

BIS Considers Export Controls on Neurotechnology and Adds New Controls on Genetic Sequencing Software and Intrusion Software

by Lawrence Ward, Dave Townsend, and T. Augustine Lo

The U.S. Commerce Department's Bureau of Industry and Security ("BIS") has said it is contemplating new export controls on certain neurotechnology items and has adopted new controls on genetic sequencing software and intrusion software in a series of announcements. Under the Export Administration Regulations ("EAR"), BIS imposes export controls on an item-specific basis with export license requirements applying on a country-by-country basis, depending on the national security and foreign policy concerns associated with the items. An export under the EAR includes actual release or shipment of an item from the United States to another country but also includes providing controlled technology or source code to foreign persons, including employees of businesses, in the United States.

Companies whose operations involve neurotechnology, genetic sequencing software or intrusion software should examine these new export controls to see if export license requirements may apply to provide such newly-controlled software or technology to non-U.S. destinations or to foreign persons in the United States.

Potential Neurotechnology Controls.

On October 25, BIS announced that it is considering new export controls on Brain Control Interface ("BCI") hardware and technology. In its advanced notice of public rulemaking ("BCI Notice"), BIS asks for public comments on the scope and extent of these potential controls and whether they should be aligned with export controls implemented by international allies. Public comments are due to BIS on December 10, 2021. BIS has posed a series of questions for public comment (see below). BIS states that it seeks to identify whether BCI could provide U.S. adversaries with "a qualitative military or intelligence advantage." BIS defines BCI as a "direct communication pathway between an enhanced or wired brain and an external device" that can translate commands to control machines, communicate with other humans, or assess or enhance human functioning.

Related People

- Lawrence Ward
- Dave Townsend
- T. Augustine Lo

Related Capabilities

- International Trade
- National Security Law
- Emerging Companies
- China
- Technology

Although BIS does not yet propose any specific export controls on BCI, it seems likely the BCI Notice is intended to result in the creation of such BCI export controls in the near future. BIS issued the BCI Notice under the Export Control Reform Act of 2018 (“ECRA”), which directs BIS to establish new export controls on emerging and foundational technologies. BIS had originally requested public comments on what items should be considered within “emerging technologies” in November 2018 and specifically identified BCI as a potential emerging technology that is essential to U.S. national security. In response, BIS received 13 comments that discussed BCI. Most of the comments expressed concern over potential BCI export controls harming U.S. business interests (e.g., in artificial intelligence for automobiles or by providing an advantage to non-U.S. businesses that may not be subject to such BCI controls).

BIS therefore seems intent on creating some form of BCI export controls, although it is too early in the federal rulemaking process to predict what those controls ultimately will look like. However, BIS has posed a series of questions for public comment and response:

- (1) What specific uniform standards for BCI technology would need to be adopted to ensure their application on a global basis (i.e., as international standards for BCI technology)?
- (2) Where does the development of BCI in the United States stand with respect to other countries (e.g., is the United States on the forefront of BCI technology development)?
- (3) Is BCI technology currently available for commercial use in certain foreign countries and, if so, where and for what specific purposes (e.g., have foreign companies already developed devices or chips for specific commercial applications)?
- (4) Has the current stage of development with respect to invasive and/or non-invasive BCI technology reached the point at which such technology is ready for commercial production and use?
- (5) Is the main progress with respect to non-invasive brain signal sensors being made in terms of real-time algorithms designed to transform neural signals into commands (i.e., what is developing faster: “software” (algorithms) or hardware (sensors))?
- (6) What impact would the establishment of export controls on BCI technology have on U.S. technological leadership (i.e., not only in the field of BCI technology, but overall) and would this impact be distinctly different if controls were placed primarily on “software” as opposed to hardware, or vice versa?
- (7) How is the future development of artificial intelligence (AI) technology or other emerging technologies likely to impact the development of BCI technology, or vice versa?
- (8) What types of ethical or policy issues are likely to arise from the use of BCI technology (e.g., for medical or military purposes)?

(9) What kinds of risks and benefits currently exist, or are likely to arise, as a result of the application of BCI technology?

(10) What are the potential advantages or disadvantages of using invasive and noninvasive BCI chips/sensors and related “software” (e.g., algorithms for signal processing) for specific applications? To what extent would these advantages or disadvantages correspond (or differ) based upon whether invasive or non-invasive BCI chips/sensors and related “software” were being used?

(11) Are there any BCI technologies that are significantly more vulnerable than others to cybersecurity threats (e.g., military systems employing BCI technologies that could adversely impact U.S. biodefense)?

(12) What is the potential for transmitted BCI data to be hacked or manipulated to influence the user or machine? Is such data inherently more vulnerable to hacking or manipulation than other forms of data? Would the invasive or non-invasive characteristics of BCI data have any impact on the potential vulnerability of such data?

New Genetic Sequencing Software Controls.

On October 5, 2021, BIS published new narrowly drawn export controls on certain genetic sequencing software. These new export controls, like the BCI Notice discussed above, also were published as part of BIS’s review of “emerging technologies” under the ECRA. However, unlike the proposed controls under the BCI Notice, the new controls on genetic sequencing software already are in effect (as of October 5, 2021).

The BIS export controls on genetic sequencing software build on existing controls that cover genetic sequencing assemblers and synthesizers that are automated and can generate continuous nucleic acids greater than 1.5 kilobases in length with error rates less than 5% in a single run. Such automated assemblers and synthesizers are controlled under Export Control Classification Number (“ECCN”) 2B352.j. In its new export controls, BIS will control software designed for the automated assemblers and synthesizers in ECCN 2B352.j if such software is capable of designing and building functional genetic elements from digital sequence data the new ECCN 2D352. In addition, technology for the development of such ECCN 2D352 software will now become subject to the existing controls under ECCN 2E001.

The new controls implemented by ECCNs 2D352 and 2E001 are designed to prevent the export of software and related technology that can be used to generate certain pathogens and toxins without the need to acquire controlled genetic elements and organisms themselves. BIS noted in issuing these new controls that instructions for creating harmful pathogens and toxins could, accordingly, be manufactured by using 2D352 software, thereby escaping any current export controls that only cover the synthesizers and assemblers as hardware items.

BIS wanted to extend current export controls to cover any such software that is subject to the jurisdiction of BIS under the EAR. As of October 5, 2021, export licenses are

required to export genetic sequencing software controlled under ECCN 2D352 to countries indicated under the Country Chart in Supplement No. 1 of EAR Part 738 and its chemical and biological weapons column two or “CB2” controls. The CB2 controls apply to numerous countries such as China and Russia.

New Intrusion Software Export Controls.

Finally, and separately, BIS published new controls covering intrusion software designed for malicious cyber activities and network surveillance. BIS is still accepting public comments on the rule until December 6, 2021, although the controls will become effective on January 19, 2022. BIS is adding three new ECCNs – 4A005, 4D004, and 4E001.c – to control malicious software and related hardware and technology. All of the new controls target “intrusion software,” defined as software designed to “avoid detection by monitoring tools, or to defeat protective countermeasures, of a computer or network-capable device,” and that can: (a) extract of data or information from a computer or network-capable device, or modify a system or user data; or (b) modify the standard execution path of a program or process in order to allow the execution of externally provided instructions. However, the term intrusion software does not include any of the following: Hypervisors, debuggers or Software Reverse Engineering (SRE) tools; Digital Rights Management (DRM) software; or Software designed to be installed by manufacturers, administrators or users for the purposes of asset tracking or recovery.

At the same time, BIS also published a new license exception, Authorized Cybersecurity Exports (“ACE”), to permit limited exports of intrusion software. BIS explained that the new ACE license exception is “necessary to avoid impeding legitimate cybersecurity research and incident response activities.” ACE allows exports to most destinations, except to destinations embargoed under U.S. law, or to government end-users of certain countries, such as Russia. ACE is intended to address concerns of the private sector that the new export controls on intrusion software could also reach items intended merely to test cybersecurity defenses or to remedy detected security breaches.

BIS had originally proposed new controls on certain intrusion software in 2015, which resulted in more than 300 comments from industry. Most of those comments opposed the proposed controls as overly broad, potentially burdensome, and sweeping in numerous common software programs and anti-intrusion software that were not the intended targets of the controls. As a result of such strong industry opposition, BIS significantly scaled back these new intrusion software controls to those described above and also added the new ACE license exception.

Dorsey’s attorneys can assist companies with assessing the potential impact of the export controls discussed above. For additional information, please feel free to contact the attorneys listed, or see Dorsey’s website at www.dorsey.com.