Before the Department of Commerce
Bureau of Industry and Security
Washington, D.C.

In the Matter of	)	
	)	
Request for Comments on Future	)	Docket No. BIS 2020-0001
Extensions of Temporary General	)	RIN 0694-ZA02
License (TGL)	)	
	)	

COMMENTS OF GSMA

David Walsh
General Counsel

GSMA
The Walbrook Building, 25 Walbrook
London, EC4N 8AF, UK
Tel: +44 (0)207 356 0600
Fax: +44 (0)207 356 0601

March 25, 2020

Submitted electronically via https://www.regulations.gov

Mr. Richard E. Ashooh
Assistant Secretary for Export Administration
Bureau of Industry and Security
U.S. Department of Commerce
14th Street and Pennsylvania Avenue, NW
Washington, DC 20230

Re: Comments of the GSM Association on BIS's *Request for Comments on Future Extensions of Temporary General License (TGL),* Notification of Inquiry, Docket No. BIS 2020-0001, RIN 0694-ZA02

Dear Mr. Ashooh:

On behalf of its members, the GSM Association ("GSMA") submits these comments in response to the Bureau of Industry and Security's ("BIS") March 12, 2020 *Request for Comments on Future Extensions of Temporary General License (TGL)*.[1] Since it was first issued in May 2019, BIS's temporary general license ("TGL") authorizing certain limited transactions with Huawei Technologies Co., Ltd. and its affiliates listed on BIS's Entity List (collectively, "Huawei") has been extended four times and has been amended to limit participation in international telecommunications standards setting activities.[2] All but one of these extensions has been announced nearly simultaneously with the expiration date, leaving U.S and global consumers, operators, and manufacturers in a perpetual state of uncertainty as to whether critical network operation and security-related activities will continue to be permitted and for how long.

[1] U.S. Department of Commerce, Bureau of Industry and Security, *Request for Comments on Future Extensions of Temporary General License (TGL)*, Notification of Inquiry, 85 Fed. Reg. 14428 (Mar. 12, 2020) ("NOI").

[2] *See* U.S. Department of Commerce, Bureau of Industry and Security, *Temporary General License*, Final Rule, 84 Fed. Reg. 23468 (May 22, 2019); U.S. Department of Commerce, Bureau of Industry and Security, *Temporary General License: Extension of Validity, Clarifications to Authorized Transactions, and Changes to Certification Statement Requirements*, Final Rule, 84 Fed. Reg. 43487 (Aug. 21, 2019); U.S. Department of Commerce, Bureau of Industry and Security, *Temporary General License: Extension of Validity*, Final Rule, 84 Fed. Reg. 64018 (Nov. 20, 2019); U.S. Department of Commerce, Bureau of Industry and Security, *Temporary General License: Extension of Validity*, Final Rule, 85 Fed. Reg. 8722 (Feb. 18, 2020); U.S. Department of Commerce, Bureau of Industry and Security, *Temporary General License: Extension of Validity*, Final Rule, 85 Fed. Reg. 14416 (Mar. 12, 2020).

As GSMA has previously urged,[3] BIS policies regarding the scope and duration of the TGL must promote stability and predictability, which are particularly important in the current environment of substantial global economic uncertainty. Especially in light of the global challenges arising from the COVID-19 pandemic, the effects of which are sure to last for many months, the private sector should not be subjected to further economic uncertainties or burdens. BIS should refrain from adopting policies that will disrupt the availability and quality of communications networks and services around the world, which are proving to be vital to citizens and governments battling the global COVID-19 pandemic. Accordingly, GSMA respectfully requests that BIS extend the TGL for a minimum of an additional 18 months. As explained in greater detail below, additional time is critical to U.S. and global consumers, operators, and manufacturers, especially as the United States continues to work through policy issues related to supply chain regulation and the promotion of viable alternatives to Huawei. GSMA also requests that BIS reinstate and modify the authorization for activities in furtherance of or for the development of global telecommunications standards.

A. Background on GSMA Interest and History of Proceeding

GSMA represents the interests of mobile network operators (some of which are also fixed operators) around the world, uniting nearly 750 mobile operators with more than 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers, and Internet companies, as well as organizations in adjacent industry sectors. GSMA has a history of collaboration with the U.S. government on security and economic issues,

[3] *See* Letter from J. Shane and M. Brown, Counsel to GSMA, to K. Nies-Vogel, BIS, re: *Request for Extension of Temporary General License to Permit Transactions with Huawei that Are Necessary for the Operation of Telecommunications Networks and Provision of Critical Updates and Repairs for Consumers* (Aug. 6, 2019).

with the shared goal of supporting deployment of interoperable advanced telecommunications technologies.

Since Huawei was added to the Entity List in May 2019,[4] GSMA has been actively engaged with BIS and GSMA's members to address our shared interest in national security, network integrity, and supply chain risk management. Huawei is the world's largest telecommunications equipment manufacturer, and its equipment is deployed in current-generation wireless networks across the globe. The addition of Huawei to BIS's Entity List as well as other recent U.S. government actions have imposed significant costs on global operators and have shifted the market for equipment and managed services. While these actions have improved the ability of some companies to compete in certain markets, these actions have not yet led to the creation of new competitors. Supply chains in many areas remain limited, and the transition remains costly and challenging. GSMA and its members appreciate BIS's flexibility and openness to industry input on the effects of the Entity List designations and welcome the opportunity to submit these comments.

B. BIS Should Extend the TGL for a Minimum of an Additional 18 Months

As noted above, the TGL has been extended four times since it was first issued in May 2019, and in all but one of these cases, the extension was announced almost simultaneously with the expiration date. While GSMA appreciates BIS's ongoing recognition that the TGL remains necessary "to prevent the interruption of existing network communication systems and equipment . . . and allow time for companies and persons to shift to other sources of equipment, software and technology,"[5] such repeated, short-term extensions are not conducive to planning and predictability in complex global operations and service delivery. BIS should therefore extend the

[4] *See* U.S. Department of Commerce, Bureau of Industry and Security, *Addition of Entities to the Entity List*, Final Rule, 84 Fed. Reg. 22961 (May 21, 2019).

[5] NOI, 85 Fed. Reg. at 14429.

TGL for a minimum of 18 months in lieu of *ad hoc* 45- and 90-day extensions. Doing so will promote predictability for industry participants across the U.S. and global economies, whose supply chains and alternative sourcing are not ascertainable in 45- and 90-day time periods.

A long-term extension is particularly important for many U.S. operators currently faced with short-term replacement burdens that could impact their service offerings, such as rural operators struggling to implement recently enacted Federal Communications Commission ("FCC") restrictions and potential rip and replace obligations.[6] The recently enacted Secure and Trusted Communications Networks Act, which mandates the establishment of a $1 billion reimbursement fund over the next year to help small operators remove such equipment, highlights that replacing Huawei equipment will require significant amounts of time and money.[7] Moreover, because most countries are not subsidizing the removal of Huawei equipment, such equipment will remain in existing networks around the world for the duration of its useful life.

Global operators similarly should not be strained at a time when they are focused on maintaining service levels in underserved communities in the midst of a worldwide public health crisis. Connectivity remains more vital than ever, regardless of whether a consumer is located in New York City, Madrid, or Japan. The COVID-19 pandemic highlights the vital role that telehealth, virtual meetings, online school, and social media are playing across the globe as governments, non-governmental organizations, public health officials, and ordinary citizens deal with an unprecedented global challenge that is expected to last 18 months or longer.[8]

---

[6] *See* Federal Communications Commission, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs; Huawei Designation; ZTE Designation*, Final Rule, 85 Fed. Reg. 230 (Jan. 3, 2020); Federal Communications Commission, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Proposed Rule, 85 Fed. Reg. 277 (Jan. 3, 2020).

[7] *See, e.g.*, A. Cullen, "Trump Signs $1B Bill To 'Rip and Replace' Huawei, ZTE Gear," Law360 (Mar. 12, 2020), *available at* https://www.law360.com/articles/1252892/trump-signs-1b-bill-to-rip-and-replace-huawei-zte-gear.

[8] *See* P. Baker and E. Sullivan, "U.S. Virus Plan Anticipates 18-Month Pandemic and Widespread Shortages," N.Y. Times (Mar. 17, 2020), *available at* https://www.nytimes.com/2020/03/17/us/politics/trump-coronavirus-plan.html.

C. BIS Should Work with Policymakers to Harmonize and Simplify U.S. Regulation of Exports, Supply Chain Regulation, and National Security Evaluation of the Communications Sector

The Federal Register notice asks about "potential alternatives" to extending the TGL. Numerous work streams are underway in the United States to address supply chain security in telecoms, ICT, and otherwise. GSMA urges BIS to consider its approach in the context of the other supply chain and export control issues under consideration. For example, the Commerce rulemaking to implement the Executive Order on supply chain security creates additional complexities for companies with overseas operations and relationships. Likewise, Congress has been looking at these companies in particular and at broader supply chain issues, as reflected in the recent *Secure and Trusted Communications Networks Act*. GSMA urges BIS to try to simplify compliance burdens and harmonize its approach to export controls as part of the government's overall approach to supply chain.

D. BIS Should Preserve the TGL's Existing Authorizations

The TGL currently authorizes the following three categories of activity:

- Continued operation of existing networks and equipment;
- Support to existing personal consumer electronic devices and Customer Premises Equipment; and
- Cybersecurity research and vulnerability disclosures.

GSMA urges BIS to retain clear protections for each of these categories. If the TGL is not extended, consumers will be left with outdated handsets and other electronic devices and therefore significantly more susceptible to cybersecurity threats. Securing handsets and other devices is a collaborative process among manufacturers, operating system developers, and wireless network operators, often requiring the provision of U.S. software and/or technology subject to export

restrictions. Although the device manufacturer engages in the bulk of the work required to build security updates/patches, the collaborative process requires the provision of certain software and/or technology that may be subject to the Export Administration Regulations ("EAR") to Huawei.

Moreover, the U.S. government has recognized that keeping software up to date is essential for safeguarding against cyberattacks, and protecting consumers from identity theft, fraudulent charges, and other cyber threats is of paramount importance. Indeed, to protect consumers against malicious attacks, the Federal Trade Commission recommends that industry ensure that "*all* mobile devices receive operating system security updates for a period of time that is consistent with consumers' reasonable expectations."[9] The ability to update devices is critical to help wireless network operators stay ahead of threats in the current rapidly changing environment. Limited engagement with Huawei to protect the security of devices in the market will continue to benefit American and global consumers. In contrast, the inability to develop, manage, and supply security updates to the millions of customers who have purchased Huawei devices – both in the United States and around the world – would create an enormous gap in security.

It is also important that the TGL continue to authorize transactions necessary to maintain and support existing and currently fully operational networks and equipment. Telecommunications networks require massive, complex, and expensive infrastructures that can contain hundreds of thousands of connected components spread throughout a network's coverage area and require the

[9] Federal Trade Commission, *Mobile Security Updates: Understanding the Issues, Commission Report February 2018* at 5, *available at*: https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf; *see also* FCC, Press Release, *FCC Wireless Telecommunications Bureau Launches Inquiry into Mobile Device Security Updates* (May 9, 2016), *available at*: https://apps.fcc.gov/edocs_public/attachmatch/DOC-339256A1.pdf; DHS, *Strategic Principles for Securing the Internet of Things (IoT)* (Nov. 15, 2016), *available at*: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

support of thousands of individual employees, contractors, and service providers. Network operators typically use multiple vendors to build and operate their networks to manage supplier concentration risk and drive competitive pricing. Even with a multiple vendor strategy, however, large areas of a network often depend on a specific vendor, such as Huawei. Huawei equipment is deployed in current generation wireless networks across the globe, and for some GSMA members, up to 90% of in-service Huawei devices contain U.S.-sourced hardware and/or software at a component level (*e.g.*, power supply units, CPUs, control boards, line cards, *etc.*). These devices are integral to a wide range of telecommunications network operations and services, and this equipment has a relatively long planning and in-use timeframe as compared to handsets and other consumer electronic devices, which make supply chain shifts much more difficult.

E. BIS Should Authorize Collaboration on Global Telecommunications Standards Setting

GSMA has consistently emphasized the importance of global standards work to promote interoperability and economies of scale. The original TGL explicitly recognized the need for collaboration on 5G and future standards in a variety of venues by authorizing limited engagement with Huawei "as necessary for the development of 5G standards as part of a duly recognized international standards body."[10] The subsequent abrupt removal of this authorization[11] has created uncertainty and hesitance that has had a chilling effect on important collaboration on technical issues necessary to develop standards and technology for publication. While GSMA appreciates BIS's August 2019 guidance on standards setting and development activities involving Huawei,[12]

---

[10] *See* U.S. Department of Commerce, Bureau of Industry and Security, *Temporary General License*, Final Rule, 84 Fed. Reg. 23468, 23471 (May 22, 2019).

[11] U.S. Department of Commerce, Bureau of Industry and Security, *Temporary General License: Extension of Validity, Clarifications to Authorized Transactions, and Changes to Certification Statement Requirements*, Final Rule, 84 Fed. Reg. 43487 (Aug. 21, 2019).

[12] BIS, *General Advisory Opinion Concerning Prohibited Activities in the Standards Setting or Development Context When a Listed Entity Is Involved* (Aug. 19, 2019), *available at:*

certain preparatory activities leading up to the creation of published standards may fall outside the confines of Section 734.7 and other carve-outs in the EAR and therefore would not be permissible without a specific license. The resulting uncertainty and reticence to engage in limited technical exchanges with Huawei necessary to develop international standards may prove particularly challenging for the development of open RAN, virtualized networks and other innovations that necessarily require input from world leaders in global technology standards.

Moreover, U.S. policymakers have recently emphasized the importance of the U.S. engaging "actively and effectively in forums setting international information and communications technology standards."[13] This depends on "robust and integrated participation from the federal government, academia, professional societies, and industry."[14] Restricting U.S. efforts is at odds with this aggressive call to strengthen U.S. participation and leadership in developing telecommunications standards, which provide the building blocks for emergent technology and enable the design and production of products that are critical to U.S. competitiveness. The White House's recently released national strategy to secure 5G networks and infrastructure similarly recognizes the importance of "preserv[ing] and enhanc[ing] United States leadership on 5G in relevant organizations that set standards in concert with the private sector, including . . . commercial, academic, and like-minded international partners."[15] To that end, the United States has committed to "promote and support increased participation by the private sector

---

https://www.bis.doc.gov/index.php/documents/advisory-opinions/2437-general-advisory-opinion-concerning-prohibited-activities-in-the-standards-setting-or-development-context-when-a-listed-entity-is-involved/file.

[13] *Cyberspace Solarium Commission Report*, Recommendation 2.1.2 (March 2020), *available at* https://www.solarium.gov/report.

[14] *Id.*

[15] Office of the President, *National Strategy to Secure 5G of the United States of America* (March 2020), at 6.

and ensure that such participation is informed by appropriate public-private coordination."[16] BIS should reinstate the TGL's standards setting authorization to facilitate these important objectives. Importantly, however, this authorization should not be limited to the development of 5G standards, since the expansion of 4G and LTE will remain a global priority in the coming years for a number of reasons. First, many parts of the world have not yet fully deployed 4G, and they will need to do so on their path to 5G. As McKinsey reports, many global "operators will still have to upgrade their 4G networks to cope with growing demand" in the run up to 5G.[17] Second, 5G does not represent a brand new technology that renders 4G obsolete: "Like 4G, 5G is not going to be a flash cut. Instead, 5G will evolve side by side with 4G, with logical evolution phases taking place over the next decade."[18] McKinsey explains that "elements of current 5G technology build on 4G networks, rather than representing a complete departure—and that means mobile operators can take an evolutionary approach," for example, "by upgrading the capacity of their existing 4G macro network by refarming a portion of their 2G and 3G spectrum."[19] 5G is building on and will be heavily integrated with 4G and earlier technologies, ensuring as little disruption to customers as possible. Building out 4G networks does not present national security concerns, and thus BIS should consider how to make sure that the entity listing does not inadvertently stifle 4G deployment and maintenance.

---

[16] *Id.*

[17] McKinsey & Company, *The road to 5G: The inevitable growth of infrastructure cost* (Feb. 2018), https://www.mckinsey.com/industries/telecommunications/our-insights/the-road-to-5g-the-inevitable-growth-of-infrastructure-cost.

[18] Shane McClelland, Vice President, Strategy and Business Development, Head of Transport at Ericsson blogpost, *5G transport security: What service providers need to evolve?*, https://www.ericsson.com/en/blog/2019/7/5g-transport-security-what-service-providers-need-to-evolve-part1.

[19] McKinsey & Company, *The road to 5G: The inevitable growth of infrastructure cost* (Feb. 2018), https://www.mckinsey.com/industries/telecommunications/our-insights/the-road-to-5g-the-inevitable-growth-of-infrastructure-cost.

Accordingly, and given the interrelationship between earlier telecommunications technologies and nascent technologies, BIS should ensure that the reinstated authorization expressly covers transactions that are **"in furtherance of or for the development of global telecommunications standards as part of a duly recognized international standards body."** We urge BIS to clarify the rules of the road for companies participating in standards work. GSMA would be happy to brief BIS on standards work so that it can evaluate what steps are needed to ensure that innovators in the United States can be part of standards work while protecting the integrity of their innovations.

* * *

For the foregoing reasons, GSMA urges BIS to extend the TGL for a period of at least 18 months to permit vital transactions necessary to continue to operate and maintain existing telecommunications network equipment and to provide security updates and repairs to customers with Huawei handsets and other devices. GSMA also requests that BIS reinstate and clarify the authorization permitting exchanges in furtherance of or for the development of global telecommunications standards as part of a duly recognized international standards body. Now more than ever it is essential that BIS's actions foster predictability and stability and limit any disruptions to the availability and quality of communications around the world.