October 15, 2024

Sharron Cook, Senior Export Policy Analyst
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, D.C. 20230

BIS-2024-0029 Proposed Rule "End-Use and End-User Based Export Controls, Including U.S. Persons Activities Controls; Military and Intelligence End Uses and End Users" (RIN 0694-AJ43)

BSA | The Software Alliance appreciates the opportunity to offer the following comments in response to the Bureau of Industry and Security's ("BIS" or "the Bureau") proposed rule, "End-Use and End-User Based Export Controls, Including U.S. Persons Activities Controls; Military and Intelligence End Uses and End Users" ("MEU rule").

I. Introduction

BSA is the leading advocate for the enterprise software industry before governments and in the international marketplace.[1] Enterprise software—or business-to-business (B2B) software—enables the commercial operations of other companies. It helps organizations of all sizes and across all industries operate more safely and efficiently, enhance product and service development, and increase opportunities to innovate and grow. By offering trusted and responsible software solutions to support their business clients' needs, enterprise software companies enable other organizations to service their own customers in turn.[2]

BSA strongly supports the Bureau's mission of advancing US national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system.[3] This includes the Bureau's development of controls to "stem the proliferation of weapons of mass destruction and the means of delivering them, to halt the spread of weapons to terrorists or countries of concern, and to

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Cohere, Databricks, DocuSign, Dropbox, Elastic, EY, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

[2] BSA, How Enterprise Software Empowers Businesses in a Data-Driven Economy, at: https://www.bsa.org/files/policy-filings/011921bsaenterprisesoftware101.pdf

[3] https://www.bis.doc.gov/index.php/about-bis/mission-statement

further important US foreign policy objectives." BSA also welcomes the Bureau's commitment to ensuring that its "regulations do not impose unreasonable restrictions on legitimate international commercial activity that is necessary for the health of US industry," and its commitment to avoiding "actions that compromise the international competitiveness of US industry without any appreciable national security benefits."

Finally, BSA supports the Bureau's "partnership with the private sector"; its openness to "public-private partnerships and market-based solutions"; and its recognition that US security and continued US technology leadership are mutually supportive. In respect of the Bureau's activity over the past 12-18 months, BSA offers three general recommendations:

- First, we encourage the Bureau to be cognizant of the challenges created by the incremental expansion of increasingly complex license requirements. Such complexity and a lack of legal clarity impacts business continuity and jobs.

- Second, we encourage the Bureau to include industry stakeholders in its deliberations regarding future controls as early as possible in the process. US export controls have evolved very rapidly in recent months, with many new controls being proposed in rapid succession. The range and frequency of these updates creates an increased risk of unintended consequences. Such engagement is also important from an economic perspective, as commercial commitments in any supply chain business model are made many months, or even years, in advance. These may include new investments in real estate, digital infrastructure, and complex contractual arrangements with new product and service suppliers.

- Third, in this dynamic and evolving environment, we encourage the Bureau to seek to institutionalize greater engagement with US allies and partners. Such engagement is a critical component of ensuring that new controls and restrictions are focused and effective. To avoid unintended impacts, it is important to ensure that US and allied export controls are as coordinated and consistent as possible.

II. Discussion

According to BIS, the proposed revisions and additions to the EAR's end-use, end-user, and ''U.S. persons'' activity controls would purportedly implement expanded Export Control Reform Act of 2018 (ECRA) authority to control certain ''U.S. persons'' activities under the EAR. Specific to the EAR's ''U.S. persons'' activities controls, BIS is proposing amendments to control 'support' furnished by ''U.S. persons'' to military end users and military-production activities, as well as intelligence end users that are not otherwise already regulated under or prohibited by U.S. law. In addition, BIS is proposing to revise the definition of 'support' set forth in the EAR's ''U.S. person'' activity control provision in response to requests by the public for clarification. According to BIS, the revisions of controls on military and intelligence end users and end uses, and the creation of four categories of end-users – (Military End User (MEU), Military Support End User (MSEU), Intelligence End User (IEU) and Foreign-Security End User (FSEU)) – would further the national security and the foreign policy of the United States.

A. Controls on US Person Activities

The unilateral nature of US person controls, particularly in relation to foreign origin items and activities outside the United States, significantly disadvantages US companies and individuals by fueling perceptions of unreliability amongst non-US business partners. The impact of these expanded controls will be increasingly difficult to quantify due to lost opportunity costs but will clearly exceed the original intent of the ECRA.

US persons, including natural persons, will also increasingly vulnerable to retaliatory controls. As a retaliatory mechanism, U.S. persons including natural persons may be confronted with disparate enforcement of local laws and regulations where they may not be afforded due process protections.

The proposed rule does not differentiate between natural persons and entities even when a natural person is working for a U.S.-headquartered entity. Additionally, the scope of these proposed controls extends beyond what has already been adopted by BIS with respect to the development and production of advanced node integrated circuits and associated semiconductor manufacturing equipment; a natural person would be captured regardless of where located or the nationality of their employer. This unfairly disadvantages individuals and risks having U.S. technological talent falling behind in global leadership due to shrinking opportunities.

We recommend that BIS take steps to ensure that any proposed controls on US persons activities rely on uniform understanding and compliance with the term "support" as defined by BIS. BSA seeks clarity, consistency and restraint in implementation controls with appropriate consideration of the risks of retaliatory controls and sanctions.

B. End-User and End-Use Controls

The proposed rule seeks to expand existing Military End Use/End-User and Intelligence End-Use/End-User controls, increasing the challenge of due diligence and end user determinations for regulated US entities. We outline below several of the due diligence and identification challenges that we anticipate US entities will face in seeking to comply with the proposed rules. We would ask BIS to seek to clarify the following questions.

1. Military Hospitals

Are military hospitals considered to be MSEUs? Does it matter if the Hospital is a military unit? For example, is the Royal Cambodian Armed Forces (RCAF) Institute of Health Sciences (a state institution) considered to be an MSEU when their defined roles and responsibilities include:

- Examination and treatment for civilian students
- Check and treat the staff of the whole institute
- Check and treat local people free of charge
- A place to provide student practice
- Cooperate with the Ministry of Labor to obtain the National Social Security Fund (NSSF) to contribute to poverty reduction.

We do not believe military hospitals are MSEUs because per the definition in §744.22.f, MSEU means any person or entity whose actions or functions support 'military end uses' as defined in §744.21. 'Military end use' is defined in §744.21.f as:

> Military end use means incorporation occurring outside the United States into a defense article described on the U.S. Munitions List (USML) (22 CFR 121.1, International Traffic in Arms Regulations); incorporation into items classified under Export Control Classification Numbers (ECCNs) under "600 series" ECCNs; or any item that supports or contributes to the operation, installation, maintenance, repair, overhaul, refurbishing, "development," or "production," of defense articles described on the USML, or items classified under ECCNs under"600 series" ECCNs.

Military hospitals do not perform any of these functions nor does providing hardware, software, or services to a military hospital result in the items being used for any military end uses.

We further note that in a separate, but related context, BIS has indicated that hospitals related to Entity List parties are not subject to the applicable restrictions. Per a BIS FAQ:

> BIS Website - Are hospitals and medical centers of Indian Department of Atomic Energy entities that are on the Entity List included in the entries for those entities?
> No. Hospitals and medical centers of Indian Department of Atomic Energy (DAE) entities are not—and were never intended to be--captured by the Entity List. Consequently, hospitals and medical centers of DAE entities are not subject to the Entity List's licensing requirements. Note that the licensing requirements found elsewhere in the EAR may be applicable to such hospitals and medical centers. Such hospitals and medical centers would also be generally subject to destination-based licensing requirements that apply to India.

2. Universities

If a university department is doing research on behalf of the military, does that make the entire university a MSEU? Are transactions with other departments of the university permitted, for example with the university library or the registrar's office?
When designating universities on the Entity List, to the extent possible, BIS has always limited its designation to the specific school/department and Entity List restrictions apply only to the specified department when there is no knowledge that the item will be diverted from another department/school to the restricted entity (e.g., Chinese Academy of Sciences Institute of Computing Technology is on the Entity List, the Chinese Academy of Sciences Institute of Botany is not.) The MSEU rule should be clarified so that it is explicitly clear that even if an academic institution has departments engaged in MSEU activities, the overall academic institution is not considered to be an MSEU.

3. Is there a minimum threshold for an entity to be considered a military support end user?

Does direct support of a Military End User (MEU) in any fashion make an entity an MSEU? For example, would a company that provides point of sales (POS) terminals for a military base cafeteria be considered an MSEU? What about the food suppliers to the base cafeteria?

Is there a degree of support or minimum threshold of support? For example, a cyber security company that provides services to both government and civilian end users where some of the government agencies could be national armed services. Does the cyber security company meet the definition of a MSEU?

We believe that in order to qualify as a military support end user, the relationship must be direct and explicit in order to avoid restricting export to and the continued function of legitimate entities that may support both the private and public sectors.

C. Intelligence End User Controls

BSA respectfully submits that the Intelligence End User (IEU) country and product scope is overly broad and risks the U.S. Government's intelligence sharing relationships with certain countries in the Middle East. We urge BIS to account for these concerns.

The proposed IEU rule's country scope to include all Group D countries puts the U.S. Government's intelligence sharing abilities with partner countries in the Middle East at risk. As the IEU rule would cover all countries in the Middle East, including close allies such as Jordan, the unintended, but easily foreseen, consequences of this rule are clear: it will be more difficult for intelligence agencies in the Middle East that work with the US intelligence community to source critical IT hardware and software from US suppliers.

The US intelligence community's relationships with their counterparts in the Middle East have been widely reported. For example, as a 2022 Congressional Research Service report noted:

> Jordan also is a longtime U.S. partner in global counterterrorism operations. U.S.-Jordanian military, intelligence, and diplomatic cooperation seeks to empower political moderates, reduce sectarian conflict, and eliminate terrorist threats in the region. U.S. officials frequently express their support for Jordan. U.S. assistance has helped Jordan address serious vulnerabilities, both internal and external.

Now, under the proposed IEU rule, the General Intelligence Department (GID) in Jordan will face export licensing requirements and delivery delays for anything that it procures from a U.S. company such as defensive cybersecurity software updates and critical IT hardware parts for network repairs.
Beyond Jordan, it has been widely reported that the intelligence services in Saudi Arabia and the UAE shared information with U.S. intelligence agencies related to Iran's April 2024 drone attack on Israel. New reports noted that:

> Several Gulf States, among them Saudi Arabia and the United Arab Emirates, passed on intelligence about Iran's plans to attack Israel, providing vital information that was key to the success of the air defense measures that almost entirely thwarted the massive assault, the Wall Street Journal reported Monday citing Saudi, US, and Egyptian officials.

Again, creating export licensing requirements for critical IT infrastructure and defensive cybersecurity software for these intelligence agencies in the Middle East that are supporting U.S. policy goals may prove counterproductive.

We recommend that the county scope of the IEU rule, like the other rules in the July 2024 Proposed Rules, should be limited to only the D:5 and E countries. There should be uniformity of country scope across all of these proposed rules to assist the regulatory community with their due diligence efforts and their ability to effectively implement internal compliance processes. Limiting the country scope of the IEU rule to only the D:5 and E countries will also serve the best interests of the U.S. intelligence community and the intelligence agencies that they work with the Middle East.

We further recommend that the product scope of the IEU rule should be limited to those items that the U.S. government believes pose a significant national security concern, rather than the overly broad set of controls on all items subject to the EAR – from pencils to supercomputers. As previously noted, the export license burden on both industry and BIS will make implementation of all of the July 2024 Proposed Rules difficult.

D. Foreign Security End User

BIS needs to provide greater clarity to its preamble commentary about the scope of the FSEU rule. Specifically, BIS states the following:

> In this proposed rule, BIS would not apply the term 'foreign-security end users' to civilian emergency medical, firefighting, and search-and-rescue end users. In situations in which a country integrates police, emergency medical, firefighting, and search-and-rescue services into a single public safety department, BIS seeks to ensure that the export, reexport, or transfer (in-country) of items necessary to protect lives is not disrupted and therefore would apply a case-by-case review standard. BIS also seeks to ensure that the export, reexport, or transfer (in-country) of items necessary to protect lives at airport terminals, railway and rapid transit stations, and other public transport hubs is not disrupted.

How would BIS define "not disrupted" if export licensing delays cause IT network issues or cybersecurity vulnerabilities in an agency that includes civilian emergency medical, firefighting, and search-and-rescue as well as more traditional policy/security functions?

With regard to the comment about airport terminals, railway and rapid transit stations, and other public transport hubs, is BIS indicating that police and security agencies at these facilities are not subject to the FSEU rule? How would BIS "seek to ensure" that its export licensing processing times do not impact public safely at these facilities if critical items are not received in time and impact operational readiness and public safety?

E. Foreign Security End User (FSEU)

The FSEU proposed rule includes a definition of foreign security end user that includes ''governmental and other entities with the authority to arrest, detain, monitor, search, or use force in the furtherance of their official duties.'' The rule then provides some additional examples of FSEUs that includes "analytic and data centers (*e.g.,* genomic data centers), forensic laboratories, jails, prisons, detention facilities, labor camps, and reeducation facilities." While the proposed rule notes that the definition of FSEU includes "all levels of the government police and security services, from the national headquarters or the ministry level to all subordinate agencies/bureaus (*e.g.,* municipal, provincial, regional)," it neglects to make clear whether the Ministry of Justice, courts at any level of government, or other judicial bodies would be considered FSEUs. Since the judicial system plays a role related to the police and criminal justice (even in countries with flawed human rights records), we would presume that they would be captured by the FSEU rule. However, if BIS intends to include these types of legal and judicial entities in the definition of an FSEU, it should make an explicit reference in any final rule.

III. Conclusion

BSA thanks the Bureau for the opportunity to provide these comments. Please contact Joseph Whitlock at josephw@bsa.org with any questions.