August 16, 2019

Ms. Nazakhtar Nikakhtar
Acting Under Secretary for Industry and Security
Bureau of Industry and Security
Department of Commerce
1401 Constitution Avenue, N.W.
Washington, D.C. 20230

Subject: The Temporary General License

Dear Under Secretary Nikakhtar:

The U.S. Chamber of Commerce welcomes the Bureau of Industry and Security's (BIS') May 22, 2019, rule that created the Temporary General License (TGL).[1] It authorizes certain transactions with a specific foreign company and its affiliates (collectively, covered companies or entities) that were added to the BIS Entity List on May 16, 2019.[2] The TGL is set to expire on August 19, 2019.

The decision by BIS to apply the TGL to 4 categories of transactions (which are discussed on pages 2–4 of this letter) between U.S. firms and the covered entities was constructive from economic and security perspectives. The determination also spared many U.S. businesses from having to file multiple export license applications with the agency. The Chamber wants to acknowledge BIS' action and would appreciate discussing the TGL and related issues with you. We also encourage BIS to continue to solicit industry feedback on the TGL in the coming weeks.

SUMMARY

The Bureau of Industry and Security's (BIS') decision to apply the Temporary General License (TGL) to 4 categories of transactions between U.S. businesses and the covered companies/entities is positive from economic and security perspectives.

The U.S. Chamber of Commerce urges BIS to renew categories 1–3 of the TGL for 12–18 months and exempt U.S. participation in standards bodies (category 4) from BIS regulations.

- The prohibition of American exports to covered companies could have unintended consequences on U.S. and other customers that rely on the availability of products and services of covered entities to operate networks and equipment.
- U.S. firms and our trading allies need a reasonable period of time to modify their commercial relationships and global supply chains in line with policy and regulatory developments.
- The Chamber urges BIS to clarify that standards development activities should be excluded from the agency's export control regulations. Assertive and sustained U.S. engagement in standards bodies is instrumental to America's security and innovative edge.

The Chamber would welcome discussing the TGL and related issues with BIS and other stakeholders.

RENEWING CATEGORIES 1–3 AND EXEMPTING CATEGORY 4 FROM REGULATION

The Chamber urges BIS to renew categories 1–3 of the TGL for 12–18 months and exempt U.S. participation in standards bodies (category 4) from BIS regulation.

First, extending categories 1–3 is warranted for a couple of reasons:

- The swift prohibition in May 2019 of U.S. business exports to covered companies could have detrimental effects on U.S. and other customers that rely on the products and services of covered entities, many of which lawfully procured components and services from American vendors prior to changes to the BIS Entity List.

- U.S. firms, as well as our trading allies, need a reasonable amount of time to adjust their commercial connections and global supply chains in line with new and emerging policy, legal, and regulatory developments. Extending the TGL pragmatically accounts for continuity and change, while prioritizing public- and private-sector security concerns.[3] Allied countries and companies need a transition period to stabilize these business relationships and supply chains, including to shift relationship dependence away from the covered companies.

Second, TGL category 4 should be clarified/revised. As currently written, the TGL restricts U.S. business participation to a subset of international standards bodies (e.g., the 3rd Generation Partnership Project, or 3GPP) and can be interpreted to preclude U.S. companies from contributing to a wider number of information and communications technology (ICT)-related standards bodies in which covered entities may participate.

The Chamber believes that BIS should clarify that standards development activities are excluded from BIS regulations tied to export controls. As drafted, the TGL would place American businesses at a severe competitive disadvantage in standards communities. This, in turn, would prevent U.S. industry from shaping the development of international standards, effectively ceding influence to foreign parties (e.g., covered companies).

The Chamber provides our thinking in greater detail on the 4 categories vis-à-vis the TGL.

Category 1: Continued operation of existing networks and equipment.[*] BIS' judgment that existing networks and equipment should be supported, if only for a transitional period, is spot on. Wireless communications systems are complex undertakings that span the globe; many contain U.S.-sourced hardware, software, and other vital components. System operators regularly rely on a mix of vendors to build and operate their networks. Still, it is common for some telecommunications providers to leverage specific providers, possibly including the covered companies that are the focus of BIS regulations. Moreover, given the global nature of telecommunications, carriers often connect with foreign entities that may utilize covered entity equipment. To best preserve the free flow of safe and reliable international communications, the TGL should be extended to afford businesses' time to modify their business ties and global supply chains.

[*] The titles of the 4 categories come from BIS in its May 22, 2019, final rule. They are not the Chamber's.

As policymakers and industry leverage the opportunities and/or tackle the challenges associated with increasing the scope and functionality of next generation wireless, it is prudent to provide foreign customers with the parts and services they require to avoid supply chain disruptions (e.g., potential network failures that could significantly affect individuals and institutions). Renewing the TGL would enable continuity and change in the marketplace and strengthen security.

Category 2: Support to existing handsets. As with maintaining networks and equipment, supporting handsets should be part of extending the TGL for a designated period of time. Handset security frequently involves key U.S. actors (e.g., wireless network operators, device manufacturers, and operating system and application service providers) collaborating to build, test, and disseminate software patches and updates. Many of these U.S.-sourced technologies are covered under BIS' new export restrictions, which could lead to unwanted consequences.

For example, handsets that lack software patches/updates can expose users to cyber risks and open gaps in wireless ecosystem security. Such outcomes are largely preventable with appropriate support and run counter to U.S. policy.[4] Much of the work needed to create security fixes is managed by the handset maker. However, devices under warranty need to be periodically repaired or replaced, including with the assistance of U.S. firms. These type of narrow transactions with covered companies should be allowed.[5]

In short, the Chamber believes that extending the TGL is warranted to safeguard consumers from risks associated with unsupported handsets. Given the rapidly changing cyber threat landscape, cutting-edge security should be an integral part of each generation of technology.

Category 3: Cybersecurity research and vulnerability disclosure. The TGL should be expanded to permit security research and vulnerability disclosure activities to continue. The U.S. cyber research community has a crucial role to play in managing security risks that impact public- and private-sector entities domestically and internationally. The Chamber is sensitive to cultivating trust and transparency in public-private cybersecurity efforts and enhancing the trustworthiness of digital products that are used globally.

Networking equipment and devices made by covered entities currently operate on a limited basis in the U.S. but more widely overseas. In the Chamber's experience, vendors typically seek to patch a product or system vulnerability to prevent criminal hackers from taking advantage of the weakness. U.S. technology companies should be permitted to help industry players (e.g., ranging from startups to critical infrastructure entities) manage network software and hardware lifecycle issues as they consider adjusting their supply chains in the medium- to long-term time frames commensurate with emerging U.S. policies, laws, and regulations.

Category 4: Engagement as necessary for development of 5G standards by a duly recognized standards body. The TGL sensibly authorizes U.S. organizations to engage 5G standards bodies. At the same time, the Chamber is troubled by company reports that some standards work is being put on hold due to uncertainties and disruptions caused by the export ban and expiring TGL.

The U.S. benefits when industry and the federal government effectively influence the development or revision of international technology standards. The smart development of international standards for 5G deployments advances U.S. commercial and security priorities by facilitating constructive outcomes—including improved interoperability, greater trust in online transactions, and

strengthened competitiveness of American products and services. There is a strong relationship between standards and innovation that BIS and the Chamber have a shared interest in promoting.[6] Assertive and sustained U.S. engagement in standards bodies is instrumental to America's economic well-being. The standards development process should continue to be industry led, open, consensus based, and balanced. Specifically, there should be meaningful involvement from a broad range of parties—including any business that is interested in participating—to prevent any single group, foreign nation, or company from dominating the decision making.[7]

Additionally, the Chamber argues the TGL should clarify that U.S. company participation in all international standards bodies is excluded from the Export Administration Regulations (EAR), notwithstanding the participation of foreign organizations of concern. Only direct transfers of controlled information to covered entities from U.S. businesses for purposes that are unrelated to standards development activities should be prohibited.

Since the ultimate goal of standards development activity features the publication of a standard(s) for any stakeholder to adopt, standards engagement should continue to be exempt from the EAR. The U.S. has much more to gain economically and security-wise from investing its time and energy in standards development organizations than sitting on the sidelines watching foreign parties take the lead.

The Chamber urges BIS to amend its TGL language to ensure that it frames engagement as necessary for the development of international standards by open standards bodies. We believe that BIS' emphasis on 5G standards is overly specific and should, instead, accommodate a broad array of recognized and transparent international standards efforts that govern current and future telecommunications, the internet, and cybersecurity. Other crucial areas of standards setting include those connected to the Internet of Things (IoT) and virtual/augmented reality.

FRAMING THE DEBATE: CULTIVATE MARKET OPTIONS AND STREAMLINE POLICIES, LAWS, AND REGULATIONS

This letter centers on the TGL. However, the Chamber would like to stress that a greater portion of the 5G debate should be framed toward cultivating innovative business approaches—such as virtualized networking technology (aka network function virtualization)—that can reduce current and/or future U.S. dependency on covered companies by leveraging a broader array of off-the-shelf ICT solutions. The discussion can constructively spotlight the importance of having an interoperable supply chain that increases market competition and vendor alternatives—outcomes that are in the interest of both industry and the administration.

Also, concerns about 5G have been directed, in part, at risks to ICT supply chains. Several industry actors are challenged by the array of congressional and executive branch 5G/supply chain policies, laws, and regulations that the business community must contend with. The Chamber supports the administration's call to reduce duplicative supply chain activities within the U.S. government.[8] (See the appendix on page 6.) We look forward to collaborating with BIS and other agencies to identify leading cyber supply chain threats and work toward sound, lasting solutions that have business buy-in.

***

Public and private organizations have been working diligently for years to establish the ICT infrastructure and policies needed to support the rollout of next generation wireless, or 5G. The advent of 5G offers stakeholders favorable circumstances to enhance network security and consumer experiences. The business community is acutely aware of enterprise-level cybersecurity threats coming from criminal groups and nation states or their proxies.

The Chamber shares the U.S. government's interest in deploying and securing 5G infrastructure domestically and globally. We agree with those who say that there is an opportunity for the public and private sectors to collaborate to both maximize the technological benefits of next generation wireless and promote the security and resilience of emerging 5G networks.

If you have any questions or need more information, please do not hesitate to contact Christopher Roberti (croberti@uschamber.com, 202-463-3100) or Matthew Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,

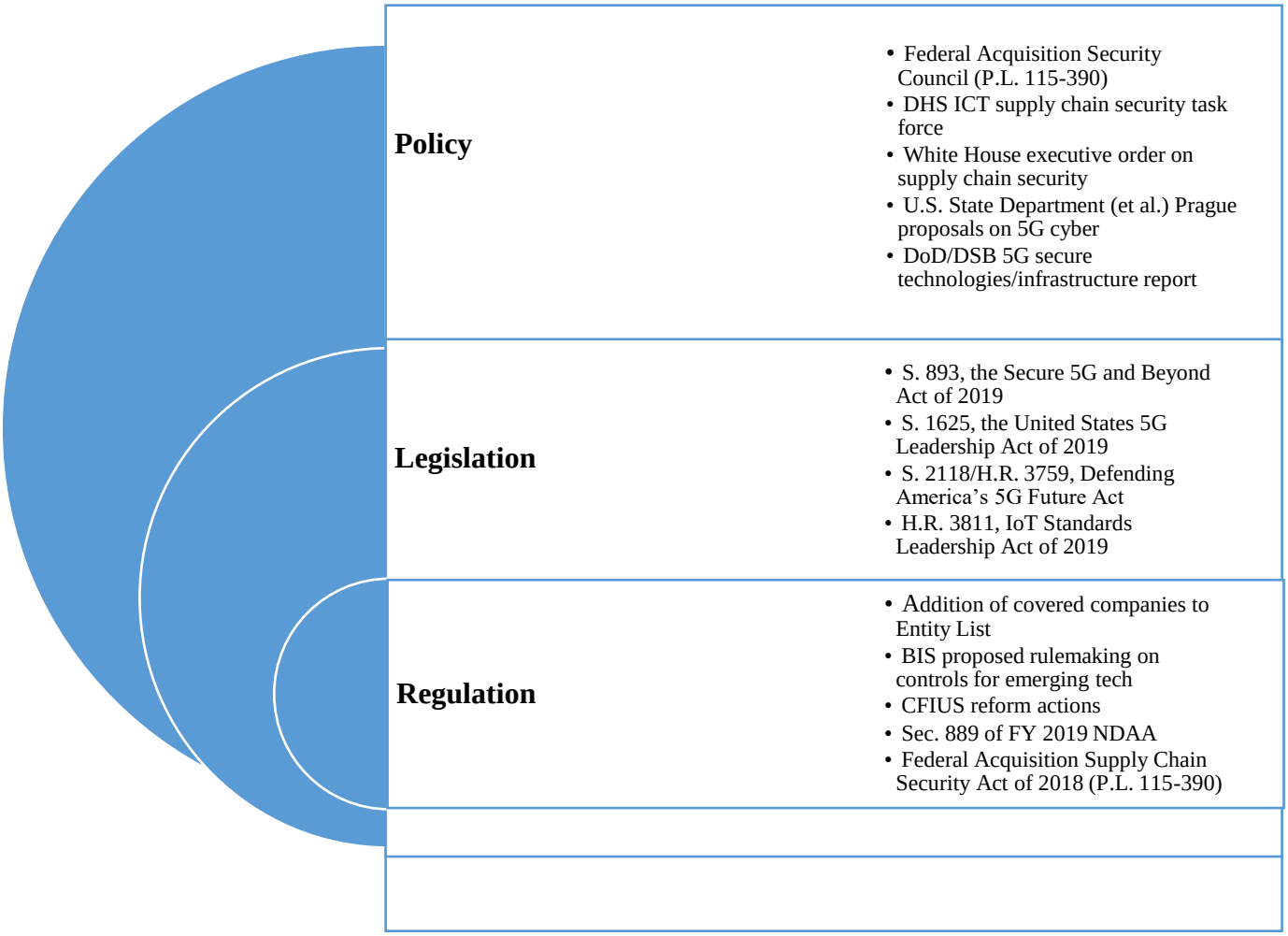
Christopher D. Roberti
Chief of Staff
Senior Vice President, Cyber, Intelligence, and Security

Matthew J. Eggers
Vice President, Cybersecurity Policy

Cc: Karen H. Nies-Vogel, Director, Office of Exporter Services, BIS

Appendix

There are dozens of policy, legislative, and regulatory security issues that relate to or overlap with 5G and supply chain matters that are beyond the scope of this letter. A sampling is provided here.



Endnotes

[1] Bureau of Industry and Security (BIS), Temporary General License, *Federal Register* (May 22, 2019). www.federalregister.gov/documents/2019/05/22/2019-10829/temporary-general-license

[2] BIS, Addition of Entities to the Entity List, *Federal Register* (May 21, 2019). www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list

[3] On April 30, 2019, the Chamber testified in the Senate on Internet of Things (IoT) cybersecurity. In response to questions about national security concerns raised by covered companies, we said that industry groups are working tirelessly alongside their federal partners (e.g., the FBI and the Department of Homeland Security) to mitigate significant threats coming from foreign adversaries and their surrogates. The Chamber noted that corporations operate in a highly competitive marketplace and conduct business worldwide. From our vantage point, a number of U.S. companies have decided not to enter into commercial arrangements with covered entities, while others have owing to powerful economic incentives. Still others are

carefully evaluating their potential exposure to covered companies and contemplating next steps, including how best to wind down existing relationships.

Also, we cautioned that the government should tread carefully when considering policies that would ban all commercial transactions between U.S. interests and covered entities. Such policies can have unintended economic consequences and may not be sustainable. The Chamber recommends bolstering the dialogue between industry and policymakers about the utility of focusing on any single threat in securing 5G.
www.commerce.senate.gov/public/index.cfm/2019/4/strengthening-the-cybersecurity-of-the-internet-of-things

[4] A February 2018 Federal Trade Commission report, *Mobile Security Updates: Understanding the Issues*, notes, "[I]ndustry should ensure that *all* mobile devices receive operating system security updates for a period of time that is consistent with consumers' reasonable expectations. Support for particular devices will, of course, vary depending on the circumstances. Reasonable security support should be a shared priority, reflected in policies, practices, and contracts throughout the mobile ecosystem" [italics in the original].
www.ftc.gov/news-events/press-releases/2018/02/ftc-recommends-steps-improve-mobile-device-security-update

[5] Department of Commerce, "Remarks by U.S. Commerce Secretary Wilbur L. Ross at the Bureau of Industry and Security Annual Conference on Export Controls and Security" (July 9, 2019).
www.commerce.gov/news/speeches/2019/07/remarks-us-commerce-secretary-wilbur-l-ross-bureau-industry-and-security

[6] National Institute of Standards and Technology (NIST), *The Role of Standards in Innovation* (July 1, 2000).
www.nist.gov/publications/role-standards-innovation

[7] NIST, *Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity* (December 23, 2015; updated November 10, 2018)
www.nist.gov/publications/interagency-report-strategic-us-government-engagement-international-standardization
www.uschamber.com/sites/default/files/september_24_2017_chamber_comments_draft_nistir_8074_intl_cyber_standardization_final.pdf

[8] The White House, *National Cyber Strategy* (September 2018).
www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf