Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

WRITTEN *EX PARTE* SUBMISSION OF HUAWEI TECHNOLOGIES CO., LTD AND HUAWEI TECHNOLOGIES USA, INC.

Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc. (collectively, "Huawei"), by their undersigned counsel, submit this *ex parte* presentation to supplement the record in the above-captioned docket. On December 21, 2018, the President signed the SECURE Technology Act (H.R. 7327) into law. This Act includes the Federal Acquisition Supply Chain Security Act of 2018 ("Supply Chain Security Act"). The Supply Chain Security Act is a singular and refreshing change of approach by Congress in addressing supply-chain issues. The Supply Chain Security Act requires development of government-wide criteria and rules for identifying, assessing, and mitigating supply chain risks posed by any global supplier, rather than following earlier, flawed approaches like that under consideration in this rulemaking docket of blacklisting specific entities in isolation, based solely on where they are headquartered. The Act also provides meaningful safeguards and due process procedural protections to promote accurate and equitable results, including notice, opportunity for rebuttal, and judicial review.

Huawei has been a long time victim of the lack of fair process. For years, it has been criticized for security risks by the U.S. government, even though the only evidence of backdoors in Huawei's equipment was the result of implants by the NSA. Huawei has been condemned for its

relationship with the Chinese government, though it is exclusively owned by employees, while its 'western' competitors use joint ventures with Chinese government to build products for the U.S. Huawei has been punished for not being able to prove its innocence, even though it was the only company that invited government investigators to come to its headquarters and inspect corporate records concerning its ownership, financials and more.

The absence of due process also undermines the public interest. As the record in this proceeding makes clear, Huawei is a critical supplier to numerous rural providers, which might not be able to provide service absent the availability of Huawei's lower cost, high-quality equipment. Huawei is also the unparalleled leader in 5G equipment. As a result, unreasonable and unfair restrictions on the sale and use of Huawei equipment would limit the U.S. to inferior and more expensive substitute equipment and jeopardize its commitment to building the most advanced 5G network in the world.

In contrast to targeted and restrictive policies driven by politics and competitors, the Supply Chain Security Act promises to provide due process and rationality in assessing supply chain security. The Act will appropriately allow the government to evaluate and respond to risks across the entire global supply chain, rather than preemptively excluding a handful of companies on an ad hoc basis in one sector of the telecommunications industry. Indeed, the Supply Chain Security Act mirrors the recommendations provided by commenters representing a diverse set of interests throughout this proposed rulemaking and further confirms that the FCC should terminate this rulemaking proceeding as irredeemably flawed.

I. THE FEDERAL ACQUISITION SUPPLY CHAIN SECURITY ACT OF 2018

The SECURE Technology Act, including the Supply Chain Security Act, was signed into law on December 21, 2018. The Supply Chain Security Act has three major substantive components. First, it creates a new Federal Acquisition Security Council, which is required to identify and develop a strategy to address supply chain risks and has requisite authority to designate supply chain security risks for exclusion or removal. §§ 1322-25. Second, it requires the heads of each executive agency to assess, plan for, and provide information about information technology security risks. § 1326. Third, it authorizes executive agencies, under certain circumstances, to exclude sources from procurements involving sensitive information technology. § 4713. The Act also provides notice, opportunity to respond, and judicial review for decisions by either the Council or agencies.

A. The New Federal Acquisition Security Council

The Supply Chain Security Act creates a new Federal Acquisition Security Council within the executive branch. § 1322(a). The Council is composed of designees from expert agencies tasked with national security and related areas of responsibility—for instance, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, the National Counterintelligence and Security Center, the Federal Bureau of Investigation, the National Security Agency, and the National Institute of Standards and Technology. § 1332(b). It also includes designees from expert agencies tasked with procurement-related responsibilities, such as the Office of Management and Budget (OMB), the General Services Administration, and other agencies as determined by the Council's Chairperson. *Id.* The FCC is not one of the enumerated agencies Congress included in the Council.

The Council has several functions. First, it is to develop government-wide criteria for assessing threats to national security from acquisition of information technology and to share information and guidance about managing those threats. § 1323(a). It is also tasked with developing an overall strategic plan for addressing supply chain risks. § 1324.

When it identifies risks, the Council is required to establish criteria and procedures for recommending the exclusion or removal of those risks. § 1323(c). Exclusion recommendations would order exclusion from agency procurements and can cover either entire sources or specific "covered articles." § 1323(c)(1)(A); *see also* § 1321(3) (defining "covered article" by reference to § 4713(k)(2), which defines the term to include various types of information technology and telecommunications). Similarly, recommendations for removal direct agencies to remove existing "covered articles" from their information systems. § 1323(c)(1)(B). Recommendations must include, among other things, information sufficient to identify sources or covered articles and information about the scope and applicability of the recommended exclusion or removal. § 1323(c)(2).

Notice of recommendations is required "to any source named in the recommendation." § 1323(c)(3). Notice must include an opportunity for the source to submit information and argument in opposition within 30 days. *Id.* The notice is to include the criteria relied upon and, "to the extent consistent with national security and law enforcement interests," the information relied upon. § 1323(c)(3)(B).

Once notice and an opportunity to submit opposition are provided, the Secretary of Homeland Security (for civilian agencies), the Secretary of Defense (for national security systems), or the Director of National Intelligence (for intelligence systems) reviews the materials

and "may issue exclusion and removal orders based upon such recommendations." § 1323(c)(5)(A). Notice of the exclusion or removal is then provided to the affected entity, again with information supporting the notice to the extent consistent with national security and law enforcement interests. § 1323(c)(6). There is no express limit on the length of time that exclusion or removal orders can be in effect, but such orders can be rescinded by the official authorized to implement them in the first place under § 1323(c)(5)(A). *See* § 1323(c)(5)(E).

B. Agency Assessment and Management of Internal Supply Chain Risks

Similar to the Council's duty to assess supply chain risks, the Supply Chain Security Act separately directs the heads of all executive agencies to assess the supply chain risks to their agencies from various types of information technology. § 1326. Agencies are directed to consider the Council's recommendations and to prioritize mission-critical systems for assessment. For interagency acquisitions, the agency providing funding is responsible for the assessment. The Department of Homeland Security is tasked with providing support in making assessments of security risks under Section 1326.

C. Mitigation of Supply Chain Risks in Agency Procurement

The Supply Chain Security Act additionally creates new procedures for agencies to exclude sources from agency information technology procurements in specific circumstances. § 4713. The Act authorizes agencies to take so-called "covered procurement action[s]," which are defined as acquisition of various types of information technology made while excluding some potential providers of that technology. *See* § 4713(k)(2)-(4) (defining "covered procurement action[s]," "covered procurement," and "covered article[s]"). The exclusion authorization is procurement-specific even though it involves designating a particular source of information

technology. In practice, this approach limits exclusions to the information technology to be acquired in the particular procurement. In sum, agencies are allowed to exclude an information technology source as to a particular procurement if they conclude that the source poses a supply chain risk to that procurement.

However, before making an exclusion determination, an agency must get a recommendation from the agency's chief acquisition officer and chief information officer concluding that there is a significant supply chain risk in the procurement at issue. § 4713(b)(1). Similar to the exclusion or removal provisions of § 1323, the agency generally must also provide notice of the conclusion to the source, including the information that forms the basis for the recommendation, to the extent consistent with national security and law enforcement interests. § 4713(b)(2). The source must be provided with 30 days to submit information and argument in opposition. *Id.* The agency must then document its decision in writing, including discussion of why less intrusive measures are not reasonably available, and provide notice of the determination to Congress. § 4713(b)(3).

There is an exception to the procurement exclusion process above, but only if the head of the agency "determines that an urgent national security interest requires" a procurement that excludes a particular source. § 4713(c). In such situations, the agency may temporarily delay notice to the source. *Id.* However, the urgent national security interest determination only authorizes such procurements for the following 60 days, and notice must be provided in any event "as soon as practicable after addressing the urgent national security interest" by following the processes in § 4713(b). *See* § 4713(c)(2). Each agency head is also required to inform Congress at least annually of all such procurement actions taken. § 4713(h).

D. Judicial Review of Decisions by Council or Agencies

The Supply Chain Security Act appropriately provides for judicial review of either a Council exclusion or removal order of a source or item or of an agency decision to bar a source from participating in a procurement. § 1327. Sections 1327(a) and (b)(3) provide that the procedures provided generally are exclusive, notwithstanding any other provision of law, with discretionary review by petition for certiorari to the U.S. Supreme Court.

Section (b)(1) provides that, within 60 days of an exclusion or removal decision or of a covered procurement action, the entity impacted by the decision "may file a petition for judicial review" in the U.S. Court of Appeals for the D.C. Circuit. § 1327(b)(1). The statute has its own standard of review that repeats, nearly verbatim, the requirements of the Administrative Procedure Act (APA), 5 U.S.C. § 706(2)(A)-(E). Those provisions generally allow judicial review of claims that an action is arbitrary or capricious, contrary to constitutional right, not authorized by statute, lacking substantial factual support, or not procedurally proper. § 1327(b)(2)(A)-(E).

The judicial review provisions require filing of the information relied upon by the Council or agency in issuing an exclusion or removal order or taking a covered procurement action. § 1327(b)(4)(B). They require all unclassified, non-privileged, non-trade secret information to be provided to the party challenging the decision. § 1327(b)(4)(B)(ii). They also allow classified, privileged, or Foreign Intelligence Surveillance Act materials to be filed with the court in camera and ex parte. § 1327(b)(4)(B)(iii).

II. THE HOLISTIC APPROACH OF THE SUPPLY CHAIN SECURITY ACT PROVIDES A SUPERIOR APPROACH TO THE USF RULEMAKING

As the preceding discussion demonstrates, the Supply Chain Security Act now provides a comprehensive government-wide approach to managing supply chain security risks. That ap-

proach reflects a singular and refreshing change of method by Congress. It is far superior to the FCC's proposed rule and consistent with the recommendations of commenters here. The FCC should step back and allow the new Federal Acquisition Security Council to follow the fresh course charted by Congress rather than continuing the flawed approach of blacklisting individual entities piecemeal.

Commenters on the FCC's USF rulemaking have already pointed out numerous shortcomings of the FCC's simplistic and misguided approach. *See, e.g.*, Huawei Comments, WC Doc. No. 18-89 (June 1, 2018); Huawei Reply Comments, WC Doc. No. 18-89 (July 2, 2018); Huawei Ex Parte Submission, WC Doc. No. 18-89 (Aug. 6, 2018); ITTA Comments, WC Doc. No. 18-89 (June 1, 2018); Mark Twain Communications Co. Comments, WC Doc. No. 18-89 (June 1, 2018). The Supply Chain Security Act highlights these flaws by providing an actual, concrete and contrasting approach to how important supply chain security concerns in the technology arena should be managed.

For example, as commenters have explained, the FCC lacks the authority and expertise to evaluate and act on national security concerns. The Supply Chain Security Act embraces a government-wide approach directed by an interagency Council whose expert agency members have expertise in a variety of relevant areas, and is the appropriate way to manage supply chain security risks. Significantly, in selecting these government agencies to populate the Council, Congress chose not to include the FCC.

Further, as the record in this proceeding reflects, virtually every equipment provider relies on a global supply chain, and thus an effective approach to managing supply chain risks cannot just single out a few providers. It must instead provide a framework to assess and mitigate

those risks across all providers. That is what the Supply Chain Security Act does by creating an interagency Council that gives the government the flexibility to address changing facts, needs, and risks across the entire global supply chain as they arise with respect to any supplier.

Unlike the FCC's one-dimensional proposed approach, the Supply Chain Security Act balances meaningful supply chain security with critical procedural protections for suppliers. It allows the government to respond quickly to perceived threats but also gives both entities and manufacturers of articles considered for exclusion, removal, or bar from procurements notice and opportunity to be heard at the agency level as well as judicial review of those decisions. Those procedural protections are derived from traditional concepts of due process and follow familiar, well-defined principles of agency law developed through legislation and decades of administrative law proceedings. By contrast, as commenters have explained, such protections are not provided by the current FCC proposed rule.

Such due process is particularly important here, where neither the rulemaking record nor the public record more generally contains *any* evidence that Huawei's equipment includes any backdoors or other vulnerabilities implanted or used at the behest of the Chinese government. Ironically, the only evidence of such implants is reported activity by the NSA, which apparently targeted Huawei routers and also was able to gain access to internal Huawei emails and source code.[1] Without due process, the banner of national security runs the risk of being used as

[1] See David E. Sanger and Nicole Perlroth, N.S.A. Breached Chinese Servers Seen as Security Threat, THE NEW YORK TIMES A1 (Mar. 22, 2014), available at https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html (NSA "found a way into Huawei's headquarters" and copied founder's emails); Jeremy Hsu, U.S. Suspicions of China's Huawei Based Partly on NSA's Own Spy Tricks, IEEE

camouflage for unfair competition. In the present FCC docket, the single active supporter of anti-Huawei policies, TIA, is simply a consortium of Huawei's competitors. Due process protections such as those provided in the Supply Chain Security Act afford much needed safeguards to insulate critical national security decisions from undue influence and help ensure that purported national security concerns are not selectively applied to exclude one competitor to the benefit of others that also rely on a global supply chain.

The Supply Chain Security Act also provides a mechanism to ensure consistent government standards. As other commenters in this docket have noted, it is counterproductive for multiple government agencies to adopt overlapping, likely inconsistent standards. *See, e.g.*, CCIA Section 889 Comments, WC Doc. No. 18-89, at 2 (Nov. 16, 2018) ("To the extent the Commission is called upon to make judgments regarding national security, it should defer to the expert U.S. Government agencies."). Even some commentators who were in general supportive of restrictions recognized that there are significant coordination problems with the FCC acting unilat-

---

SPECTRUM (Mar. 26, 2014), available at https://spectrum.ieee.org/tech-talk/computing/hardware/us-suspicions-of-chinas-huawei-based-partly-on-nsas-own-spy-tricks ("A joint NSA and CIA operation targeting Huawei products appears under the code name 'Turbopanda' in several software exploits described by the NSA catalog. One persistent backdoor software implant named 'Headwater' targets Huawei routers so that the NSA could monitor Internet traffic passing through them. Another backdoor software implant called 'Halluxwater' targets Huawei's Eudemon series of hardware firewalls—computers that guard an organization's internal network from the rest of the Internet."); *id.* (NSA was able to "steal the source code for specific Huawei products that could be used to exploit those products for espionage or cyberwarfare"); *id.* ("There is no solid evidence that Huawei has in fact installed hardware back doors in its products that could be used for either state intelligence or corporate espionage."). See also Marcel Rosenbach, Holger Stark, & Bernhard Zand, New Documents Reveal the Struggle of American and Chinese Secret Services for Supremacy in the Network, DER SPIEGEL (Jan. 22, 2019), available at https://magazin.spiegel.de/SP/2014/13/126149146/ ("The evaluators were disappointed, however: many emails were spam, other companies' promotional offers, expense reports and travel plans by Ren and Sun.").

erally when there are government-wide solutions in progress. *See, e.g.*, NCTA Section 889 Comments, WC Doc. No. 18-89, at 3-4 (Nov. 16, 2018). Such concerns have even more weight now that the Supply Chain Security Act has been enacted. Before, there was a significant likelihood that the FCC's USF rulemaking would result in inconsistent results if other agencies followed suit; now the Council provides a unified government body that should avoid that outcome. But it can only do so if the FCC recognizes that it should pause in its headlong rush to judgment to allow the Council to do the work it was created to do.

III. CONCLUSION

For the foregoing reasons, the Commission should terminate this rulemaking proceeding in favor of a more comprehensive, holistic approach to supply chain security.

Respectfully submitted,

/s/

Glen D. Nager
Bruce A. Olcott
Ryan J. Watson

JONES DAY
51 Louisiana Ave, NW
Washington, D.C. 20001
(202) 879-3939
(202) 626-1700 (Fax)
gdnager@jonesday.com
bolcott@jonesday.com
rwatson@jonesday.com

Andrew D. Lipman
Russell M. Blau
David B. Salmons

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave, NW
Washington, DC 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com
david.salmons@morganlewis.com

Counsel to Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc.