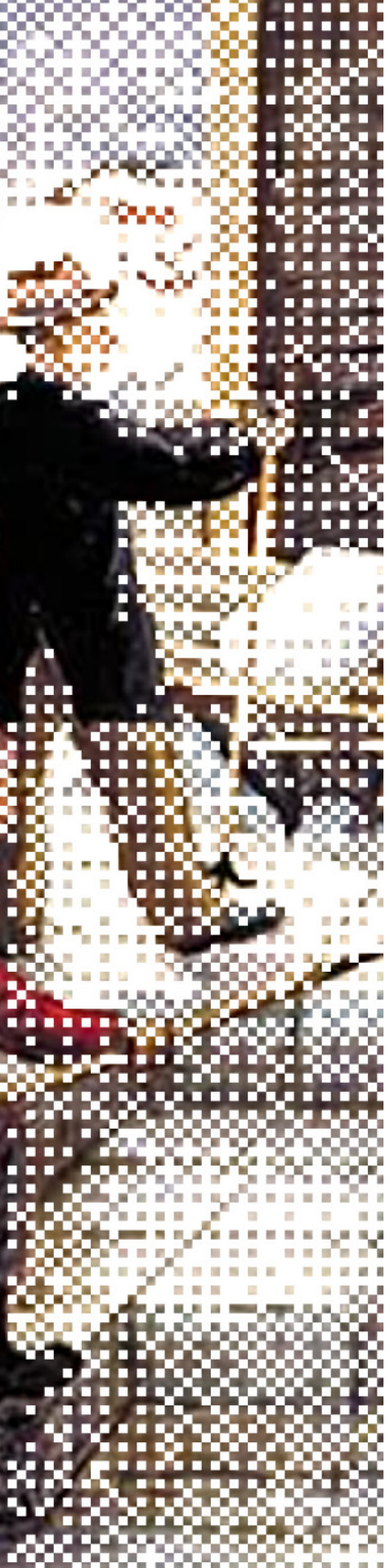


■ National Security

Conditional Export Controls on AI Chips

Tao Burga

SUMMARY

The Bureau of Industry and Security (BIS) implements US export controls on dual-use technology. To be effective at preventing misuse and smuggling, some of these controls, such as those on AI chips, must restrict exports to dozens of countries. Although this blanket-ban approach weakens US industry's competitiveness in the short and long term, current oversight and enforcement mechanisms leave little alternative.

Conditional export controls offer a more effective approach within BIS's authorities. This approach allows BIS to specify the conditions under which export restrictions apply, increasing restrictions on technologies that are easy to smuggle or misuse, but not on those that include security features to enable better oversight or reduce misuse potential. This would incentivize AI chip firms to develop more secure versions of their chips in order to avoid tougher export restrictions.

Using the pressing case of AI chips, BIS should reform the Low Processing Performance (LPP) license exception to lower the yearly cap of AI chip exports to single firms, while allowing chip firms to use LPP's current (higher) cap for chips that

include security features to help detect or prevent smuggling and/or hinder their misuse. By linking export access to security features, conditional export controls would enhance national security, help sustain US technological leadership, reduce smuggling, and drive security-focused innovation—all without additional government spending.

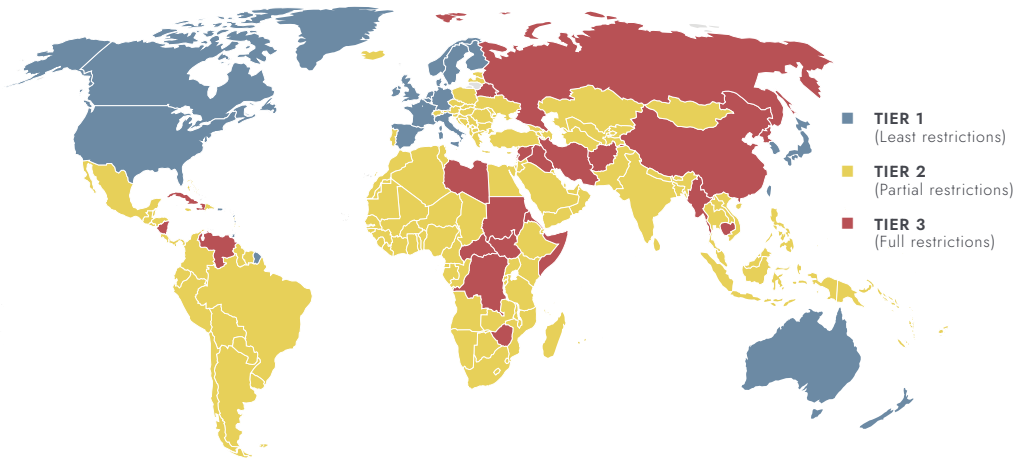
PROBLEM

Conditional export controls follow two principles:

1. Export controls should be *conditional*: restrictions should vary based on how effectively technologies can be protected against misuse or smuggling.
2. This conditionality should be *forward-looking*. BIS should not take the set of currently existing technologies as fixed; instead, it should specify which properties a technology would need to have to face lower restrictions, and let US industry innovate to meet this security requirement.

Although applicable to any technology that can be modified to decrease its misuse potential, this piece focuses on AI chips. Extensive smuggling shows that AI chip export controls are being easily circumvented. This mounting evidence is in part responsible for prompting BIS to repeatedly expand the scope of its controls on AI chips, from merely restricting exports to China and a few other arms-embargoed countries in 2022 to extending some form of AI chip export restrictions to all but 18 countries in the world in 2025.

AI CHIP EXPORT RESTRICTIONS AFTER JANUARY 2025



Map: Tao Burga. Source: Bureau of industry and security

To be effective, blanket bans on exports must be far-reaching, covering not only target countries but also every country suspected of facilitating smuggling. But these broad export restrictions come at a cost: in the short term, they weaken the competitiveness of American firms, and in the long term, they risk pushing global supply chains away from US technology. By driving demand toward foreign alternatives, they create room

for the emergence of foreign competitors and incentivize the deliberate "designing out" of American components. Moreover, blanket bans cannot address the underlying dual-use problem of AI chips themselves; once a chip has been smuggled, export controls do nothing to lower the chips' misuse potential.

By clearly specifying the conditions under which export regulations will vary, the US government can incentivize industry to develop products with built-in safety and security features that reduce misuse potential. These incentives would accelerate defensive innovation, spurring a "race to the top" among firms competing for increased market access in allied or neutral countries (though not in adversarial countries such as China or Russia, given the risk of circumventing security measures (see appendix)). Conditional export controls would thus allow the US to maintain foreign market access for its firms while achieving stronger national security outcomes, all without additional government spending.

BIS recently made progress by making access to National Validated End User (NVEU) authorizations conditional on the applicant's ability to verify that chips have not been moved from the intended destination country, explicitly including delay-based location verification as a potential mechanism. This is the most concrete and recent case of BIS implementing a conditional export control policy. Despite this, AI chip export controls continue to have major gaps: BIS's LPP license exception allows "Tier 2" countries (those facing partial restrictions) to receive up to 1,700 advanced AI chips (NVIDIA H100 or equivalent total processing performance) per firm per year with no country-wide limit or export license requirements, amounting to $42.5 million worth of chips today. LPP will likely prove to be the weakest link in today's chip export control regime, since smugglers can set up shell companies online for as little as a few thousand dollars in a matter of hours or days and take advantage of LPP.

SOLUTION

BIS should strengthen existing export controls on AI chips by amending the LPP license exception. Specifically, BIS should lower the annual import cap per firm in "Restricted LPP Destinations" from 1,700 to 200 H100-equivalent chips. This new quantity would be low enough to make large-scale smuggling much more difficult while not restricting smaller transactions, and is equal to the current reporting threshold for single shipments under LPP. Restricted LPP Destinations would be those in Tier 2 countries that are less trusted or suspected of being chip diversion hotspots (see appendix for the proposed list and detailed implementation recommendations).

Additionally, BIS should permit exports of additional chips—up to the original 1,700 limit, although it could be higher or lower—conditional on these chips having a new "High Security" (HS) certification granted by BIS and interagency partners. This does not roll back current export controls; it expands them *only* for less-secure chips.

The security goals for HS certification and example hardware-enabled mechanisms to achieve them should include:

1. Effective oversight: Knowing whether the chips have been moved to restricted regions, are being used by prohibited entities, or are being used for prohibited

uses. Possible mechanisms include privacy-preserving location verification to detect smuggling and metering to detect policy violations without revealing sensitive data.

2. Rule enforcement: Enforcing export restrictions by limiting the usefulness of the chip when in restricted regions or used for prohibited uses. Possible mechanisms include selling AI chips in fixed sets and bandwidth bottlenecking to prevent unauthorized dual-use AI model training, and offline licensing to enforce end-user or location-based export restrictions.

Some of these mechanisms, like delay-based location verification, can be implemented with little delay by leveraging functionality already present on advanced chips. Others may require years of R&D to be implemented securely. BIS should therefore consider a staged compliance delay (see appendix).

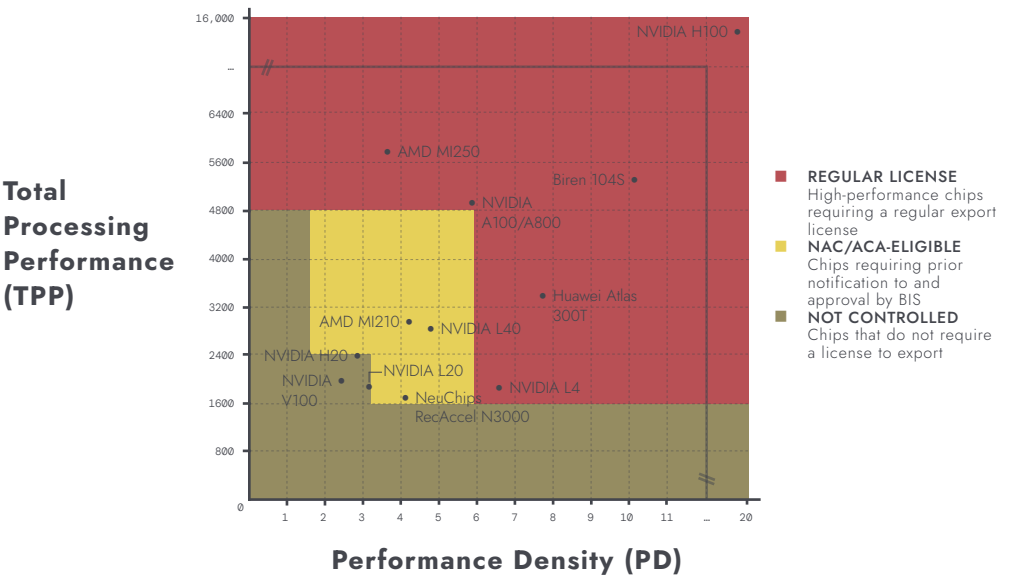
All these mechanisms should incorporate robust hardware security, tamper resistance, and privacy protections to prevent circumvention while maintaining trust in American technology. To ensure continued compliance, exporters should be required to submit regular reports to BIS detailing whether HS chips are still compliant with the terms of HS certification.

JUSTIFICATION

Precedent

BIS is authorized to set conditions for accessing export licenses under the Export Control Reform Act of 2018. Blanket export controls are already routinely implemented conditionally based on the technical characteristics of the items—indeed, current AI chip export controls apply only on chips above specific performance parameters, as shown below.

DATACENTER CHIPS



Source: Center for Security and Emerging Technology

What BIS has done comparatively less is make these conditions forward-looking to create incentives to adopt safer technologies. Still, this has precedent: In 2016, BIS created the "encryption carve-out," which exempts sensitive or dual-use data from normal export restrictions if stringent cryptographic security requirements are met. At the time, consultants advised companies to ensure adherence to this high security standard to simplify compliance and be able to serve customers that need to transfer sensitive data overseas. The success of BIS's 2016 encryption carve-out later prompted the amendment of the International Traffic in Arms Regulations (ITAR) to likewise create a successful encryption carve-out for the export of sensitive data within its jurisdiction. Today, all major US cloud computing providers offer data storage and transfer services that comply with the security standard set by BIS, even touting it as a feature to attract users.

Challenges to implementation and recommended solutions

If BIS has the authority and successful precedent to implement conditional export controls, why doesn't it do so more often? The most important challenges to overcome are:

- Specification: BIS's conditions for lowering export restrictions need to be well specified, which is harder to do for technologies that do not yet exist or have not been widely adopted.
- Credibility: Given the specification problem described above, BIS may be reluctant to take on the task of testing the on-chip security mechanisms in-house. This would take time, money, and expertise that BIS may not have.
- Unintended consequences: BIS may fear that on-chip mechanisms for governance could be tampered with and circumvented post-export, reducing their efficacy.
- Capacity constraints: BIS has already expressed interest in conditional export controls and implemented one in their NVEU program, but it has not had capacity to scope and implement more such changes because it is chronically underfunded and understaffed.

The proposed solution addresses these concerns by recommending:

- A discretionary (yet minimally burdensome) approach to give BIS flexibility in adjudicating applications, thus eliminating the risk of negative outcomes from bad early specifications.
- Placing the burden of proof for HS applications on US chip firms, since they have the required technical knowledge and capacity to run or fund these evaluations.
- Conditionally expanding, not reducing, export controls. This means little downside risks to national security, even if the on-chip mechanisms are circumvented. If US chip firms choose not to apply for HS licenses, the effect will merely be a reduction in the number of chips that can be sold without a license to less trusted Tier 2 countries. In the worst-case scenario, if HS-certified chips are sold but are later found out to be easy to skirt their security mechanisms, the level of effective restrictions on chip exports will still be no higher than they are currently. ■

FURTHER RESOURCES

- Tim Fist, Tao Burga, and Vivek Chilukuri, "Technology to Secure the AI Chip Supply Chain: A Working Paper," Center for a New American Security, 2025
- Asher Brass and Onni Aarne, "Location Verification for AI Chips," Institute for AI Policy and Strategy, 2024

Tao Burga is a Technology Fellow at the Institute for Progress, where he focuses on compute governance, export control, and accelerating innovation in AI security.

APPENDIX

How to implement HS certification

To implement an HS certification for AI chips and qualify them for lower export restrictions, BIS, in collaboration with interagency partners, would adjudicate applications on a per-model basis, granting HS certification automatically to all identical chips with the same security-enhancing modifications. Chips with previously approved security mechanisms could also be fast-tracked for certification.

This discretionary adjudication process could be modeled after that of the Notified Advanced Computing (NAC) license exception, reducing set-up costs. But unlike for NAC, HS certification should only require one blanket approval for all identical chips or security mechanisms. This would differ from NAC's per-shipment process, which has proven cumbersome for BIS and industry alike.

A non-formulaic approach is important because creating precise technical specifications may be difficult for BIS to do in advance. Instead, discretionary approaches would allow BIS to specify security goals, and let US chip firms choose the best ways to meet them. A precise, formulaic process could still be used for some better-understood mechanisms like delay-based geolocation.

Because BIS is chronically underfunded and understaffed, it is unlikely to be able to conduct the relevant evaluations fully in-house. That is why it should, first, rely on its interagency partners, including the Department of Defense and the National Institute of Standards and Technology, for technical assistance, and, second, advise private industry that they are responsible for meeting the burden of proof and showing the functionality and robustness of their hardware security mechanisms.

The draft rule text below (alongside a more detailed application form) could be used to establish HS Certification:

> *(a) HS Certification.* Exporters may apply for HS certification on a per-model basis (i.e., separate certification is needed for items with different designs or technical specifications), to show that the item meets the security requirements (as specified in subparagraph (a)(i)), to the satisfaction of the Bureau of Industry and Security and its interagency export control partners.

(i) Security requirements. To be eligible for HS certification, exporters must show that the item has features which:

(1) (starting 60 days after [PUBLICATION DATE]) Enable the exporter and the Bureau of Industry and Security to continuously (e.g., monthly) and easily verify that the item has not been moved to an ineligible destination (e.g., from ping times to nearby secure servers) with a focus on avoiding false negatives (the item does not appear to be in a restricted region, but it is), as specified in paragraph [PARAGRAPH] of this section, AND/OR

(2) (starting 10 months after [PUBLICATION DATE]) Significantly decrease the item's usefulness for some activities described in part 744 of the Export Administration Regulations, and especially for dual-use AI model training, by significantly throttling performance (e.g., by revoking an operating license and bottlenecking interconnect bandwidth), especially if the item is moved to ineligible destinations as specified in paragraph (b)(i) of this section; AND

(3) Are tamper-resistant or tamper-evident and costly to circumvent, for example by requiring significant time or cost proportional to the number of items from which security features are removed.

(ii) Incident reporting requirement. Exporters with knowledge of incidents or evidence that suggest that the added security of an HS-certified item is being successfully tampered with or circumvented must immediately report these incidents to BIS.

(iii) Revocation of certification. HS Certification may be revoked, at the discretion of BIS, if an HS-certified mechanism or model of an item is found to no longer satisfy the security requirements specified in paragraph (a)(i) of this section.

Proposed amendments to License Exception LPP

BIS should amend 15 C.F.R. § 740.29 as follows:

1. Add a new subparagraph to paragraph (d) to read as follows:

(d)(1) Notwithstanding paragraph (d), any ultimate consignee that is located in, headquartered in, or has an ultimate parent company headquartered in a "Restricted LPP Destination" (as defined in paragraph (h)(3) of this section) may receive no more than 3,200,000 TPP per calendar year under License Exception LPP, unless the exported or reexported items are HS-certified (as defined in paragraph (h)(4)). If the exported or reexported items are HS-certified, the standard 26,900,000 TPP limit in paragraph (d) applies.

2. Modify subparagraph (f)(ii) by deleting "*26,900,000 TPP*" and replacing it with "*3,200,000 TPP for non-HS certified items or 26,900,000 TPP for HS-certified items (as defined in paragraph (h)(4))*"
3. Modify subparagraph (g)(2) by deleting "*26,900,000 TPP*" and replacing it with "*TPP set forth in paragraph (d)*"
4. Add two new definitions in paragraph (h) to read as follows:

(h)(3) Restricted LPP Destination. *For purposes of paragraph (d)(1) of this section, a "Restricted LPP Destination" means any destination specified in Country Group D:1 or Country Group D:4, as well as India, Indonesia, Malaysia, the Philippines, Singapore, and Thailand. [See justification below.]*

(h)(4) HS-certified item. *For purposes of this license exception, an "HS-certified item" is an item that has been granted a High Security (HS) certification by BIS, in consultation with its interagency export control partners, upon a determination that such item incorporates on-chip security measures designed to facilitate post-export oversight (e.g., geolocation from the ping times to nearby secure servers) or to reduce misuse potential, including dual-use AI model training and large-scale inference (e.g., offline renewable licensing to enforce end-use agreements) and that the item's security mechanisms cannot be easily bypassed (e.g., by relying on robust hardware security to make tampering costly and/or easy to detect).*

The justification for "Restricted LPP Destinations" is that Country Groups D:1 and D:4 were already export-controlled in October 2023 as the result of concerns about national security and missile technology proliferation. The other countries are added because of modeling that indicates they may be hotspots for AI chip diversion (e.g., to China). This excludes Taiwan, a key strategic ally. The list should be amended as AI chips with geolocation capabilities increase our insight into which countries are responsible for most chip diversion.

Frequently asked questions

Q: Does this approach roll back current export controls?

A: No. Conditional export controls are a tool with a broad range of possible implementations. The goal is to have higher restrictions for less secure technology compared to more secure versions of that same technology. For example, this proposal achieves this goal by increasing export restrictions *only* on less-secure chips. Alternative approaches could seek to decrease net restrictions by creating broader carve-outs for more secure chips.

Q: Would it be safe to export AI chips with security and oversight-enhancing mechanisms to adversarial countries such as China and Russia?

A: No. All such mechanisms carry some risk of circumvention, especially by motivated nation-state-level actors. If conditional export controls are used to facilitate exports of more secure chips, this should only be done for currently restricted allies or neutral countries. Some of these are countries that faced no AI chip export restrictions before January 2025, many of which are US allies or strategic partners, such as Poland, Iceland, Turkey, Colombia, and others that are neither suspected of widespread misuse or chip diversion.

Q: Why not just require US chip firms to modify all their export-grade chips to make them more secure?

A: Blanket requirements could backfire by forcing industry to implement security mechanisms that are not yet commercially viable. While such requirements would be reasonable for well-understood mechanisms implementable with functionality already present in chips, such as delay-based location verification, many promising security features still require substantial R&D to ensure that they are effective without compromising performance or adding prohibitive costs. Conditional export controls offer a balanced approach by creating strong incentives for innovation in chip security while allowing flexibility in implementation. This reduces the risk of unintended consequences and prevents potential harm to US industry's competitiveness if certain mechanisms prove difficult to implement.

Q: Should conditional export controls only be applied to AI chips?

A: No. Although this proposal focuses on AI chips, other export-controlled technologies would be good candidates for conditional export controls. In general, conditional export controls should be targeted at modifiable dual-use technologies in areas where the US is ahead of the competition. In this context, "modifiable" means that it could be made safer to export with technical alterations.

Another technology where conditional export controls seem particularly valuable is benchtop DNA synthesizers. A report from the Institute for Progress investigated technical mitigations that should be implemented on these devices, which could serve as a tentative list of potential security-enhancing modifications that would lead BIS to implement less restrictive export controls.

Q: Is delay-based location verification fully privacy preserving?

A: Yes. Delay-based geolocation can identify only the broad area (tens to hundreds of miles) where a chip may be located, and it does so without communicating any private or sensitive information. This is because it relies on sending a simple "ping" to AI chips and calculating the time it takes to return to the server of origin. This can already be implemented with cutting-edge AI chips' existing functionality.

Q: Is delay-based location verification easy to circumvent?

A: No, not easily and without raising alarms. There are two broad ways it could be circumvented: taking the chips offline and spoofing. Taking chips offline is comparatively easy, but would raise red flags: although the chip wouldn't positively attest that it has been smuggled, it would stop positively asserting that it hasn't. This would alert BIS to potential smuggling, allowing it to focus its enforcement efforts on these cases

while not worrying about chips that continue to provide consistent location data. That is, even if some motivated actors are able to stop transmitting location data, having this functionality is an immense improvement over BIS's current oversight capabilities.

The second approach, spoofing, could be actively misleading (e.g., showing a location outside of China when the chip is actually in China). However, this would be very difficult to accomplish at scale. It may require per-GPU private key extraction (potentially through complex side-channel attacks) and forging responses for thousands of GPUs with precise timing. This may only be feasible for openly adversarial state-backed actors with physical access to the chips. Even then, it would cost significant resources, slow down smuggling, catch failed circumvention attempts, and significantly narrow down potential smuggling routes.

Therefore, while no security measure is perfectly foolproof, delay-based location verification would significantly enhance BIS's monitoring capabilities and act as a strong deterrent against AI chip diversion.

Q: How could US chip firms meet their burden of proof for HS certification?

A: Firms could meet their burden of proof by subjecting their modified products to adversarial testing or red-teaming, potentially launching bug bounty programs and hiring independent evaluators; demonstrating post-export oversight mechanisms, such that they would know if a certain solution has been circumvented; adhering to existing rigorous hardware/cybersecurity standards when applicable; and gradually rolling out new solutions to test them under real-world conditions.