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

RE: 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

Dear Ms. Cook:

The National Foreign Trade Council (NFTC) appreciates this opportunity to respond to the Bureau of Industry and Security's (BIS) proposed rule seeking comments on the expansion of controls on military and intelligence end users and end uses.

NFTC supports the objectives of this rule in furthering U.S. national security and foreign policy goals. We understand that this proposed rule and its corresponding Foreign Security End User ("FSEU") rule, RIN-0694-AJ43, published on July 29,2024, further implements and builds on authorities codified in the Export Control Reform Act of 2018 ("ECRA") and expanded in the FY23 National Defense Authorization Act ("NDAA"). NFTC and its member companies have concerns that the creation of four overlapping categories of end-users: Military End User (MEU), Military Support End User (MSEU), Intelligence End User (IEU) and Foreign-Security End User (FSEU), as well as expanded controls on related U.S. persons activities place at risk the U.S.' ability to respond to the national security threats of today as well as future challenges.

Our comments and recommendations seek to tailor scope and implementation of this proposal to clearly align with and address specific and articulable national security concerns. Our prescriptive approach includes developing carve-outs for end-users for whom information is already known as well as targeting only items controlled for National Security reasons on the Commerce Control List for inclusion in this rule. It is important that these regulatory changes remain narrow in scope and are carefully tailored to achieve policy objectives including promoting human rights and supporting intelligence-sharing capabilities with like-minded allies and trading partners whilst not creating a cascade of knock-on effects that ultimately harm national security interests. Failing to maintain the balance between the national security

interests of the United States and the strength and robustness of U.S. industry undermines the effectiveness of these regulations.

NFTC recognizes and affirms that the primary objective of these rules must always be to safeguard and promote national security. However, the potential impact of what is essentially a new regulatory regime built on an unprecedented expansion of current practices must be assessed holistically and objectively. It is important to consider how allies, trading partners, members of current multilateral export control regimes and foreign adversaries of today and the future may react to the measures proposed in this rule. Retaliatory sanctions and controls, particularly if imposed by foreign adversaries, may bypass rule of law and deliberately seek ways to maximize harm to U.S. interests at home and abroad. Certainly, China has been expanding its export controls program and continues to ramp up its "Anti-Foreign Sanctions Measures", and in recent cases have created "conflict of law" scenarios, placing punitive measures on U.S. companies complying to U.S. controls. We do not take lightly the potential for trade disruptions or reputational damage, and we implore BIS and its interagency partners to carefully consider how U.S. companies and their U.S. person employees affected by this rule may bear the brunt of potential consequences.

Controls on U.S. person activities

The significant expansion of controls on US person activity related to foreign origin items disadvantages US industry vis-a-vis foreign entities that do not have to comply with these restrictions. This increased compliance burden will result in increased costs. The unilateral nature of the proposed U.S. person controls, particularly in relation to foreign origin items and activities outside the United States, significantly disadvantages U.S. companies and individuals by fueling perceptions of unreliability amongst non-U.S. business partners. Global supply chains of U.S.-headquartered companies generally rely on U.S. person/entity support and systems that cannot easily be unlinked for purposes of ensuring compliance with the proposed rule in day-to-day global operations. This also applies to any company, regardless of where headquartered, that employs U.S. persons in the Country Groups affected by this rule and potentially creates situations where U.S. workers may be discriminated against. The impact of these expanded controls will be increasingly difficult to quantify due to lost business opportunities and increased compliance costs but will clearly exceed the original intent of the ECRA. The ambiguous and broad terms used by BIS create confusion around wholly commercial transactions that have no bearing on national security.

U.S. persons, including natural persons, will also be increasingly vulnerable to retaliatory controls. As a retaliatory mechanism, U.S. persons, especially natural persons, can be exposed to disparate enforcement of host country and local laws and regulations where they may not be afforded due process protections. Mere compliance with U.S. laws and regulations should not place any U.S. entity or natural person in jeopardy from non-U.S. authorities Care must be taken to protect U.S. persons from exposure to capricious or retaliatory enforcement from foreign adversaries.

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 they are 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.

Recommendation: The proposed controls on U.S. persons activities rely on uniform understanding and compliance with the term "support" as defined by BIS. NFTC seeks clarity, consistency and restraint in implementation controls with appropriate consideration of the risks of retaliatory controls and sanctions.

Common Carrier Exclusion

NFTC appreciates the exclusions described in this proposal rule including those for administrative services and commercial activities related to transportation services provided by common carriers. However the introduction of a "knowledge" standard diminishes the utility of such an exception. Applying a "knowledge" standard to the identification of MEU, MSEU, and IEU entities without using a list-based designation process raises the due diligence required of common carriers to the same level as parties to the underlying transaction – an unrealistic and unsustainable level for a group that is intended to be excluded from the rule.

Recommendation: In order to meet national security objectives without unduly burdening common carriers, BIS should more clearly delineate the specific due diligence expectations for all U.S. persons -- individuals (e.g., employees), common carriers, exporters of record and other transaction parties.

Services

The proposed rule restricts the ability of U.S. persons to procure even basic and routine general services from the entities in the countries of concern. For example, telecommunications and utility infrastructure companies provide undifferentiated services to their customers in the relevant jurisdictions. If such entities are designated as MEU, MSEU or IEU, the U.S. persons and entities will not be able to procure such basic and routine services in these countries without first seeking authorization to do so.

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 and differentiate between MEU, MSEU, and IEU. The parallel rule noted above creates yet another category, the Foreign Security End-User (FSEU). This drives all responsibility for due diligence and end user determinations to the business community without providing sufficient clarity or resources to ensure that such determinations can be made consistently regardless of size of business, global footprint, sophistication of compliance operations or industry sector. The lack of "bright line" distinctions between each category potentially harms U.S. national security by creating an environment where inconsistencies in compliance are nearly inevitable, particularly given the overlapping nature of these categories.

It is important to note that both proposed rules impose stringent due diligence requirements on 100% of transactions and counterparties even for companies that engage purely in commercial business with no MEU, MSEU, IEU or FSEU touchpoints. Nonetheless, even companies that never expect to apply for an export license for one of these end-user categories must still exercise the same level of due diligence. In many cases, the paucity of open-source information about prospective end-users as well as impediments to conducting on-the-ground due diligence in specific destinations of concern make compliance variable at best.

The broad assumption that any end-user could be a MEU, MSEU, IEU or FSEU demands extensive due diligence to rule out the presence of these parties regardless of the benign nature of a transaction. Similarly, the broad product scope and licensing policies applied to these end-users is inconsistent with long-held policy objectives of creating "high fences around small yards".

The expansion of MEU to include persons and entities that perform combat and similar functions extends to "mercenaries, paramilitary or irregular forces", and is intended to cover "private companies, non-state actors and parastatal entities". These are not entities nor individuals for whom corporate compliance functions are set up to screen for nor are they parties for whom open source due diligence is readily and reliably available.

The definitional scope of FSEU seeks to address activities that could be implicated in human rights violations. However, while the proposed rule seeks to include subordinate agencies/bureaus of national level police and security services as well as private parties engaged to support these entities, it is silent with regard to the definition, scope or application of due diligence and licensing requirements to paramilitary organizations. There remains a divide between how the EAR addresses concerns regarding Military End-Users (MEU) and FSEU. The rule also fails to clarify the inclusion or exclusion of Ministries of Justice including the courts and other judicial bodies at each of the levels noted in the rule. In certain countries and jurisdictions, Ministries of Justice also administer prisons and other detention facilities where human rights abuses may be particularly problematic. This rulemaking must noy further opportunities for human right violations.

Recommendations for new end-user categories: Given these complexities, NFTC strongly recommends a Savings Clause as well as extension of existing licenses and authorizations for current MEU and MIEU to include MSEU. We also respectfully suggest phased implementation of any final rule be built around significant and sustained interaction with industry to drive greater clarity, coherency and consistency in compliance practices.

Due to the overlapping nature of the four categories, BIS should also provide guidance on which end user classification takes precedence if exporters determine an end user could be classified into multiple categories. Changing automated screening processes and enhancing escalation procedures require time and resources. Engaging in industry outreach can help BIS gather data to better inform future rulemaking and restricted party designations.
BIS should also consider providing sample templates for end use certifications that companies can use, in conjunction with other screening processes, to establish bona fides.

NFTC also respectfully suggests excluding from scope current end-users of items subject to the EAR. At a minimum, implementation of new controls for items destined to MEU, MSEU, IEU and FSEU should not require the suspension or disruption of any current active authorizations including export licenses, shipments to Validated End-Users or shipments made under current license exceptions.

Provision of Services

Military Hospitals

NFTC notes that certain end-user types, specifically hospitals and universities, can be particularly difficult to categorize. Hospitals with military designations do not always serve only uniformed military or paramilitary personnel. For example, the Royal Cambodian Armed Forces Institute of Health Sciences, a state institution, would be considered a Military Support End-User (MSEU) even though the Institute provides medical services for military and civilians including local citizens. Moreover, many doctors and other medical staff in military hospitals have trained overseas, including in the United States. It is impossible to stand at the door of a hospital and know whether an incoming patient is civilian or military. However, the blanket inclusion of military hospitals as MEU and MSEU is certain to disrupt direct patient care.

In addition, hospitals in China, including military hospitals, play an important role in drug development. Disrupting clinical trials including those involving patients at hospitals with People's Liberation Army designations, ultimately harms patients in the U.S. and around the world. Clinical trials do not involve the transfer of technology or patient data to clinical trial sites or from one trial site to another. If PLA hospitals in particular (not to mention potentially in other countries) are considered within scope, U.S. companies, or any companies using U.S. items, would effectively be prohibited from continuing their R&D activities with these institutions, including basic laboratory research to identify targets for treatment and preclinical in vitro testing (e.g., testing in tubes or petri dishes), in addition to clinical testing.

PLA hospitals have also historically cooperated with the United States including through U.S. Veterans Administration-supported medical programs such as on the treatment of pediatric burns, research on brain injury, and the use of acupuncture to treat post-traumatic stress disorder. There are more than 20,000 publications in the National Institutes of Health's ("NIH's") National Library of Medicine authored by one or more researchers affiliated with PLA hospitals in China, including 700 supported by NIH grants and 26 funded by the U.S. Veterans Administration. The inclusion of military hospitals in this proposed rule as either MEU or MSEU would create a serious chilling effect on research cooperation, particularly research that involves U.S. developed and manufactured products. Consideration should also be given to the impact of severing cooperative research and development ties on counterparties, who may be forced into retaliating against U.S. interests.

Recommendations: NFTC requests that BIS "carve out" military hospitals from MEU and MSEU definitions. This is consistent with its FAQ on Military End-Users dated April 28, 2020 and updated December 10, 2021:

> "Due diligence is required to determine whether the "military hospital" is part of the national armed services of Burma, Cambodia, China, Russia and Venezuela, which

would depend on a number of factors, such as the actual relation of the "military hospital" to the country's national armed services and the patient population served by the hospital, or whether it is an entity that develops, produces, maintains, or uses military items."

A carve-out could be achieved by re-defining MEU and MSEU to exclude either all or just military hospitals and medical facilities delivering direct patient care. BIS could also consider publishing a "white list" of hospitals, medical facilities and research centers that have previously received items through an authorization or who have been the subject of a favorable End-Use Visit in the form of Pre-License Check or Post-Shipment Verification. BIS' recent creation of Validated End-User Data Center ("Data Center VEU") could be a model for future consideration of highly vetted hospitals with a strong history of compliance with license conditions.

Alternatively, we respectfully request that BIS limit scope only to military hospitals that have been specifically designated on the Entity List for documented involvement in military end-uses, military support functions or intelligence support functions (see discussion below).

In order to protect patient access and continuity of care, NFTC also seeks expansion of License Exception MED to include certain EAR99 medicines and related items destined to military hospitals currently captured by this proposed rule. A minimum baseline of products for consideration could be the BIS List of EAR99 Medical Devices. Such an exclusion would be consistent with long-standing U.S. policy to facilitate humanitarian assistance and avoid causing harm particularly to civilians.

Universities

U.S. and non-U.S. companies work with universities around the world to develop commercial products and technologies. In some cases, U.S. and non-U.S. companies have provided equipment and/or funding to support basic education and fundamental research. These efforts are similar to other "people-to-people" programs in extending soft power by fostering cooperation and building brand recognition. They can also be useful in providing line-of-sight into the R&D trajectory of countries of concern. However, in some cases universities also have relationships with military, military support and intelligence entities. It can be difficult if not impossible to isolate specific departments, professors or student groups (e.g., ROTC-like organizations) at each university. There is the question of whether entire educational institutions would be designated as a military end user, and if so, the rule could prohibit cooperative non-dual use research.

Recommendation: NFTC respectfully seeks further clarification regarding criteria for including universities as MEU, MSEU and IEU entities. At a minimum, BIS should clarify the due diligence measures it deems minimally acceptable for universities. Are U.S. persons required to know every individual with the ability to access U.S.-origin items and technologies?

Military Support End-User

NFTC notes potential inconsistency between Sections 744.6(a)(1) as proposed and 744.22(f) of the EAR. We have also closely reviewed publicly available information regarding recent export enforcement actions taken against a naturalized Australian citizen accused of providing training

to Chinese nationals in Australia and against U.S. and former U.S. persons who provided defense services to the United Arab Emirates. Whilst we note that these two enforcement cases involved violations of the Arms Export Control Act ("AECA") and its implementing regulation the International Traffic in Arms Regulation ("ITAR"), NFTC references concurrent publication of a new "defense services" rule by the Department of State, Directorate of Defense Trade Controls ("DDTC").

Recommendation: NFTC respectfully seeks definitional clarity including specific scenarios, to help companies consistently identify MSEUs that may be captured by this proposed rule. The lack of clarity around the definition of "support" could undermine compliance efforts and thus lead to inconsistent support for national security objectives.

We also suggest narrowing thresholds for defining "support", for example, does a cybersecurity company that provides services to government and civilian end-users meet the definition of a MSEU? NFTC respectfully suggests that MSEUs must have a direct, explicit and exclusive relationship with military end-uses as defined in the regulation. BIS should also consider outlining specific scenarios and/or thresholds under which entities will be considered an MSEU.

Intelligence End-User definition and scope

Section 744.24(f) of the EAR defines an "intelligence end user" to include "other entities performing functions on behalf of such organizations." This is an incredibly broad definition that potentially captures entities serving functions unrelated to the primary activities of the organization. The rule, as written, also transfers the responsibility to identify foreign intelligence service and affiliates to companies, adding significant due diligence burden to companies. In many cases, U.S. companies do not have the required information, personnel, and resources to identify foreign intelligence services, which is why such processes have historically been the responsibility of the intelligence community.

Recommendation: NFTC respectfully seeks alignment of the IEU definition consistent with how a "Foreign Security End-User" is defined in Section 744.25(f)(2) of the EAR.

The inclusion of all Group D countries undermines U.S. national security by imposing new export licensing requirements for critical IT infrastructure and defensive cybersecurity software. The proposed IEU rule's overly broad country scope to include all Group D countries – including all of the countries in the Middle East except Israel - creates the risk that intelligence agencies in this region with whom the U.S. has shared, and is sharing, sensitive intelligence information will turn, over time, to alternative and less secure foreign suppliers for their information technology (IT) hardware and software needs. Governments around the world, including many in the Middle East and other countries within the scope of the IEU rule, currently rely on U.S. technology for their IT networks for everything from hardware for daily operations and data recovery to software for email, database management, and, most critically, defensive cybersecurity. While U.S. companies are technological leaders in many of these IT hardware and software products, there are other foreign sources of supply that these government agencies can choose from.

As has been noted, the increase in the export licensing burden to comply with this rule - for both industry and the U.S. government - will have a negative impact on U.S. industry's ability to continue to provide, in a timely manner, foreign government agencies with critical IT hardware and software that secures their IT network infrastructure.

It is inevitable that some of these intelligence agencies will turn to alternative, and less secure, sources of supply to meet their IT hardware and software requirements. If the licensing delays create network outages or expose them to cybersecurity threats from hostile countries and actors, these agencies can replace U.S. hardware with hardware supplied by Huawei from China and replace U.S. cybersecurity software with similar products from Kaspersky in Russia. The U.S. government has sanctioned both Huawei and Kaspersky and has repeatedly underscored the national security threat that they pose. Having such hardware and software in the networks of intelligence agencies that the U.S. government works with on a regular basis cannot be in the national security interests of the United States.

Recommendation: NFTC respectfully requests that BIS revise the scope of IEU to D:5 and E countries, and limit product scope to specific items enumerated on the Commerce Control List that present an articulable national security concern such as those already controlled for National Security reasons.

Foreign Security End-User

In the preamble commentary to the FSEU rule 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."

Comment: How would BIS define "note 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 will 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?

Licensing Impacts

Scope
NFTC suggests that all items subject to the EAR is over-broad and will contribute to significant licensing burden even with a presumption of denial without benefit to national security.

We note that the product scope for MEUs and IEU is all items subject to the EAR and the product scope for MSEU and FSEU is all items enumerated on the Commerce Control List; we respectfully submit that these are over-broad. BIS' own FAQs describe EAR99 as "generally consist(ing of) low-level technology, consumer goods, etc." Additionally, encryption hardware and software described respectively in ECCN 5A992 and 5D992 of the CCL are released as "mass market" and broadly available to government end-users in Country Group D.

Recommendations: NFTC respectfully proposes targeting the scope of items to be covered by the MEU, MSEU, IEU and FSEU to be limited to items controlled for National Security reasons on the CCL and Crime Control items for FSEU. For example, "600 series" items are already not available to end-users in Country Groups D:5 and E. For EAR99 items specifically relevant to national security concerns in D:5 and E countries, BIS could develop a focused list of sought-after items warranting additional due diligence. BIS could then contemplate an "is informed" standard to ensure visibility into these potential transactions and assess risks accordingly. In essence, this would model the Common High Priority Items List currently in use.

Facial Recognition Software
As drafted, the proposed ECCN 3D980 in the FSEU rule will control facial recognition software that does not have the capability to be used for "mass-surveillance and crowd scanning" applications that BIS intends to target. The definition of software controlled under 3D980.b is broad and would capture software that does not have the technical capabilities to recognizes faces from "in the wild" video feeds that are typical for "mass-surveillance and crowd scanning." BIS should amend this ECCN to clarify that the only software "specially designed" for facial recognition for mass-surveillance and crowd scanning is covered.

The ECCN clarifies that it does not control software that is solely for "authentication to facilitate individual access to personal devices or facilities." However, software used for facial recognition to authenticate access to a bank account would be controlled. Based on BIS's comments, this type of individual access control is not the contemplated use case of concern to BIS. BIS should expand this carve out to cover facial recognition that is used by a variety of services and not just for personal devices and facilities.

- It is also not clear how "person detection" is different from "facial recognition." Is "facial recognition" referring to the ability to detect a person without determining their identity?
- Further, the CC1 controls are too broad for the concerns listed. As BIS explains in the FR notice, the primary target of these control is foreign-security end users that may exploit facial recognition technology, therefore the software should be restricted to these types of end-users. BIS should also provide a general license or an exception that would authorize exports to allied countries at a minimum.

The unilateral nature of this control further undercuts BIS' own efforts to seek multilateral and plurilateral controls wherever possible. This leads to additional "knock on" effects including

avoidance of items and services that could be associated with facial recognition technology including use of U.S. data centers and cloud computing services to store such information.

Entity List recommendations

While the immediate movement of military end-users and intelligence end-users to the Entity List would appear to facilitate compliance and screening efficiencies, doing so without the case-by-case review and methodological rigor currently used for Entity List designations risks degrading the integrity of the End-User Review process. Moreover, BIS' FAQ for the Entity List affirms that a hospital must not be treated as an Entity List party unless it has been so designated:

> "Q: 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?
>
> A: No. Hospital 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 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."

Recommendation: NFTC understands the importance of the Entity List and its use by U.S. companies for making appropriate compliance and business decisions. The current designation and off-ramping process as administered by the interagency End-User Review Committee provides companies with the assurance that such actions are not taken lightly, includes a thorough review of available information and requires consensus.

National Security impact

NFTC and its member companies reaffirm our commitment to supporting U.S. national security and foreign policy goals and objectives. However, regulatory initiatives must include consideration of how implementation measures, whether by government or industry, could potentially degrade national security. We reiterate our concern that the use of Entity List and other designations, as well as company due diligence recordkeeping, can be exploited by foreign adversaries and their intelligence services.

Recommendation: Our regulations must ensure a process where the designation of parties from these defined end-user categories cannot be used by foreign adversaries to deduce U.S. intelligence capabilities regarding the military industrial complexes of countries in Country Groups D and E. We note that earlier this year BIS provided "Tier 1 Supplier Lists" to certain U.S. companies to assist in assessing their compliance risks. We recommend that BIS consider a similar program and establish a blanket "is informed" policy so that companies could apply a consistent due diligence and compliance standard across industries.

About NFTC

The NFTC, organized in 1914, is an association of U.S. business enterprises engaged in all aspects of international trade and investment. The NFTC supports open, rules-based trade, including a level and competitive playing field. Our membership covers the full spectrum of industrial, commercial, financial, and service activities. Our members value the work of BIS and other agencies in addressing national security threats from foreign adversaries.

Our goal is to always protect national security and economic security interests. Robust trade relationships are central to economic and national security. NFTC's National Security Policy Initiative brings the voice of business to policymakers on global security issues affecting international trade. Companies play a vital role in promoting American values, including human rights and democracy. Our data driven recommendations support American competitiveness and technology leadership that is central to our national security.

Thank you again for this opportunity to comment on this NPRM. We welcome the opportunity to discuss this important matter and answer any questions that you may have regarding these comments or recommendations. I can be reached at (202) 887-0278 or via email at jchu@nftc.org.

Sincerely,

Vice President for National Security Policy
Executive Director, Alliance for National Security and Competitiveness