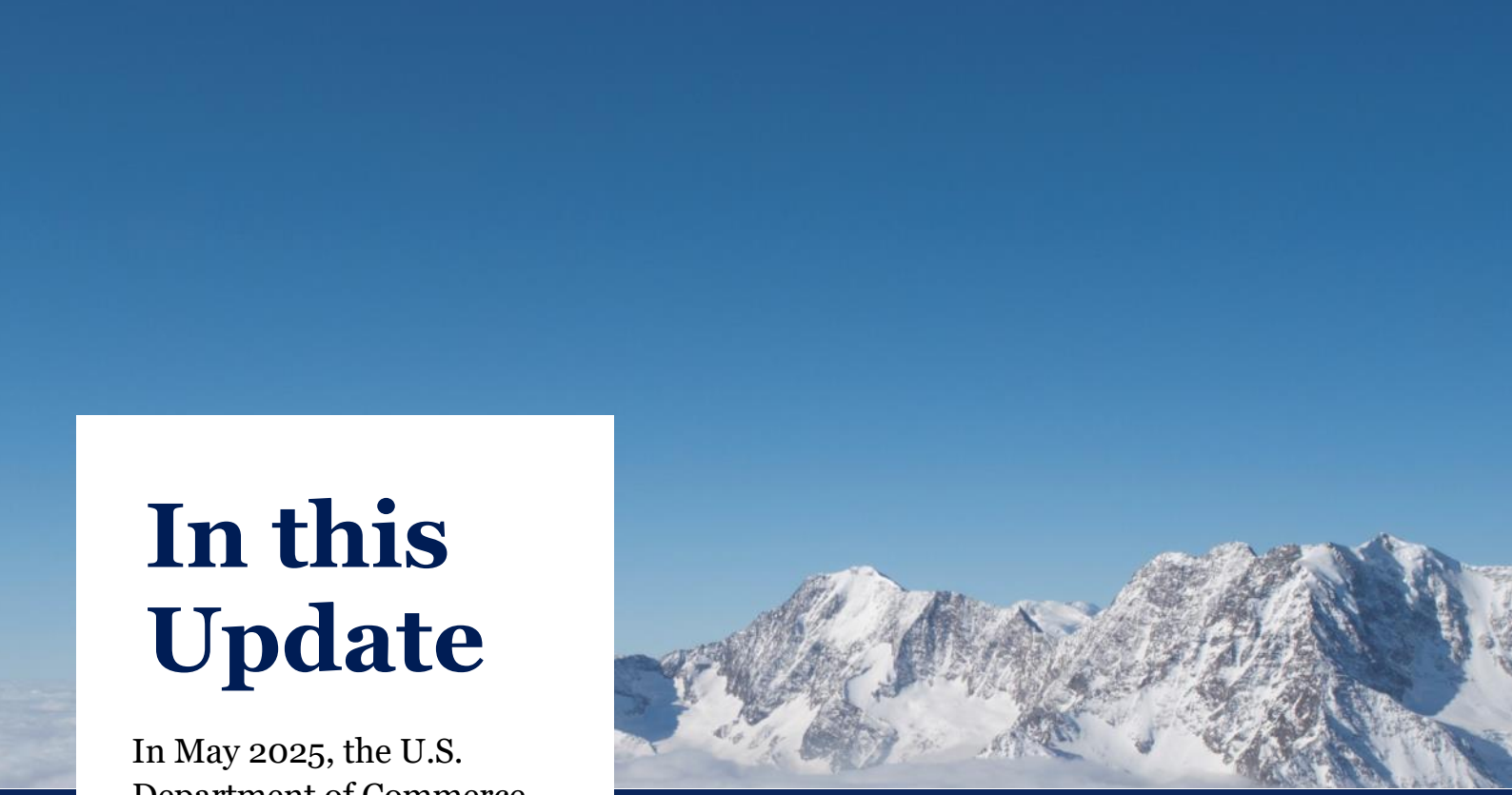
DREW & NAPIER

THE HUAWEI AI-CHIP RESTRICTIONS AND ITS IMPLICATIONS FOR COMPANIES OPERATING IN SINGAPORE

2 June 2025

LEGAL UPDATE



In this Update

In May 2025, the U.S. Department of Commerce, through the Bureau of Industry and Security, issued guidance which clarified that the use of Huawei Technologies Co., Ltd AI Processor Chips anywhere in the world would amount to a violation of the U.S. Export Administration Regulations.

In this update, we examine the implications of this guidance for companies operating in Singapore. While Singapore is not obligated to enforce U.S. export controls, Singapore-based companies that attempt to circumvent U.S. export controls could nonetheless face criminal liability under Singapore criminal law, drawing on recent enforcement examples such as the Nvidia Chips Incident. This update also outlines a risk-based compliance framework to help Singapore-based companies navigate this evolving regulatory landscape.

I. THE EXPORT ADMINISTRATION REGULATIONS

A. Restrictions on the use of Huawei Technologies Co., Ltd ("Huawei") AI Processor Chips anywhere in the world

On 13 May 2025, the United States of America ("**U.S.**") Department of Commerce, through the Bureau of Industry and Security ("**BIS**"), issued formal guidance warning that the use of Huawei's latest Ascend 910B, 910C, and 910D AI processor chips (collectively, "**Processor Chips**") anywhere in the world would violate U.S. export controls[1].

The Trump administration justified this on national security grounds and stated that the Processor Chips, which are designed by Huawei, a company headquartered in the People's Republic of China ("**PRC**"), are likely produced in violation of the Export Administration Regulations ("**EAR**"). The Processor Chips are likely "*either designed with certain U.S. software or technology or produced with semiconductor manufacturing equipment that is the direct product of certain U.S.-origin software or technology, or both*"[2]. Accordingly, the **use** of such Processor Chips may amount to a violation of General Prohibition 10 of the EAR, which reads (§ 736.2(b)(10) of 15 Code of Federal Regulations ("**CFR**")):

> *"You may* ***not sell, transfer, export, reexport, finance, order, buy, remove, conceal, store, use, loan, dispose of, transport, forward, or otherwise service, in whole or in part, any item subject to the EAR and exported, reexported, or transferred (in-country) or to be exported, reexported, or transferred (in-country) with knowledge that a violation of the Export Administration Regulations****, the Export Control Reform Act of 2018, or any order, license, license exception, or other authorization issued thereunder has occurred, is about to occur, or is intended to occur in connection with the item. Nor may you rely upon any license or license exception after notice to you of the suspension or revocation of that license or exception. There are no license exceptions to this General Prohibition Ten in part 740 of the EAR."*
>
> (emphasis added)

The latest guidance is not a new rule *per se*, but rather a "*public confirmation of an interpretation that even the mere use anywhere by anyone of a Huawei-designed advanced computing [integrated circuit] would violate export control rules*"[3]. The continued use of the Processor

[1] BIS, Guidance on Application of General Prohibition 10 (GP10) to People's Republic of China (PRC) Advanced-Computing Integrated Circuits (ICs) ("**Guidance on Application of GP10**") at page 2.
[2] Guidance on Application of GP10 at page 2.
[3] Financial Times, US warns against using Huawei chips 'anywhere in the world' (14 May 2025) at https://www.ft.com/content/2033b5b3-974d-4d40-8498-1c46d3a8db79.

Chips would therefore be viewed as a violation of the EAR and subject companies to BIS enforcement action.

B. The extraterritorial application of the U.S. Export Administration Regulations

The U.S. EAR identifies the scope of the items that are subject to the EAR, as set out in § 734.3(a) of the CFR:

> *(a) Except for items excluded in paragraph (b) of this section, the following items are subject to the EAR:*
>
> > *(1) All items in the United States, including in a U.S. Foreign Trade Zone or moving in transit through the United States from one foreign country to another;*
> >
> > *(2) All U.S. origin items wherever located;*
> >
> > *(3) Foreign-made commodities that incorporate controlled U.S.-origin commodities, foreign-made commodities that are 'bundled' with controlled U.S.-origin software, foreign-made software that is commingled with controlled U.S.-origin software, and foreign-made technology that is commingled with controlled U.S.-origin technology:*
> >
> > > *(i) In any quantity, as described in § 734.4(a) of this part; or*
> > >
> > > *(ii) In quantities exceeding the de minimis levels, as described in § 734.4(c) or § 734.4(d) of this part;*
> >
> > *(4)* ***Certain foreign-produced "direct products" of specified "technology" and "software," as described in § 734.9 of the EAR; and***
> >
> > *(5) Certain foreign-produced products of a complete plant or any major component of a plant that is a "direct product" of specified "technology" or "software" as described in § 734.9 of the EAR.*
> >
> > (emphasis added)

EAR jurisdiction will be triggered when **any person** has possession of foreign-produced *"direct products"* of specified *"technology"* and *"software"*, including the Processor Chips. Accordingly, **any person** who intends to use such Processor Chips, regardless of whether they are in the U.S. or not, are expected to comply with EAR regulations.

It is clear that the BIS is ready and willing to exercise extraterritorial jurisdiction to prosecute any violation of the EAR. In April 2023, BIS announced a US$300 million settlement with Seagate US and **Seagate Singapore**, including a mandatory multi-year audit and a five-year suspended denial order, to resolve alleged export violations related to the

sale of hard disk drives to Huawei[4]. Earlier, in May 2019, the BIS had added Huawei and its non-U.S. affiliates to the Entity List, and imposed licensing requirements on the exports, re-exports and transfers (in-country) of all items subject to the EAR destined to or involving these listed Huawei entities. In August 2020, BIS included additional Huawei affiliates on the Entity List and imposed further licensing requirements[5].

Despite these licensing requirements, Seagate U.S., Seagate Singapore and other affiliates repeatedly engaged in transactions with Huawei without BIS authorization and therefore violated US export controls[6]. The Seagate incident demonstrates the BIS's readiness to pursue extraterritorial enforcement against non-U.S. affiliates of U.S. companies.

II. LOCAL ENFORCEMENT REGIMES MAY APPLY

A. No obligation for Singapore to enforce US laws, although companies operating in Singapore are cautioned to obey other countries' laws

The Singapore government has no obligation to enforce other countries' regulations, including the U.S. EAR. However, the Singapore Ministry of Trade and Industry, as well as the Singapore Customs, has issued a Joint Advisory[7] stating that:

> "*Businesses operating in Singapore should also remain informed of and take into account the implications of other countries' export controls on their international business activities. The Singapore Government does not condone businesses deliberately using their association with Singapore to circumvent or violate the export controls of other countries. This applies to all our trading partners.*"[8]

The Joint Advisory explicitly states that the Singapore Government does not condone businesses deliberately using their association with Singapore to circumvent the export controls of other countries, and that action will be taken against those who engage in dishonest practices to evade applicable export controls.

The Joint Advisory also adds that "*all companies operating in Singapore must conduct their activities transparently and in full compliance with these*

[4] BIS, BIS imposes $300 Million Penalty Against Seagate Technology LLC Related To Shipments To Huawei: Largest Standalone Administrative Penalty in BIS History (19 April 2023) ("**BIS imposes $300 Million Penalty Against Seagate Related To Shipments To Huawei**") at page 1.
[5] Federal Register, Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) (17 August 2020) at https://www.federalregister.gov/documents/2020/08/20/2020-18213/addition-of-huawei-non-us-affiliates-to-the-entity-list-the-removal-of-temporary-general-license-and
[6] BIS imposes $300 Million Penalty Against Seagate Related To Shipments To Huawei at page 1
[7] Ministry of Trade and Industry Singapore, Joint Advisory: Export controls on advanced semiconductor and artificial intelligence (AI) technologies (4 April 2025) ("**Joint Advisory**")
[8] Joint Advisory at [4]

laws and regulations, and that firm and decisive action will be taken against any violations"[9].

B. Importing / Exporting the Processor Chips may lead to criminal liability in Singapore

The Joint Advisory is likely targeted at companies which may have deployed concealment strategies to disguise their trade of Processor Chips. Depending on the circumstances of each case, concealing the use of Processor Chips may lead to the following criminal offences in Singapore:

(i) Section 424B of the Penal Code 1871

Fraud by false representation is an offence under Section 424B of Singapore's *Penal Code 1871* ("**PC**"):

> ***Fraud by false representation, non-disclosure or abuse of position***
>
> *424B.—(1) A person shall be guilty of an offence if he, fraudulently or dishonestly —*
>
> *(a) makes a false representation;*
>
> *(b) fails to disclose to another person information which he is under a legal duty to disclose; or*
>
> *(c) abuses, whether by act or omission, a position which he occupies in which he is expected to safeguard, or not to act against, the financial interests of another person.*
>
> *(2) A person may be guilty of an offence under subsection (1) whether or not the acts in subsection (1)(a), (b) or (c) were material.*
>
> *(3) A person who is guilty of an offence under subsection (1) shall on conviction be punished with imprisonment for a term which may extend to 20 years, or with fine, or with both.*

Section 424B of the PC may be triggered where:

- a company makes false declarations about the end-recipient of the Processor Chips. In a recent Singapore case involving the alleged illegal movement of Nvidia chips to the PRC, three men were charged under Section 424B of the PC ("**Nvidia Chips Incident")**[10]; or
- a company makes false declarations about the manufacturer of the chips, including by falsely representing that the Processor Chips are manufactured by a different manufacturer.

[9] Joint Advisory at [3]

[10] Ministry of Home Affairs Singapore, Transcript of Media Conference With Mr K Shanmugam, Minister for Home Affairs and Minister for Law, Regarding the Case Involving the Three Men Who Were Charged on 27 February 2025 for Fraud by False Representation (3 March 2025) at https://www.mha.gov.sg/mediaroom/speeches/transcript-of-media-conference-with-mr-k-shanmugam-minister-for-home-affairs-and-minister-for-law-regarding-the-case-involving-the-three-men-who-were-charged-on-27-february-2025-for-fraud-by-false-representation/

Upon conviction, an offender shall be punished with imprisonment for a term which may extend to 20 years, or with fine, or with both.

(ii) Section 424 of the Penal Code 1871

The dishonest or fraudulent concealment of property is an offence under Section 424 of the PC:

> ***Dishonest or fraudulent removal or concealment of property or release of claim***
>
> *424. Whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any demand or claim to which he is entitled, shall be punished with imprisonment for a term which may extend to 3 years, or with fine, or with both.*

Section 424 of the PC may be triggered where:

- a company makes false declarations about the end-recipient of the Processor Chips. While such an act will be caught under Section 424B of the PC (as explained above), such an act may also be caught under Section 424 of the PC if it is shown that the goal of the company making such false declarations is to dishonestly or fraudulently conceal their ownership of the Processor Chips; or
- there are acts of fraud or dishonesty involved in routing Processor Chips through shell companies or third-party entities, and the goal of the company routing the Processor Chips through such intermediaries is to conceal their ownership of the Processor Chips.

Upon conviction, an offender shall be punished with imprisonment for a term which may extend to 3 years, or with fine, or with both.

III. KEY LEARNING POINTS FOR COMPANIES OPERATING IN SINGAPORE

Companies must be cognisant of the fact that operating in Singapore does not insulate them from liability, especially when engaging in activities that conceal the use of restricted technologies.

Creative concealment strategies to circumvent U.S. export controls, such as rebranding the Processor Chips under a different name, obscuring the true manufacturer of the Processor Chips (i.e. *"white-labelling"*) or concealing the end-user of the Processor Chips may attract criminal liability under Singapore's own laws. This is in addition to enforcement actions which might be taken by the BIS independently. Singapore's response to the

Nvidia Chips Incident offers a cautionary example of what may happen if companies operating in Singapore attempt to circumvent the U.S. EAR.

To mitigate these risks, companies should adopt a unified, risk-based compliance framework that integrates U.S. EAR requirements with Singapore laws:

(a) companies should conduct a forensic mapping of their supply chain to trace component origins, verify end-use and end-user authenticity, and identify the presence of shell companies or third-party entities;

(b) companies should conduct targeted training and awareness programs particularly for procurement, logistics, sales, and legal teams. Training must emphasize the legal ramifications of false statements, fraudulent documentation, and concealment of critical information. Companies should also share about real-world case studies such as the Nvidia Chips Incident, which among other things, underscore the risks and consequences of false representations;

(c) companies should deploy real-time transaction-screening tools that automatically flag suspicious transshipment routes and transactions, anomalies in end-use declarations, and other indicators of potential non-compliance;

(d) companies should establish secure, anonymous whistleblower channels to encourage internal reporting of suspected violations or false representations, ensuring prompt investigation and remediation; and

(e) companies should engage local counsel to monitor evolving enforcement trends - ensuring that companies are apprised of new legal developments and allowing them to adapt their compliance framework to new laws and export control regimes. This is consistent with the recommendation in the Joint Advisory to seek legal expertise where necessary[11].

IV. CONCLUSION

Given the current state of US-China relations, navigating the global supply chain is fraught with difficulty. Companies operating in or from Singapore, besides grappling with the extra-territorial nature of the U.S., should be cognisant that actions such as *"white-labelling"* or concealing the ultimate recipient of goods subject to U.S. export controls may attract additional criminal liability locally. Companies should likewise not abuse their association with Singapore to circumvent U.S. export controls. Companies would do well to adopt a risk-based compliance framework as outlined above.

[11] Joint Advisory at [6(b)]

If you have any questions or comments on this article, please contact:

Gary Low
Director, Dispute Resolution
Co-Head, Criminal Law Practice

T: +65 6531 2497
E: gary.low@drewnapier.com

Victor David Lau
Associate Director, Dispute Resolution

T: +65 6531 2491
E: victordavid.lau@drewnapier.com

Drew & Napier LLC
10 Collyer Quay
#10-01 Ocean Financial Centre
Singapore 049315

www.drewnapier.com
T : +65 6535 0733
T : +65 9726 0573 (After Hours)
F : +65 6535 4906

DREW & NAPIER