Information Technology (IT) sectors among the 16 critical infrastructure sectors, PPD-21 designates the Department of Homeland Security (DHS) as the Sector Specific Agency responsible for coordination with the Communications and IT sectors.

---

[166] *See, e.g.*, Notice, Statement of Commissioner Brendan Carr (noting the importance of "coordinating with our fellow agencies").

[167] PPD-21, *supra* n.76.

Activities by other agencies – either within or outside of the security context – may have a direct and immediate impact on the Commission's goals in this proceeding, and thus warrant close attention. Perhaps most notably, in April 2018, the Department of Commerce issued an order banning ZTE from buying products from U.S. suppliers.[168] While unrelated to state-sponsored cyberespionage, the order focused on ZTE's failure to abide by commitments it made after the U.S. government determined in March 2017 that the company had conspired to evade U.S. export controls.[169] As noted above, the President has recently indicated his willingness to mitigate the penalties imposed by the order, contributing to a fluid situation in which the outcome remains uncertain.[170] Meanwhile, according to a media report, Huawei has been issued a subpoena related to technology and services it provided to Cuba, Iran, Sudan and Syria, though to date it has not formally been accused of wrongdoing.[171]

---

[168] U.S. Department of Commerce Bureau of Industry and Security, *Order Activating Suspended Denial Order Relating to Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd.*, Apr. 15, 2018, https://www.commerce.gov/sites/commerce.gov/files/zte_denial_order.pdf.

[169] The order stated that ZTE's corporate behavior has been characterized by "a pattern of deception, false statements, and repeated violations." *Id.* at 6. It concluded that "ZTE still cannot be relied upon to make truthful statements, even in the course of dealings with U.S. law enforcement agencies, and even with the prospect of the imposition of a $300 million penalty and/or a seven-year denial order." *Id.* at 8-9.

[170] *See supra* nn.50-52.

[171] Paul Mozur, *Huawei, Chinese Technology Giant Is Focus of Widening U.S. Investigation*, N.Y. TIMES, Apr. 26, 2017, https://www.nytimes.com/2017/04/26/business/huawei-investigation-sanctions-subpoena.html. The U.S. government investigation that found that ZTE had conspired to sell telecommunications equipment to Iran and North Korea, in violation of U.S. export sanctions, implicated another as-yet-unnamed equipment supplier engaged in similar activity. Some believe this company could be Huawei. *See* Paul Mozur, *ZTE Document Raises Questions About Huawei and Sanctions*, N.Y. TIMES, Mar. 18, 2016, https://www.nytimes.com/2016/03/19/technology/zte-document-raises-questions-about-huawei-and-sanctions.html (describing how an internal ZTE document "cited as a model – and a cautionary tale – a rival company it called F7," and that "the description offered … matches a company far larger and more politically sensitive: Huawei Technologies, its chief rival").

In short, this attention in other arenas to the companies identified in the Notice could inform if not supersede any specific efforts the Commission may take in the context of this proceeding. Keeping these concurrent activities within the Commission's peripheral vision thus will be essential as it pursues its specific universal service goals here.

B. An Interagency Process Could Address These Issues Comprehensively and Effectively.

As described in Section IV.A *supra*, the Commission should adopt a forward-looking approach – and avoid the need for a future rulemaking – by anticipating the establishment of a future interagency process that is empowered to make national security determinations on behalf of the entire (non-military) federal government. That process should be based on specific criteria similar to those we have described above.

1. An Interagency Process Should Involve Agencies with Appropriate Expertise and Provide Due Process to Avoid Inadvertently Impacting Trusted Suppliers.

Although the Commission would not be tasked with creating or overseeing any interagency process, we describe here the basic principles that might underlie that process in order to orient this policy discussion that the Notice has accelerated, and into which the Commission's ultimate action must fit. The Commission should make clear through its actions here that it sees its own targeted role on supply chain security issues as complementary to such broader processes.

Study and interagency process. Congress should task intelligence agencies with appropriate technical expertise to study these issues. An interagency process should also be established, since such a process is likely to be more flexible and effective than targeting individual companies by name in legislation. Such process could be established by statute, executive order, or other means.

Participants and information sharing. These longer-term efforts should include the Department of Homeland Security as the Sector Specific Agency for the IT and Communications Sectors, and should also include mechanisms for meaningful input from a diverse set of private sector stakeholders, similar to the initiatives that the Commerce Department has facilitated to develop the NIST Cybersecurity Framework and to promote stakeholder action to reduce botnets and other distributed, automated threats. For example, incorporating supply chain security issues under the DHS-administered Protected Critical Infrastructure Information Act ("PCII") could potentially facilitate better information sharing from and among the private sector regarding supply chain security issues.[172]

Determinations. Any determination that a given supplier poses a national security risk should be made only after careful investigation of all available evidence, some of which may be classified. Such assessments should be made by intelligence officials equipped to consider evidence in the appropriate geopolitical context, following process-oriented and cautious deliberations.

Due process. To the extent possible, and subject to considerations of classified information, the interagency decision-making process should afford targeted companies some measure of due process, to guard against any scenario whereby a trusted supplier is inadvertently caught up in the interagency process with a negative designation, or whether changes would

[172] *See* U.S. House of Representatives Subcommittee on Communications and Technology, Hearing on Telecommunications, Global Competitiveness, and National Security, *Statement of Clete D. Johnson, Partner, Wilkinson Barker Knauer, LLP,* May 16, 2018, at 5 https://docs.house.gov/meetings/IF/IF16/20180516/108301/HHRG-115-IF16-Wstate-JohnsonC-20180516-U31.pdf. These protections have been supported by previous CSRIC recommendations and have support from key players in the regulated ISP sector. *See* CSRIC IV, Cybersecurity Risk Management and Best Practices, CSRIC IV, Working Group 4 Final Report (Mar. 2015), *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

warrant alteration of such designation. For example, if greater corporate transparency, verification through independent audits, changes in the home country's legal environment, or some combination of various factors would enable a company to be removed from a security restriction list, that information should be provided to the company. Such due process may also be legally required – for instance, the D.C. Circuit has held that a Chinese-owned company that was adversely affected by a CFIUS decision had the right to challenge that determination, which included the right to receive any non-classified evidence.[173]

2. Identification and Prohibition of Particular Suppliers Should Be Based Upon Well-Defined Criteria.

As described throughout these comments, the Commission's actions should be heavily tied to national security determinations made in some manner by the President, executive agencies with appropriate national security staffing and expertise, or Congress. Although we would not expect the Commission itself to take primary responsibility for this designation (and in fact we discourage it from doing so), below we propose a set of decisional criteria for identifying vendors of specific concern in order to help orient the policy discussion and highlight for the Commission the sort of factors that warrant emphasis.[174]

---

[173] *Ralls Corp. v. Committee on Foreign Inv. In the U.S.*, 758 F.3d 296 (D.C. Cir. 2014). The court held that the company had a "right to notice of the … designation as well as the unclassified support therefor and the opportunity to rebut the unclassified supporting evidence…." *Id.* at 318.

[174] These criteria are not to be applied lightly. In general, we agree with Nokia that any decision-making body applying these criteria should "make clear that identifying a company as a prohibited provider is an extraordinary act" that the decision-making body "expects would be used sparingly, and based on a review that takes into account the totality of the circumstances." Nokia Ex Parte, *supra* n.112, at 2.

Nation-specific criteria. There are enhanced risks associated with companies that are headquartered in countries considered to pose a threat to U.S. national security interests. Certain factors could be assigned extra weight:

- Given the critical importance of cybersecurity to national security, a designation might be based in part on whether a nation has a record of extensive state-backed espionage and/or theft of commercial IP or trade secrets.

- Decisionmakers should also consider the laws and judicial processes that govern foreign-headquartered companies. They should note the extent to which those companies are compelled to answer to foreign intelligence services considered adversarial to the U.S. For example, China's Cybersecurity Law[175] and Counter-Terrorism Law[176] set out requirements for companies to comply with Chinese government requests for information. Chinese companies operating in other countries may be required to comply with intelligence requests from the Chinese government on an extra-territorial basis.[177]

- Any designation relating to countries of special concern should clearly exempt U.S. defense allies.

Company-specific criteria. In determining which specific companies pose risks, decisionmakers might want to consider a combination of inter-related factors:

- Evidence that a firm has engaged in illegal activity, or government investigations into such activity.

---

[175] Cybersecurity Law of the People's Republic of China, at art. 28, adopted Nov. 7, 2016 ("The network operators shall provide technical support and assistance when the public security organs or national security organs conduct activities aimed to safeguard national security and investigate crimes according to law.") ("China Cybersecurity Law").

[176] *See* Counter-Terrorism Law of the People's Republic of China, adopted Dec. 27, 2015. The law requires service providers to "provide technical support and assistance such as technical interface and decryption to the public security organs and state security organs in preventing and investigating terrorist activities in accordance with law." *Id.* at art. 18. "Terrorist activities" is defined to include "disruptions to public order," *id.* at art. 3, which may be broadly interpreted by a Communist Party that is highly sensitive to perceived threats to its authority.

[177] *See* China Cybersecurity Law, *supra* n.175, at art. 75 ("When any agency, organization or individual overseas attacks, intrudes into, interferes with or disrupts any critical information infrastructure of the People's Republic of China, causing serious consequences, he/it is subject to legal liability according to law. The public security department and other departments concerned under the State Council may concurrently freeze the property of such agency, organization or individual or adopt other necessary measures.").

- The degree of support (through subsidies, preferential loans, or other means) that a given ICT supplier has received from a state that has engaged in malicious or other illicit cyber activity.

- A company's corporate governance structure and the extent to which it has complied with any U.S. government requests for information. Transparency in other corporate processes may also be a relevant factor.

Product-specific criteria. Decisionmakers should consider differentiating among products, customers, and use cases by considering:

- The relevance of a particular product to security within a network. Given the globalized nature of supply chains, decisionmakers should avoid designations that would claim a wide range of low-level products to be potential security risks merely due to their place of manufacture. For example, there may be firms in China that supply U.S. companies with network components that are not considered relevant to network security.

- User type and/or use case, since national security users, general government users, and consumers may each have different security needs.

Notably, these criteria would likely apply to the companies named in the Notice, while avoiding overbreadth. For example, based on the discussion of the Department of Commerce's export ban in connection with ZTE discussed in Section VI.A above, these criteria would presumably encompass ZTE and possibly Huawei as well. At the same time, such criteria would be sufficiently non-specific that they could apply to additional entities to the extent appropriate. Further, applying these criteria in a flexible manner would allow companies that become subject to any prohibition to obtain relief if circumstances warrant.

C. Global Cooperation Is Necessary to Address This Issue.

As described above, any actions by the Commission and by the rest of the federal government will set precedents for the global community. Given the international nature of the Internet and communications ecosystem and the thoroughly global supply chains of virtually all ICT equipment and products, no single country can address the threats from potentially malicious actors or high-risk suppliers by itself.

Deliberate and coordinated action regarding suppliers of concern should begin with developing a common approach with the United States' closest defense and intelligence allies, including the other "Five Eyes" countries (the United Kingdom, Canada, Australia, New Zealand), other members of NATO, and other allies with advanced ICT markets such as South Korea, Japan and Israel. Given the present differences between the United States and many of our closest allies regarding the particular suppliers of concern identified in the Notice, even this first step of arriving at a coordinated approach with these especially like-minded nations will be difficult. However, without progress toward such a coordinated global approach, progress in addressing particular suppliers of concern will be impossible.

Moreover, in addition to concerns regarding particular suppliers, the United States must also continue efforts to establish and promote broader international cybersecurity norms with like-minded nations. To that end, TIA greatly appreciates the efforts of the U.S. government to engage in cybersecurity-related dialogues with the European Union, Japan, Australia, and India, as well as China, among others.[178] While we recognize the frustrations that have attended some international work – notably, the inability of the United Nations Group of

[178] European Union External Action, *"Joint Elements" from the 4th European Union - United States Cyber Dialogue – 14 and 15 November 2017*, May 16, 2018, https://eeas.europa.eu/headquarters/headquarters-homepage/44673/%E2%80%9Cjoint-elements%E2%80%9D-4th-european-union-united-states-cyber-dialogue-%E2%80%93-14-and-15-november-2017_en; U.S. Department of State, *Joint Statement of the Japan-U.S. Cyber Dialogue*, July 24, 2017, https://www.state.gov/r/pa/prs/ps/2017/07/272815.htm; Center for Strategic & International Studies, *Australian Prime Minister Malcolm Turnbull meets with Australia-U.S. Cyber Security experts in Washington*, Feb. 22, 2018, https://www.csis.org/news/australian-prime-minister-malcolm-turnbull-meets-australia-us-cyber-security-experts-washington; The White House, *Joint Statement: 2016 United States-India Cyber Dialogue*, 2016 DAILY COMP. PRES. DOC. 646, Sept. 29, 2016, https://www.gpo.gov/fdsys/pkg/DCPD-201600646/pdf/DCPD-201600646.pdf; U.S. Department of Justice, *First U.S.-China Law Enforcement and Cybersecurity Dialogue*, Oct. 6, 2017, https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue.

Governmental Experts to achieve consensus on this issue in 2017[179] – we hope that meaningful discussion on cybersecurity norms can resume within a multilateral framework in the future.

CONCLUSION

The Commission faces a truly extraordinary situation. National security concerns have been identified regarding certain suppliers of communications products, with actions against these suppliers having been taken or contemplated both by Congress and by officials at the highest levels of the federal government. And since the Commission adopted the Notice, it has become clear that this proceeding is now being carefully watched both at home and abroad. The Commission's actions should set an example for other federal agencies, advance the discussion among policymakers in Congress and the Administration, and potentially guide the actions of other telecom regulators around the world.

In this rapidly-changing situation, the Commission has an important but limited role to play. It should begin by adopting its proposal to restrict spending through the universal service mechanism on products from suppliers of specific concern. Establishing a narrowly-tailored rule that focuses on the problems at hand, while also keeping an eye on the future, is the best approach to promote national security immediately while simultaneously allowing the national and international conversation on these issues to continue.

For our part, TIA will continue to actively participate in that conversation, including discussions with and among our member companies: the manufacturers and suppliers of the

[179] *See* Michele Markoff, U.S. Expert to the GGE, Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, June 23, 2017, https://usun.state.gov/remarks/7880; *see also* Stefan Soesanto & Fosca D'Incau, *The UN GGE Is Dead: Time to Fall Forward*, EUROPEAN COUNCIL ON FOREIGN RELATIONS, Aug. 15, 2017, https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance.

world's ICT products. TIA and our member companies are on the front lines every day of the global struggle to ensure that ICT products are both secure and reliable, and we therefore have a vital stake in the outcome of this proceeding. We look forward to working with the Commission and with the rest of the federal government to advance the conversation on these very important issues in the months ahead.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: */s/ Cinnamon Rogers*

Cinnamon Rogers
Senior Vice President, Government Affairs

Dileep Srihari
Senior Policy Counsel and Director, Government Affairs

K.C. Swanson
Director, Global Policy

Savannah Schaefer
Policy Counsel, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Road
Suite 200
Arlington, VA 22201
(703) 907-7700

June 1, 2018

APPENDIX: PROPOSED RULE TEXT

§ 54.9 Prohibition on use of funds

(a) *Prohibition.* No universal service support may be used to purchase or obtain covered communications technology products, telecommunications services, or information services produced or provided by any company posing a national security threat to the integrity of communications networks or the communications supply chain.

(b) *Covered companies.* For purposes of this section, a "company posing a national security threat to the integrity of communications networks or the communications supply chain" shall be any company that:

(1) is prohibited by name in any federal statute from selling one or more covered communications technology products to one or more civilian federal agencies for national security reasons;

(2) is prohibited by name in any publicly-released finding, directive, order, or similar action issued by the President, the Department of Homeland Security, or any other federal national security agency from selling one or more covered communications technology products to one or more civilian federal agencies for national security reasons;

(3) is prohibited by name as the result of a federal interagency review process established either by statute or by executive order from selling one or more covered communications technology products to one or more civilian federal agencies for national security reasons; OR

(4) is a subsidiary or affiliate of, or successor-in-interest to, any company mentioned above.

(c) *Covered products.* For purposes of this section, a "covered communications technology product" means:

(1) any software or firmware, regardless of whether its known functionality includes networking functions;

(2) any equipment containing one or more logic-enabled components, as described in paragraph (3) below; OR

(3) any logic-enabled component, which are those components containing or implementing logical functions and that are capable of generating or modifying the information content of digital data. **[**This includes, but is not necessarily limited to, network controller chips, CPUs, and functional circuit boards such as network or graphics cards, but does not include analog circuits or components such as op-amps,

power supply regulators, cabling or antennas unless those components themselves contain a covered component.**]**

(d) *List of covered companies.* The Commission shall publish on its website [by December 31, 2018], and update as necessary, a list of prohibited companies it determines qualify under subsection (b). The Commission shall immediately notify the Administrator of any updates, who in turn shall promptly notify all recipients of universal service support.

(e) *Attestations.*

(1) Beginning on [January 31, 2019] and annually thereafter, any recipient of universal service support shall provide a written attestation to the Administrator that no universal service funds it receives were spent in the prior funding year to purchase or obtain covered communications technology products, telecommunications services, or information services from any covered company in violation of this section. Such attestations are required for recipients of funds from any universal service programs.

(2) When satisfying the requirements of paragraph (1), recipients may reasonably rely upon attestations from relevant suppliers that any covered communications technology products, telecommunications services, or information services provided by those suppliers do not, in turn, contain or rely upon any covered communications technology products, telecommunications services, or information services provided or obtained from any covered company. Such suppliers may reasonably rely, in turn, upon such attestations from their upstream suppliers.

(f) *Multiple products.* At a supplier's option, any attestations provided under paragraph (e)(2) may be provided on a per-product basis, for multiple products, and/or for all products sold by the supplier as of the date of attestation.

(g) *No attestation to white-labeled products.* No supplier that is not the original manufacturer of any product or component may provide any attestations under paragraph (e)(2) with regard to such product or component. No entity may rely upon such an attestation if it reasonably knew that the supplier was not the original manufacturer. Appropriate attestations must be obtained from the original manufacturer instead.

(h) *Zero percent attestation option.* Any recipient or supplier providing an attestation of non-purchase from, or non-reliance upon, any covered company, under paragraphs (e)(1) or (e)(2), may elect to attest to non-purchase of or non-reliance upon *any* software, equipment or components, in lieu of attesting to non-purchase of or non-reliance upon covered communications technology products.