Comments of the
Semiconductor Industry Association

On

The Interim Final Rule Entitled
"Export Control Revisions for Australia, United Kingdom, United States (AUKUS) Enhanced Trilateral Security Partnership"

89 Fed. Reg. 28594 (April 19, 2024)
RIN 0694-AJ58
Docket No. 240415-0109

Submitted June 3, 2024

The Semiconductor Industry Association (SIA) submits these comments in response to the request from the Bureau of Industry and Security (BIS) in the above-captioned rule. The Interim Final Rule entitled "Export Control Revisions for Australia, United Kingdom, United States (AUKUS) Enhanced Trilateral Security Partnership" (AUKUS IFR) amended the Export Administration Regulations (EAR) to remove license requirements, expand the availability of license exceptions, and reduce the scope of end-use and end-user-based license requirements for exports, reexports, and transfers to or within Australia and the United Kingdom (UK). The policy objective of the AUKUS IFR is to enhance technological innovation among the three countries and support the goals of the AUKUS Trilateral Security Partnership.

Part I of these comments contains introductory and background comments about SIA and semiconductors. Part II contains general comments about the AUKUS IFR, including the desirability of removing license requirements to Australia and the UK for encryption items and loosening other EAR controls to promote U.S. economic and foreign policy interests. Part III contains general comments on encryption controls.

Part I – Introduction and Background

SIA has been the voice of the U.S. semiconductor industry for over 45 years. SIA member companies represent more than 99% of the U.S. semiconductor industry by revenue and are engaged in the research, design, and manufacture of semiconductors. The U.S. is the global leader in the semiconductor industry today, and continued U.S. leadership in semiconductor technology will drive economic strength, national security, and global competitiveness. More information about SIA and the semiconductor industry is available at https://www.semiconductors.org/.

Semiconductors are complex products critical to the functioning of everyday consumer electronics, communications, and computing devices in the automotive, industrial, financial, medical, retail, and many other sectors of the economy. They are also critical

components for technologies relevant to the AUKUS Trilateral Security Partnership, such as artificial intelligence (AI), edge computing, and 5G/6G telecommunications.

Overseas markets play a crucial role in this capital-intensive industry; indeed U.S. headquartered semiconductor companies generate around 75 percent of revenue from sales to foreign markets, on average. Access to global markets is therefore needed to ensure that U.S. semiconductor companies are able to continually fund the very large R&D investments and capital expenditures that are required to maintain U.S. technology ahead of global competitors, a phenomenon that a BCG report[1] termed the "virtuous innovation cycle." As the U.S. government takes action intended to reduce U.S. sales of advanced semiconductors and chip manufacturing equipment to certain overseas markets, it is important for the U.S. government to also pursue policies that reduce barriers to overseas sales, and create new demand for semiconductors manufactured in the U.S. SIA thus welcomes the regulatory changes in the AUKUS IFR, which will facilitate semiconductor sales to Australia and the UK and enable greater collaboration and integration of the U.S., Australian, and UK industrial bases.

Part II – General Comments on the AUKUS IFR

We set out below general comments regarding the AUKUS IFR, including in response to BIS's request for comments on the potential impact of removing encryption items (EI) licensing requirements for Australia and the UK.

Comment II.A: SIA commends BIS for removing controls applicable to Australia and the UK in furtherance of AUKUS.

Announced in September 2021, the AUKUS Trilateral Security Partnership is intended to modernize the defense and technological relationships between the U.S. and two of its closest allies in the face of a changing global security environment. AUKUS Pillar I is an initiative to progress Australia's acquisition of conventionally armed, nuclear-powered submarines. AUKUS Pillar II focuses on the U.S., Australia, and the UK jointly developing and fielding advanced technological capabilities in areas such as artificial intelligence and advanced cyber.

The AUKUS IFR removed controls applicable to Australia and the UK in furtherance of AUKUS Pillar II. The Department of State, Directorate of Defense Trade Controls (DDTC) announced a corresponding proposed rule to amend the International Traffic in Arms Regulations (ITAR) to reduce restrictions on defense-related trade with Australia

[1] *How Restrictions to Trade with China Could End US Leadership in Semiconductors*, BOSTON CONSULTING GROUP, March 2020, https://web-assets.bcg.com/img-src/BCG-How-Restricting-Trade-with-China-Could-End-US-Semiconductor-Mar-2020_tcm9-240526.pdf.

and the UK.[2] SIA commends BIS for removing these EAR controls, which will facilitate information and technology sharing by and among industry in the United States, Australia, and the UK. SIA also encourages BIS to urge DDTC to make commensurate revisions to the ITAR.

Comment II.B: We ask BIS to consider removing "EI" controls for encryption items for Australia and UK.

BIS did not remove license requirements to Australia and the UK for encryption items (EI) in the AUKUS IFR, but invited comments on the potential impact of removing such requirements. In general terms, encryption can be defined as the process of changing data into a form that is unintelligible by unauthorized persons for the purpose of ensuring the security or confidentiality of the data and privacy of the individuals transmitting the data. A common understanding of commercial encryption is as a tool to ensure that communications are accessible only by authorized persons. However, other uses, such as verifying authenticity and preventing the undetected change of information content, are no less important.[3]

Through the AUKUS IFR, BIS removed the following list-based license requirements for items destined for Australia and the UK: Missile Technology (MT), NS (e.g., 600 series), Regional Security (RS), and Significant Items (SI) (e.g., hot section technologies and related items that give military aircraft engines critical performance advantages), as well as controls on dual-use night vision cameras and related items for military end-users. The AUKUS IFR also removed controls over a long list of specific types of items that could not be exported under License Exception STA, which was established during Export Control Reform to achieve collective security objectives (similar to those of AUKUS).[4]

Most encryption items subject to EI controls can already be exported, reexported, or transferred to or within Australia and the UK under License Exception ENC, but certain

---

[2] *International Traffic in Arms Regulations: Exemption for Defense Trade and Cooperation Among Australia, the United Kingdom, and the United States*, U.S. DEPARTMENT OF STATE, BUREAU OF INDUSTRY AND SECURITY, 89 Fed. Reg. 35028, May 1, 2024, https://www.govinfo.gov/content/pkg/FR-2024-05-01/pdf/2024-08829.pdf.

[3] *Why Do We Need Encryption Rules in the TPP?*, SEMICONDUCTOR INDUSTRY ASSOCIATION, Sep. 2013, https://www.semiconductors.org/wp-content/uploads/2018/06/Why-Do-We-Need-Encryption-Rules-in-the-TPP-Final-09-24-2013.pdf.

[4] *Export Control Reform Initiative: Strategic Trade Authorization License Exception*, U.S. DEPARTMENT OF COMMERCE, BUREAU OF INDUSTRY AND SECURITY, 76 Fed. Reg. 35,276, June 16, 2011, https://www.federalregister.gov/documents/2011/06/16/2011-14705/export-control-reform-initiative-strategic-trade-authorization-license-exception. A license is still required for (a) all destinations, including Australia, Canada, and the UK, for spacecraft and related items classified under ECCNs 9A515.a.1, .a.2., .a.3., .a.4., .g, and 9E515.f (*see* EAR § 742.6(a)(9)); and (b) for Australia and the UK of certain firearms and related items controlled under certain 0x5zz ECCNs (*see* new Footnote 9 to the Commerce Country Chart at Supp. No. 1 to EAR Part 738).

self-classification and/or CCATS requirements still apply. The AUKUS IFR removed certain semiannual reporting requirements for items exported to Australia and the UK, but those reports are still required for items reexported from Australia and the UK to third countries (*see* EAR § 740.17(e)).

In addition, there is no apparent policy rationale for a 600 series item or an item controlled for MT purposes to be no-license-required (NLR) for export to Australia or the UK under the AUKUS IFR on the one hand, but on the other hand a CCATS request is still required in order for a 5A002 encryption chip to be eligible for paragraph (b)(3) of license exception ENC. If BIS has assessed that Australia and the UK have robust enough export controls compliance programs in place to permit exports of MT and NS controlled items to these jurisdictions as NLR, then there is no apparent reason why BIS would continue to control exports of EI controlled items to the same jurisdictions.

Moreover, in the AUKUS IFR, BIS stated that under this rule, "Australia and the UK will have nearly the same licensing treatment under the EAR as Canada" and that the revisions would "further align the treatment of Australia, Canada, and the UK under the EAR." Yet, exports and reexports to Canada of encryption items are not subject to EI controls (*see* EAR § 742.15(a)). We therefore respectfully request BIS to fully harmonize its controls by removing EI controls for Australia and the UK as well.

We commend BIS for steadily loosening controls on encryption products and therefore reducing the regulatory burden on exporters. In March 2021, BIS issued a final rule eliminating reporting requirements for certain encryption items, including making certain mass market items eligible for self-classification and removing most mass market products from annual self-classification reports.[5] Eliminating EI controls for Australia and the UK would be in alignment with both past BIS rulemaking and the goals of AUKUS, and would further tighten the bonds between U.S. industry and customers in Australia and the UK.

Comment II.C: We ask BIS to consider the desirability of removing certain EAR controls to deepen technology and trade relationships with allies and partners.

Export control policy can be leveraged further to advance the principles of AUKUS. Mike Gallagher, former Chairman of the House Select Committee on the Chinese Communist Party, has advocated for the U.S. to continue reducing onerous restrictions on trade and technological collaboration with allies, stating that "there is no way to successfully compete against China…unless the U.S. is willing to assume risk and

[5] *Export Administration Regulations: Implementation of Wassenaar Arrangement 2019 Plenary Decisions; Elimination of Exporting Requirements for Certain Encryption Items*, U.S. DEPARTMENT OF COMMERCE, BUREAU OF INDUSTRY AND SECURITY, 86 Fed. Reg. 16,482, March 29, 2021, https://www.govinfo.gov/content/pkg/FR-2021-03-29/pdf/2021-05481.pdf.

break down all the barriers to collaboration both within the free world, and then constantly trying to expand the bounds of the free world."[6]

In a recent public comment submission, SIA urged USTR to leverage trade policy and market-opening trade initiatives and negotiations to boost demand for U.S. semiconductors and increase U.S. exports.[7] For such a trade policy to be effective, it will be important for export control policy to likewise facilitate secure commercial exchanges with friends and allies, rather than unnecessarily stifle cooperation.

For example, the U.S. and EU classify encryption items differently, meaning that in certain cases companies can rely on a license exception from one jurisdiction but not the other jurisdiction for the same transaction, while in other cases both the U.S. and EU might require a specific license for the same export. Senior BIS officials have indicated recently that the U.S. and the EU are seeking to harmonize export control regulations surrounding encryption items, including through the Trade and Technology Council. We encourage BIS to continue these efforts, and to eliminate overlapping license requirements where they occur.

Part III – General Comments on Encryption Controls

Comment III.A: We ask BIS to consider further revising the EAR's encryption controls for other allies and partner countries.

The functionality of semiconductors has constantly evolved to meet consumer demands, which have increasingly called for product features such as encryption. The use of encryption is not limited to government and military applications but has become standard for many information and communication technology (ICT) consumer goods such as smartphones, personal computers, smart home devices, connected vehicles, cloud storage platforms, and medical devices. Due to the global nature of the ICT supply chain, restrictions on the importation, sale, and use of encryption technology increase consumer costs and limit innovation.

Recognizing the importance of technological interoperability to promoting global economic growth, the Organization for Economic Cooperation and Development (OECD) outlined a set of cryptography guidelines in 1997.[8] The OECD stated that "due to the inherently global nature of and communications networks, implementation of incompatible [domestic] polices will not meet the needs of individuals, business and

---

[6] *National Security: Risks, Opportunities, and the Next Frontier of Critical Technologies (Panel)*, MILKEN INSTITUTE, May 6, 2024, https://milkeninstitute.org/panel/15586/national-security-risks-opportunities-and-next-frontier-critical-technologies.

[7] Comments of the Semiconductor Industry Association (SIA) on "Request for Comments on Promoting Supply Chain Resilience," (89 Fed. Reg. 16608 (March 7, 2024)), April 22, 2024, https://www.regulations.gov/comment/USTR-2024-0002-0135.

[8] *Guidelines for Cryptography Policy*, ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, March 27, 1996, https://legalinstruments.oecd.org/public/doc/115/115.en.pdf.

governments and may create obstacles to economic co-operation and development; and therefore [domestic] policies may require international co-ordination."

An example of more current "best practices" in this area are the Encryption Principles developed by the World Semiconductor Council (WSC) and endorsed at the Government and Authorities Meeting on Semiconductors (GAMS) since 2010. These principles state that "generally there should be no regulation of cryptographic capabilities in widely available products used in the domestic commercial market," and "commercial encryption products should not be regulated except in narrow and justifiable circumstances."[9] SIA and other members of the WSC have historically advocated for these encryption principles to be included in trade agreements being negotiated or contemplated by WSC governments and authorities.

As noted previously, BIS issued a final rule eliminating reporting requirements for certain encryption items, including making certain mass market items eligible for self-classification and removing most mass market products from annual self-classification reports.[10] BIS should review the existing EI controls (and corresponding National Security, Column 1 (NS1) controls for 5x002 items) to determine whether there remains a justifiable reason to continue to control the items subject to those controls based on the way the items are sold and used, and whether comparable encryption items are available in other jurisdictions.

BIS has in recent years included carveouts from new export controls for allied and partner countries. For example, BIS included a carveout in the new semiconductor manufacturing and advanced computing rules, which were promulgated for national security reasons, for items destined to allied countries – i.e., to countries identified in both Country Groups D:1, D:4, or D:5 and also A:5 or A:6 (EAR §§ 742.6(a)(6)(ii), (iii)). Moreover, BIS included a carveout for items subject to the EAR under the Russia/Belarus/Crimea foreign-direct product rule (FDPR) at EAR §734.9(f) and the Russia/Belarus military end user (MEU) FDPR at EAR § 734.9(g) for items exported or reexported from an allied country identified in Supp. 3 to EAR Part 746, meaning that BIS trusts these allied countries to regulate these items. *See* EAR §§ 746.8(a)(4).

BIS should take a similar approach to encryption controls for allies and partner countries, as follows:

- BIS could, for example, consider removing EI controls for some or all currently EI-controlled items destined for (a) all Country Group A:5 and A:6 countries, (b)

---

[9] *WSC Encryption Principles*, World Semiconductor Council, May 23, 2013, http://www.semiconductorcouncil.org/public-documents/public-documents-and-white-papers/.

[10] *Export Administration Regulations: Implementation of Wassenaar Arrangement 2019 Plenary Decisions; Elimination of Exporting Requirements for Certain Encryption Items*, U.S. DEPARTMENT OF COMMERCE, BUREAU OF INDUSTRY AND SECURITY, 86 Fed. Reg. 16,482, March 29, 2021, https://www.govinfo.gov/content/pkg/FR-2021-03-29/pdf/2021-05481.pdf.

all Country Group A:1 countries, or (c) countries already listed in Supp. 3 to EAR Part 740 (which closely aligns, but does not exactly overlap, with Country Group A:1).

- In conjunction with easing the EI controls, BIS could ease NS1 controls (e.g., by shifting the controls from NS1 to National Security, Column 2 (NS2)) for these destinations, at least for items that BIS has already identified as less-sensitive EI-controlled items – i.e., those described in paragraphs (b)(1) or (b)(3) of License Exception ENC – which would allow BIS to preserve tighter controls around the most sensitive encryption items – i.e., those already described in paragraph (b)(2) of License Exception ENC.

- Alternatively, BIS could retain EI and NS1 controls for all currently EI-controlled items destined for all locations (except Australia, Canada, and the UK, as discussed in our Comment III.B above), but consider eliminating the need for CCATS, self-classification reports, and/or semi-annual sales reports for items destined to either (a) all Country Group A:5 or A:6 countries, (b) all Country Group A:1 countries, or (c) countries already listed in Supp. 3 to Ear Part 740 (which closely aligns, but does not exactly overlap, with Country Group A:1).

- In either case, end-use and end-user controls at EAR § 744 already apply to many EI-controlled items, and could continue to apply to ensure that EI-controlled items are not used for purposes that would be contrary to U.S. national security or foreign policy interests.

* * *

Thank you for the opportunity to comment on the AUKUS IFR. If you have any additional questions or would like to discuss these comments further, please contact SIA via mthornton@semiconductors.org.

Uploaded to www.regulations.gov. ID – BIS-2023-0019-0001

Courtesy copy sent to: Eileen.Albanese@bis.doc.gov.