Via www.regulations.gov/docket?D=BIS-2020-0001

April 22, 2020

Richard E. Ashooh
Assistant Secretary for Export Administration
Bureau of Industry and Security
Department of Commerce
Washington, D.C. 20230

Subject: Request for Comments on Future Extensions of the Temporary General License (TGL)

Dear Assistant Secretary Ashooh:

The U.S. Chamber of Commerce appreciates the Bureau of Industry and Security's (BIS') 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 in May 2019.[2] The latest TGL expires on May 15, 2020.[3]

The decision by BIS to apply the TGL to certain categories of transactions 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 acknowledges BIS' positive action, and we urge the agency to continue soliciting industry feedback on the TGL in the coming weeks.

Summary

The U.S. Chamber of Commerce appreciates the Bureau of Industry and Security's (BIS') temporary general license (TGL), which constructively applies to certain categories of transactions between U.S. firms and specific foreign entities. We urge BIS to consider the following points in its proposed rulemaking on future TGL extensions:

- Enable business engagement in international standards bodies.
- Make the TGL permanent to mitigate negative impacts on industry.
- Clarify that security updates (e.g., networks and handsets) are authorized.
- Revise BIS policy to enhance the effectiveness of covered transactions, including ones outside the TGL.

Moreover, the Chamber urges BIS to consider the following points in its March 12 proposed rulemaking on future TGL extensions.[4]

Enable Business Engagement in International Standards Bodies

A top Chamber priority is to receive updated guidance for businesses concerning engagement in international standards organizations. We urge BIS to publish an update to its August 2019 *General Advisory Opinion Concerning Prohibited Activities in the Standards Setting or Development Context When a Listed Entity Is Involved (AO)*.[5] The Chamber was pleased to hear BIS leadership indicate at our March 10 roundtable on technology standards development that the release of a revised AO is expected soon.

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 advances U.S. commercial and security priorities by facilitating constructive outcomes such as 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] The U.S. will compete successfully in the international standards race if U.S. industry is allowed to participate as unfettered as possible in standards bodies.[8]

Make the TGL Permanent to Mitigate Negative Impacts on Industry

BIS should consider making the TGL permanent. The current arrangement, which provides for relatively brief extensions—ranging from weeks to a few months—is not sustainable. A permanent codification of the TGL would allow companies to make long-term planning decisions, rather than focusing on short-term strategies to mitigate business disruptions and opportunity costs.

At a minimum, the Chamber urges BIS to renew TGL in 12–18 months cycles.[9] A longer extension is appropriate because of complications stemming from the coronavirus. BIS and industry have a mutual interest in facilitating reliable communications services. We want to prevent potentially handicapping overseas networks, such as those involving covered companies and where the coronavirus is spreading.

In addition, compliance with the TGL (e.g., administrative, regulatory, and legal costs) absorbs businesses' resources and diverts them from other critical initiatives. Businesses are concerned about regulatory expenses and an overall lack of programmatic certainty. Extending

the TGL permanently would empower companies to mitigate a range of potentially negative and unforeseen consequences, including the following:

- Loss of revenue from product (e.g., software and hardware) maintenance and support (e.g., cybersecurity) services.

- Negative operational impacts on customer relationships, including customers (e.g., communications companies) that rely on critical patches and updates.

- Reputational harm, owing to companies' inability to provide secure and reliable products and services.

Clarify That Security Updates Are Authorized

Networks and equipment. BIS should clearly state that security updates are authorized for devices, equipment, and systems. 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. It is common for some communications providers to leverage specific providers, possibly including the covered companies that are the focus of BIS regulations. 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 permanently extended.

Handsets. The TGL should authorize software and firmware updates, including by authorized entities using a secure and configurable mechanism. Any company that operates older versions of software may experience difficulty shifting existing systems to different hardware. 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. As with maintaining networks and equipment, supporting handsets should be part of extending the TGL.

Further, 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.[10] 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 types of narrow transactions with covered companies should be allowed.[11] The Chamber believes that putting the TGL on stable footing 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.

Revise BIS Policy to Enhance the Effectiveness of Covered Transactions, Including Ones Outside the TGL

BIS should contemplate a number of changes to its policies to make the TGL program function more effectively for transactions inside and outside its licensing regime. The security patches and bug fixes that are authorized under the current TGL are difficult to provide on devices and equipment that are not running the latest version of software because, under the TGL, companies are also constrained to deploy newer versions that may have enhanced functionality as well. If communications companies are required to operate using older versions of software (owing to export controls), which is connected to newer technology, network stability would be further strained. Thus, BIS should permit upgrades to newer versions of software to enable communications companies to operate their networks more effectively.

The security enhancements that are authorized under the current TGL are more difficult to provide on older hardware. Software companies typically fix security issues and vulnerabilities in the latest version of software and urge customers to upgrade to the latest version through remote (e.g., network download) and/or local means (e.g., removable media). Prior software releases are often not tested from a hardware integration point of view and need to be handled manually, including in situations with covered companies, where upgrading to newer releases is not permitted by law and/or regulation.

BIS should create a new category that authorizes businesses to share technology with covered entities for the purpose of troubleshooting problems on behalf of communications companies and joint customers/end users. Limitations on businesses' ability to jointly offer support causes delays in maintenance and assistance to critical infrastructure. The Chamber believes that BIS should support contract arrangements between a covered company and a third-party communications provider that are compliant with certification requirements. This way, appropriate upgrades can be made to networks and equipment without needing to get a copy of the contract from each communications provider/end user that will receive the same upgrade.

In addition, if communications providers are compelled to switch to nonstandard hardware, software companies would be required to develop and/or certify the new hardware, which would take substantial time and resources. Policymakers' interest in switching to hardware and infrastructure of noncovered entities should be balanced against the effects (e.g., compatibility, certification, and stability issues) that such a transition would have on the software that would run on new hardware.

***

Thank you for the opportunity to comment on BIS' proposed rule, especially the additional time afforded to stakeholders. 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

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] BIS, Temporary General License: Extension of Validity, *Federal Register* (March 12, 2020). www.federalregister.gov/documents/2020/03/12/2020-05190/temporary-general-license-extension-of-validity

[4] BIS, Request for Comments on Future Extensions of Temporary General License (TGL), *Federal Register* (March 12, 2020). www.federalregister.gov/documents/2020/03/12/2020-05194/request-for-comments-on-future-extensions-of-temporary-general-license-tgl

[5] 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

[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] Several U.S. senators recently wrote to administration officials urging them to issue regulations as soon as possible to confirm that U.S. participation in 5G standards-setting is not restricted by export control regulations. “It is critical for U.S. companies to participate fully in these standards-setting bodies to ensure that their technologies are represented in the standards,” the senators said. See Sen. Marco Rubio press release, “Rubio Joins Colleagues in Urging Administration to Issue 5G Regulations” (April 14, 2020).

www.rubio.senate.gov/public/index.cfm/press-releases?id=423B6F3E-5BCF-4BDE-88CD-25FD45145D4B

See the Cyberspace Solarium Commission report (March 2020) on international standards, pp. 18, 49, and 51.
www.solarium.gov/report

[9] www.uschamber.com/sites/default/files/10-15-19_uscc_comments_sec_889_ir_final_v1.0.pdf

[10] 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

[11] 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