International Trade Alert

Akin Gump
STRAUSS HAUER & FELD LLP

BIS Has New Authorities to Impose Controls over Activities of US Persons in Support of Foreign Military, Security, or Intelligence Services

January 5, 2023

Key Points

- The Export Control Reform Act of 2018 has been amended to give BIS the authority to regulate services and other activities of U.S. persons, wherever located, when in support of foreign "military, security, or intelligence services"— even if no commodities, software or technologies subject to the EAR are involved.
- The House and Senate sponsors of the one-sentence amendment stated that its purpose is "to prevent Americans from working with or aiding foreign police and intelligence agencies that spy on dissidents, on journalists, and on American citizens . . . and represents the largest expansion of presidential export control authority in several years."
- BIS has not announced how or when it plans to implement in the EAR its new authority, or against which countries new controls on U.S. person services and other activities will apply.

Background – There Are Three Types of Export Controls: List-Based, End-User and End-Use Controls

There are three types of export controls in the Export Administration Regulations (EAR) and all other export controls. The most commonly understood type of control are those over specific commodities, software and technologies ("items") that are, for example, necessary for the development, production or use of weapons of mass destruction (WMD) or conventional weapons. This first type of control is referred to as a "list-based" control because these items are identified in lists of controlled items such as the Commerce Control List (CCL).

The second type of export control is over exports of unlisted items to specific end users. The most well-known "end user" control is the Entity List, which the Department of Commerce's Bureau of Industry and Security (BIS), as now named, began publishing in 1997 "to inform exporters of some of the organizations and companies that may be involved in proliferation activities" as part of the 1990s-era Enhanced Proliferation Control Initiative (EPCI). Although its scope and use have evolved

Contact Information

If you have any questions concerning this alert, please contact:

Kevin J. Wolf
Partner
kwolf@akingump.com
Washington, D.C.
+1 202.887.4051

Shiva Aminian
Partner
saminian@akingump.com
Los Angeles
+1 310.552.6476

Anne E. Borkovic
Partner
aborkovic@akingump.com
Washington, D.C.
+1 202.887.4432

Jingli Jiang
Partner
jjiang@akingump.com
Beijing
+86 10.8567.2229

Jaelyn Edwards Judelson
Partner
jjudelson@akingump.com
Los Angeles
+1 310.552.6477

Susan M.C. Kovarovics
Partner
skovarovics@akingump.com
Washington, D.C.
+1 202.887.4088

Kimberly M. Myers
Partner
kmyers@akingump.com
Washington, D.C.
+1 202.887.4423

Chris Chamberlain
Counsel
cchamberlain@akingump.com
Washington, D.C.
+1 202.887.4308

considerably since 1997, it is still limited in application to the export, reexport or transfer of items "subject to the EAR," which is a term that describes items and activities over which BIS exercises regulatory jurisdiction under the EAR.[1]

The third type of control, also created as part of EPCI, is an "end use" control, which imposes licensing obligations over activities of a person or a company involving unlisted items and unlisted end users. One type of end use control in the EAR is that which regulates the export, reexport or transfer by U.S. or foreign persons, wherever located, of items subject to the EAR, whether listed or unlisted, if in support of the development or production in specific countries of nuclear applications, missiles (including UAVs), chemical and biological end uses and maritime nuclear end uses. These end-use and end-user controls are referred to as "catch-all" controls. BIS created during the Bush administration controls over a list of otherwise uncontrolled items subject to the EAR if for military end uses in China. The scope of this military end use control has evolved considerably, but it is also limited in application to specific items "subject to the EAR."

The EAR Also Have End-Use Controls over Activities of U.S. Persons When the Underlying Items Are Not Subject to the EAR

Since EPCI, the EAR's end-use controls have also regulated activities of U.S. persons[2] involving the production or development of weapons of mass destruction in specific countries—even when none of the items involved are subject to the EAR. Since 1996, these U.S. person end-use controls have been codified, as amended, in EAR sections 744.6(b)(1) (if for nuclear explosive devices), 744.6(b)(2) (if for missiles), 744.6(b)(3) (if for chemical/biological weapons) and 744.6(b)(4) (if for chemical weapons precursors).

In August 2018, Congress Expanded the Authority for EAR Controls over U.S. Person Activities

The Export Control Reform Act of 2018 (ECRA) updated the statutory authority for the EAR. ECRA maintained the status quo for the EAR's end-use controls in specific statutory provisions—ECRA sections 4812(a)(2)(A), (B), (C) and (D). Congress, however, added in to ECRA's specific end-use authorities two additional topics for which there should be controls over activities of U.S. persons—those in support of "foreign maritime nuclear projects" (subsection (E)) and those in support of "foreign military intelligence services" (subsection (F)).

The bill that eventually became ECRA used the phrase "intelligence services" in its corresponding subsection (F). How and why the modifying limiter of the word "military" was added in front of "intelligence services" when the otherwise unchanged bill became law is unclear. This unexplained change is the basis for the recent amendment to ECRA.

In January 2021, BIS Implemented Its New Authorities over U.S. Person Activities in Support of "Military-Intelligence" End Uses

In January 2021, BIS implemented its new ECRA section 4812(a)(2)(F) authority by creating new EAR section 744.6(b)(5). As a result, and as amended, the EAR prohibit U.S. persons, wherever located, to "support" without a license a "military-intelligence

Thomas Krueger
Senior Policy Advisor
tkrueger@akingump.com
Washington, D.C.
+1 202.887.4215

end use" or a "military-intelligence end user" in Belarus, Burma, Cambodia, China, Russia, Venezuela, Iran, Cuba, North Korea or Syria.[3]

BIS also expanded the scope of the EAR's end-use controls by making it so that when a U.S. person knows that its activities "will support"—as opposed to the previous parameter of "will directly assist"—a covered WMD or military-intelligence application, then the activity is controlled. BIS made this change because new ECRA section 4813(d)(1)(B) authorized it to implement controls on "activities that may support" the covered applications. The new definition of "support" is significantly broader than the previous "directly assist" phrase.

For unknown reasons, BIS has not implemented in the EAR ECRA's requirement to regulate U.S. person activities in support of "foreign maritime nuclear projects."

The EAR's U.S. Person Controls Include Controls over Services Provided by U.S. Persons

A common misunderstanding is that the EAR only control the export, reexport or transfer of commodities, software and technology. The only services, the thought often goes, that are controlled as such by export control regulations are "defense services" the International Traffic in Arms Regulations (ITAR) regulate. Although this distinction is usually correct, the EAR indeed do control provision by U.S. persons of services even when there are no items subject to the EAR involved.

The first of these EAR service controls, and relevant to this alert, is a function of the EAR's broad definition of "support" in section 744.6(b)(6), which means:

1. "Shipping or transmitting from one foreign country to another foreign country any item not subject to the EAR you know will be used in or by any of the [covered catch-all] end uses or end users . . . including the sending or taking of such item to or from foreign countries in any manner;
2. Transferring (in-country) any item not subject to the EAR you know will be used in or by any of the [covered catch-all] end uses or end users;
3. **Facilitating** such shipment, transmission, or transfer (in-country); or
4. **Performing any contract, service, or employment** you know may assist or benefit any of the [covered catch-all] end uses or end users . . . including, but not limited to: Ordering, buying, removing, concealing, storing, using, selling, loaning, disposing, servicing, financing, transporting, freight forwarding, or conducting negotiations in furtherance of."

Thus, for example, the EAR impose licensing obligations on the provision by U.S. persons of any type of service that they know could "assist or benefit" something described in section 744.6, which will presumably include in 2023 foreign military, security and intelligence services in specific countries. Such new prohibitions could also include prohibitions on financing or even on conducting negotiations for the possible provision of services. Most think of such broad prohibitions on even conducting negotiations for an activity to be the type of prohibition the sanctions regulations the Treasury Department's Office of Foreign Assets Controls (OFAC) administer.

With respect to the prohibition on "facilitating" exports, reexports and transfers by others, BIS has not defined the term. In the context of the recent China-specific rules

pertaining to semiconductor- and computing-related applications, however, BIS interpreted it and related "support" terms in section 744.6(c)(2) to be, with respect to foreign-made items not subject to the EAR, limited to (i) authorizing such shipments, (ii) conducting such shipments, or (iii) servicing such items. This is far narrower than OFAC has interpreted the term.

Another services-specific prohibition in the EAR is that no person, whether U.S. or foreign, may, among other things, service any item that has been or about to be involved in a violation of the EAR. The EAR's prohibitions on acting with knowledge of a violation are described in EAR section 764.2(e), which overlaps in scope the EAR's General Prohibition 10.

In October 2022, BIS Expansively Used Its Authority to Impose Controls over U.S. Person Activities with Respect to Controls Against China's Advanced Node Semiconductor Industry

The EAR also give BIS the authority to inform U.S. persons that their activities could be in support of covered end uses, even without their knowledge, and that, therefore, a license is required for regulated activities. This is informally referred to as the "is informed" process. In October 2022, BIS took the unprecedented step of using this process to inform not just specific companies of new controls in a confidential letter, but rather to inform via regulation all U.S. persons of a new licensing obligation. Specifically, BIS informed all U.S. persons, corporate and individual, that their activities directly or indirectly in support of the development or production of advanced node semiconductors in China require a license. These new controls apply to U.S. person activities involving both items that are not subject to the EAR and to those that are. BIS stated that the policy basis for this new U.S. person control was that the Chinese government and companies in China could use advanced node semiconductors developed or produced in China to develop or produce in China WMD or to support military-intelligence end users. U.S. persons, BIS stated, may not always know of such end uses because the "PRC government expends extensive resources to eliminate barriers between China's civilian research and commercial sectors, and its military and defense industrial sectors. It also is developing and producing advanced integrated circuits (packaged or unpackaged) for use in weapons systems."

In December 2022, Congress Expanded BIS's Authority to Impose Controls over Activities of U.S. Persons in Support of Foreign Military, Security or Intelligence Services

On December 23, 2022, President Biden signed into law the National Defense Authorization Act for Fiscal Year 2023 (NDAA). Congress added to the NDAA section 5589(b) to amend ECRA section 4812(a)(2)(F) by inserting the words and punctuation "security, or" before "intelligence." The amendment is a one-sentence change, adding to ECRA only two words in a 4,408-page bill—and the only change to ECRA. Although the amendment was added without substantive references in any congressional hearings, summaries or statements, the same amendment to other legislation had been proposed in recent years four times. (Apparently, the previous efforts failed for reasons unrelated to the substance of the amendment.)

As a result of the NDAA amendment, BIS now has the clear[4] statutory authority to create and impose controls on the activities of U.S. persons, wherever located, in "support" of "military, security, or intelligence services"—even when

all the underlying items at issue are not subject to the EAR. The Biden-Harris administration has not stated how or when it plans to implement in the EAR its new authorities to regulate U.S. person activities in support of military, security or intelligence services.

However, in a press release issued by Congressman Tom Malinowski (D-NJ), multiple members of Congress, Republicans and Democrats made the following statements about their policy objectives for the amendment:

- Congressman Malinowski and Senator Wyden (D-OR) stated that the amendment will "prevent Americans from working with or aiding foreign police and intelligence agencies that spy on dissidents, on journalists, and on American citizens." The amendment "represents the largest expansion of presidential export control authority in several years."
- Congressman Malinowski stated that "Americans should not be helping foreign dictatorships spy on their political opponents or on our own citizens . . . . This new law gives the President the authority to treat the export of sophisticated hacking tools and expertise just as we treat the export of sensitive military technology, to make sure it doesn't fall into dangerous hands."
- Sen. Wyden (D-OR) stated that "American technology shouldn't be used to help authoritarians spy on their citizens or hack their political rivals . . . . I look forward to working with the administration to ensure that U.S.-made surveillance technology is not exported to intelligence and security agencies in countries with a record of abusing human rights."
- Sen. Cornyn (R-TX) stated: "Given the alarming increase of cyber threats to U.S. citizens, preventing American technology from falling into the wrong hands is critical to our national security . . . . This provision will strengthen the ability of the American government to deny services to foreign civilian intelligence agencies . . . ."
- Sen. Brown (D-OH) stated that "This key provision will expand our ability to deprive certain foreign national security and law enforcement services from accessing sensitive U.S. technologies. I thank my colleagues for their work on this provision and look forward to working with BIS to implement strong export controls using this new authority."
- Congressman Meeks (D-NY) stated that "Congress needs to ensure that Americans are not contributing to surveillance efforts and human rights abuses abroad."
- The press release went on to state that "Current law allows the President to block Americans from providing any services to a foreign military intelligence agency, but not to a civilian intelligence or police-type entity. In 2019, Reuters uncovered that the United Arab Emirates exploited weak controls to hire more than a dozen former U.S. intelligence operatives to hack dissidents, journalists, and Americans. Under this new law, the President could prohibitAmericans from providing support to that surveillance agency or any of the dozens of security agencies around the world that have used advanced technology -- such as the NSO Group's *Pegasus* spyware -- against journalists, human rights defenders, and opposition politicians. The law will also give the President a new tool to prevent American technologies or services from helping build China's system of mass surveillance, within and beyond its borders."

Conclusion and Next Steps

We do not know what BIS has in mind for how it will implement its new authorities or against which countries it would impose new controls. Examples of how it might use its new authorities are:

- BIS could impose controls over U.S. person activities in countries not subject to embargoes if in support of the production, development or use of less-sensitive foreign-origin military items not subject to the EAR that are also not described on the U.S. Munitions List (USML) of the ITAR. If the foreign-origin defense articles were described on the USML, then such services would already be controlled under the ITAR as "defense services." Thus, such a new control would be a"defense services-like" type of control and would apply, by definition, to services related to less sensitive foreign-origin military items.
- BIS could change the scope of Entity List-related prohibitions to include prohibitions on services provided by U.S. persons that could "assist or benefit" listed entities even when all the items involved in the services are not subject to the EAR. For example, BIS could decide that any listed entities that provide support to a company involved in the military-industrial complex of a country of concern should be subject to additional controls on activities of U.S. persons beyond the export, reexport or transfer of items subject to the EAR.
- The EAR's existing definition of "support" includes "financing." Thus, BIS could impose, through a broad "is informed" process, an outbound investment-like control prohibiting U.S. persons from "financing" activities that could "assist or benefit," directly or indirectly, the military, security or intelligence services in specific countries.
- BIS could also impose controls over U.S. person activities that support foreign internal security services engaged in human rights violations or other acts contrary to U.S. foreign policy interests. It might also impose controls on U.S. person support of foreign intelligence agencies. BIS states on its website that it is "actively engaged in formulating, coordinating, and implementing various export controls to counter the use of items subject to the [EAR] that could enable human rights abuses or repression of democracy throughout the world. These controls are a mix of list-based, end-user, and **end-use controls**, as well as specific licensing policies that allow review of transactions for concerns about human rights abuses and repression of democracy."
- To get a sense for some of the human rights-related issues BIS might want to help address through new prohibitions on U.S. person services and other activities, one could read the State Department's "Guidance on Implementing the 'UN Guiding Principles' for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities." It contains guidance for U.S. businesses "seeking to prevent their products or services with surveillance capabilities from being misused by government end-users to commit human rights abuses."

We do not know the timing of any possible new controls. One possibility is that there might be a new regulation published in connection with the second Summit for Democracy, which is scheduled to occur in March 2023. In any event, no new licensing or due diligence obligations will exist until BIS publishes amendments to EAR section 744.6 to implement its new authority. Whether BIS will publish such new controls as proposed rules seeking public comment or as final rules is unknown.

When new end-use controls are eventually imposed, they will certainly impose new end-use screening obligations on U.S. persons engaged in activities outside the United States. End-use controls, by definition, are not limited to regulating exports of specific identifiable items going to specific destinations. As with current end-use controls against WMD and conventional military applications in various countries, and against advanced node semiconductor development or production in China, U.S. companies and others will need to set up internal compliance systems to determine when they have knowledge of such end uses and are otherwise able to spot "red flags" that require additional compliance efforts.

[1] Items are "subject to the EAR" if they are (i) U.S.-origin, (ii) exported from the U.S., (iii) foreign-made and containing more than a de minimis amount of controlled U.S.-origin content, or (iv) the direct product of specific types of U.S. technology, software or equipment. Foreign-made items outside the United States not subject to the EAR's de minimis or direct product rules are not "subject to the EAR."

[2] The EAR define in section 772.1 "U.S. person" as meaning: (i) U.S. companies and other entities incorporated in the U.S. and their foreign branches; (ii) individuals, wherever located and regardless of the nationality of their employer, who are U.S. citizens, permanent legal residents, or refugees and asylees in the United States; and (iii) any company or individual in the United States. Foreign persons outside the United States are also affected by U.S. person controls if they are acting for and on behalf of the U.S. person.

[3] A "military-intelligence end use" is defined as the development, production, operation, installation, maintenance, repair, overhaul or refurbishing of, or incorporation into, military items, "which are intended to support the actions or functions of a military-intelligence end user." A "military-intelligence end user" is defined as being "any intelligence or reconnaissance organization of the armed services (army, navy, marine, air force or coast guard); or national guard."

[4] BIS arguably had the authority to impose such end-use controls under its broad authority in ECRA section 4813(a)(16) to "undertake any other action as is necessary to carry out this subchapter that is not otherwise prohibited by law." For reasons unknown, it did not use this authority when it implemented new end-use and end-user controls in January 2021.

akingump.com