NASSCOM®

Cryptographic Information Security

And

Export Controls in India

Category 8A502 of the SCOMET List

October 2021

Table of Contents

PREFACE

Export controls applicable to cryptographic information security items, software or technology are of importance to India's information technology industry. As the representative of this industry, NASSCOM has been playing a significant role in the overall improvement of India's export control regime.

This paper highlights the challenges faced by the industry in classifying cryptographic information security items, software, or technology under the relevant category of the SCOMET list. It details out the approaches adopted by other jurisdictions towards controlling cryptographic information security and suggests adopting some of these best practices in India.

The paper intends to serve as an input for the improvement on India's export control regime generally, and as applicable to cryptographic information security, specifically. The paper is not a legal opinion.

We hope this paper will help strengthen the SCOMET list by providing the necessary guidance to industry, as well as easing the compliance burden as per the ways identified in this paper.

I would like to acknowledge the valuable contributions from various experts in the field of export controls, members of the information technology (hardware and software) industry and my colleague Garima Prakash who has led this project. Should you have any questions or concerns relating to this paper, I request you to share them with us at policy@nasscom.in.

Ashish Aggarwal
Vice President and Head of Public Policy
NASSCOM

EXECUTIVE SUMMARY

The increasing commercial availability of cryptography as an information security tool in consumer applications, led to the classification of information security products and technology as "dual-use". Consequently, information security products and technology are subject to export control restrictions under the export control regime of India and many other countries. India maintains controls over the exports of information security products and technology through Category 8A5 Part 2 of the Special Chemicals, Organisms, Materials, Equipment and Technologies (**SCOMET**) List.

For the overall improvement of the export control regime as applicable to cryptographic information security items, software and technology in India, our study suggests the following:

1. Guidance is needed from the government for appropriate classification by the industry under the relevant text of Category 8A5 Part 2 of the SCOMET list. Specifically, there is a need for clarity on various terms and phrases, including:
    - What would constitute '*of potential interest to a wide range of individuals and businesses'* as given under Note to Cryptography Note of Category 8A502 of the SCOMET list.
    - Whether '*cryptographic functionality cannot easily be changed by the user'* as given under Cryptography Note would include turning on and off the encryption facility.
    - The meaning of primary function and non-primary functions as given under Category 8A502 a. of the SCOMET list.

2. There are approaches from other countries which can be adapted by India, given our early stage in the export control regime, which will improve the overall regime as well as assist the industry in complying with obligations. These include:
    - Introduction of bulk licences for certain cryptographic information security items, software or technology along with appropriate safeguards in the form of post-reporting requirements, implementation of internal compliance programme etc. This will significantly reduce the compliance burden on the industry.
    - Creation of a helpdesk to promptly assist the industry with classification queries. This will assist the industry in avoiding mis-classification or non-classification errors.
    - Complete digitisation of the SCOMET licensing process, that will enable the applicant to track the application status in real-time, submit and exchange all relevant application related documents in a centralised system and enable a two-way communication between applicant and licensing authority for timely resolution of gaps in the application.

INTRODUCTION

Prior to the dawn of the 'information age', cryptography and information security technology were the exclusive domain of military and intelligence applications. Cryptography and information security products were earlier classified as ammunition. However, the past three decades, have witnessed an exponential use in the use of cryptography in retail and consumer technologies, as an essential tool towards operationalising individual privacy. This has opened up new forefronts in the policy discourse surrounding regulation of cryptography and information security products.

The increasing commercial availability of cryptography as an information security tool in consumer applications, led to the classification of information security products and technology as "dual-use". Consequently, information security products and technology are subject to export control restrictions under the Wassenaar Agreement (**WA**).

The objective of the WA is to maintain international security, and ensure non-proliferation, by promoting transparency and responsible transfers of arms and dual-use technology, i.e., technology having potential military as well as civilian applications. The WA recognised that cryptography and information security products had significant civilian applications such as securing data over digital networks. Resultantly, the information security products that incorporate encryption technology for certain functions, were made subject to the controls specified under the WA. The way the signatory countries implemented the export control restrictions flowing from the WA, remained a subject of national legislation.

India acceded to the WA in 2017 and maintains controls over the exports of information security products and technology through Category 8A5 Part 2 of the Special Chemicals, Organisms, Materials, Equipment and Technologies (**SCOMET**) Licensing regime. Even though encryption technology is widely used for civil (non-military) purposes, the obligations for obtaining an export licence for export of items incorporating encryption technology for civil and military use remain largely the same in India.

While the WA list of dual-use goods and technologies controls both – cryptographic and non-cryptographic information security, in this paper, we will focus only on cryptographic information security.

This paper discusses the Indian export control regime as it applies to products, software and technology incorporating encryption. In doing so, the paper:

1. highlights the need for clarity on various terms and phrases used in Category 8A5 Part 2 of the SCOMET list,
2. discusses approaches adopted by other jurisdictions to controlling cryptographic information security, and
3. proposes a way forward for the improvement in the implementation of export control laws as applicable to cryptographic information security in India as well as assist the industry in complying with export control obligations.

EXPORT CONTROL REGIME IN INDIA

India aligns its domestic laws with its obligations under the WA through the list of SCOMET items, i.e., Special Chemicals, Organisms, Materials, Equipment and Technologies. Accordingly, Chapter IV A of the Foreign Trade (Development & Regulation) Act, 1992 deals with the SCOMET items and lists out the controls on export of specified goods, software, and technologies.

Cryptographic Information Security (systems, equipment, and components) is controlled under Category 8A502 of the SCOMET list, thereby requiring a licence for exporting items that fall in this category. The controls apply to those using symmetric algorithms with a key length over 56 bits or asymmetric algorithms with a key length over 512 bits. In practice, most encryption protocols use key lengths exceeding these levels and therefore are subject to the regulations. Consequently, irrespective of the end-use of the technology (i.e., civilian, or military applications), cryptography products, software, and technology, if they fall under Category 8A502 of the SCOMET list, require an export licence.

Export control of cryptography for civil-use

Companies routinely incorporate cryptography in software to enable data confidentiality, such as, for compliance with data protection legislation (for example, European Union's (**EU**) General Data Protection Regulation). Export control laws applicable to cryptography for data confidentiality in India, mandate the requirement of an export licence, irrespective of the end-use of the item/software being exported, provided it does not fall under the Cryptography Note or any of the technical notes given under 8A502a of the SCOMET list. As a result, an individual export licence is sought by the exporter in India, even if cryptographic functionality is for the limited purposes, such as securing personal data, each time an item that incorporates controlled encryption technology is exported.

The process from application to grant of licence sometimes takes as long as a few months. This causes a burden on the industry that heavily uses encryption for data confidentiality for civil end-use. There is a need for discussing the scope under Indian regime to introduce reduced obligations concerning export controls, in case of export of less sensitive items or software that incorporate cryptography for civil-use. This may be introduced through incorporating end-used based relaxations in licencing obligations.

Need for clarifications under Category 8A5 Part 2

The need for an export licence is determined by assessing whether the item, software or technology incorporating cryptography falls under the scope of the SCOMET list. To ascertain this, a company usually undertakes an applicability and classification exercise to map out the item, software, or technology to be exported vis-à-vis the provisions of the SCOMET list along with all the exceptions and technical notes therein. This classification is made solely on the basis of the text of the SCOMET list.

This section highlights with the help of examples, the need for clarity on various terms and phrases used in Category 8A5 Part 2 of the SCOMET list, to enable exporting companies to accurately identify the items, software or technology that require a SCOMET licence. Owing to these ambiguities under

the existing export control laws, companies in India are uncertain as to the requirement of obtaining an export licence for export of items and software which incorporate encryption technology.

i. Primary versus non-primary function

Category 8A502 of the SCOMET list differentiates, inter alia, based on cryptographic functionality being applicable for primary versus non-primary use of items. The SCOMET list covers:

(i) items with information security as a primary function; and
(ii) (where cryptography for data confidentiality supports the non-primary function of the item.

This means, that when information security is not the primary function of an item but cryptography for information security supports the primary function of an item, it does not require a SCOMET licence. However, there is no clarity among the industry to conclusively determine the definition of primary and non-primary functions. The ambiguity lies in determining what is the primary function of the item, i.e., whether it is the main purpose itself, or the functions that it performs to fulfil the main purpose.

For example, consider a data automation product that uses cryptography to secure personal data stored on the device. The main purpose of this product is data automation. For this, the product performs functions like data collection and data analysis. In this case, whether the primary function of the product is data automation or data collection and data analysis, remains unclear. There does not exist a standard practice among the industry in this regard.

- One company may interpret this to mean that data automation is the primary function and data collection which uses cryptography for information security is the non-primary function. Therefore, a SCOMET licence is required, as cryptography for information security is being used to support the non-primary function of data collection.
- Another interpretation could be that data automation is the primary function of this product, and the cryptographic functionality (i.e., securing data stored on the device) is purely to enable it to fulfil the primary function more efficiently. Therefore, this is out of the scope of Category 8A502.
- Another company may interpret it to mean that data automation is the purpose, while data collection is the primary function. Therefore, SCOMET licence is not required, as information security is neither the primary function nor is cryptography for information security being used to support a non-primary function.

Box 1: Overview of Category 8A502 a

"Information security" systems, equipment, and components, as follows:
A. Designed to use cryptography for data confidentiality, having a described security algorithm, where that cryptographic capability is usable, has been or can be activated by any means other than secure cryptographic activation, as follows:

1. Items having information security as a primary function;
2. Digital communication or networking systems, equipment or components;
3. Computers or other items having information storage/processing as a primary function;
4. Where cryptography for data confidentiality supports a non-primary function of the item;

Exclusions:

- Performing cryptographic function that is for authentication, digital signature, data integrity, non-repudiation, digital rights management
- Certain smart cards/ smart card readers and writers
- Cryptographic equipment specially designed and limited for banking use or money transactions
- Portable or mobile radiotelephones for civil-use; certain cordless telephone equipment
- Certain items where information security functionality is limited to wireless personal area network functionality implementing only published or commercial cryptographic standards
- Mobile telecommunications Radio Access Network (RAN) equipment designed for civil-use
- Routers, switches, gateways or relays where information security functionality is limited to the tasks of Operations, Administration or Maintenance ("OAM") implementing only published or commercial cryptographic standards
- Certain general purpose computing equipment or servers
- Certain items specially designed for a connected civil industry application

B. Designed or modified to enable an item to achieve or exceed the controlled performance levels for functionality specified by 8A502.a by means of cryptographic activation
C. Designed or modified to use or perform quantum cryptography
D. Designed or modified to use cryptographic techniques to generate channelising codes, scrambling codes or network identification codes
E. Designed or modified to use cryptographic techniques to generate the spreading code for spread spectrum systems, including the hopping code for "frequency hopping systems.

Suggested Solution:

- Guidance on the meaning of primary and non-primary function is necessary. For example, it may be clarified that primary function denotes the 'main purpose' of the item/software. Therefore, in the above example of a data-automation software, the primary function is data automation. Cryptographic functionality is purely to enable the performance of data automation in a proper manner, and therefore, cryptographic functionality supports the primary function. Accordingly, this falls outside of the scope of 8A502a.
- Guidance could also be given in the form of examples of what could be entailed under each of the paragraphs a. to d. of 8A502.
- It can also be in the form of a guidance note explaining the intent and purpose of adding this criterion in the text of Category 8A502 or corresponding Category 5 Part 2 of the Wassenaar Arrangement List of Dual-Use Goods and Technology.

In the US, the Bureau of Industry and Security (**BIS**) has released guidance material which enables the industry to determine what would classify as a controlled item under the US Commerce Control List. The guidance specifically on encryption items is available here.[1] This clarifies that the primary

[1] Items in Category 5 Part 2, US BIS, available here: https://www.bis.doc.gov/index.php/policy-guidance/encryption/2-items-in-cat-5-part-2/a-5a002-a-and-5d002-c-1/iv-5a002-a-1-a-4 (Last accessed on 30 September 2021).

function is the obvious or main purpose of the item. It is the function which is not there to support other functions. Similarly, the UK government clarifies the meaning of primary function and supporting the non-primary function in a note to exporters, by taking the example of a vending machine:[2]

> *"The vending machine has a primary function of supplying drinks. To support this primary function, the machine performs other tasks such as taking payment and managing stock levels… [T]he vending machine's primary function is not 'information security'. It's not a digital communication or networking system and it does not have information storage or processing as a primary function…. the machine would use cryptography with a key size over 56 bits (or equivalent) but this cryptography supports the primary function of supplying drinks. Assuming that the wifi connectivity is conducted by a standard COTS (commercial off-the-shelf) wifi chip, then this component would almost certainly not be controlled by Category 5 Part 2 because it would meet the decontrol conditions of Note 3." **

* Note 3 and Category 5 Part 2 is referred to as per the WA list of dual-use goods and technologies.

ii. Customisable items and changing the cryptographic functionality

Many Indian Information Technology (**IT**) – Business Process Management (**BPM**) companies export customised software which incorporates encryption functionality for the purposes of, for example, data confidentiality. According to the cryptography note (see Box 2 below), exporters are required to obtain an export licence if the feature set of the software is designed to customer specification and go beyond the exemptions given under the technical notes to 8A502a; this is often the case in business-to-business transactions. Moreover, many Indian companies produce items in which cryptographic functionality can be modified by the user to provide an encryption different to the originally programmed encryption. For example, an external solid-state drive (**SSD**) made to customisation, that can store data in encrypted or decrypted form, depending on the activation of this functionality by the user. In this case, there is ambiguity among the industry on the meaning of 'cryptographic functionality cannot be easily changed by the user'. The question is: (a) whether any modification in cryptography (even, turning on and off encryption facility) amounts to cryptographic functionality 'being easily changed by the user'; (b) whether changing the cryptographic functionality is relevant only if modifications are to provide an encryption different to the one originally programmed and sold to the user; and (c) ambiguity on the extent of *'ease'* of changing the cryptographic functionality.

Suggested Solution:

- Clarification is needed that changing the cryptographic functionality is relevant only if modifications are to provide an encryption different to the one originally programmed and sold to the user, and that merely switching the cryptographic functionality on or off would not suffice.
- Guidance may also be given in the form of a note explaining the intent and purpose of adding this criterion in the text of Category 8A502 or corresponding Category 5 Part 2 of the Wassenaar Arrangement List of Dual-Use Goods and Technology.

[2] Notice to exporters 2018/03: updates to controls on 'information security' products using cryptography, Department for International Trade, Government of UK, available here: https://www.gov.uk/government/publications/notice-to-exporters-201803-updates-to-controls-on-information-security-products-using-cryptography/notice-to-exporters-201803-updates-to-controls-on-information-security-products-using-cryptography (Last accessed on 30 September 2021).

Box 2: Overview of Cryptography Note and Note to Cryptography Note

The 'Cryptography Note' provides various conditions under which an item, associated software and component would not require a SCOMET licence. This includes items meeting all of the following:

A. Items that are:
   1. Generally available to the public by being sold without restriction at retail selling points by way of over-the-counter transactions, mail order transactions, electronic transactions or telephone call transactions;
   2. The cryptographic functionality cannot easily be changed by the user;
   3. Designed for installation by the user without further substantial support by the supplier; and
   4. When necessary, details of the goods will be provided upon request to the appropriate authority in India to ascertain compliance with conditions described in 1. to 3. above.

   AND

   - The item must be of potential interest to a wide range of individuals and businesses; and
   - The price and information about main functionality of the item must be available before purchase without the need to consult the vendor or supplier.

B. Hardware components or executable software of items described in paragraph A above, in which:
   1. Information security is not the primary function;
   2. It does not change any cryptographic functionality or add new cryptographic functionality to the item;
   3. The feature set is fixed and not customisable; and
   4. When necessary, details of the goods will be provided upon request to the appropriate authority in India to ascertain compliance with conditions described in 1. to 3. above.

iii. Potential interest to a wide range of individuals and businesses

There is lack of clarity on the meaning of '*potential interest to a wide range of individuals and businesses*'. Companies export items that incorporate encryption functionality to certain enterprises. There is lack of clarity on whether an item or software that incorporates encryption functionality and is of interest to a segment of customers, would qualify as being of interest to a wide range of individuals and businesses. There is no standard industry practice in this regard. For instance, high capability hard disks which are developed for enterprise segments, may or may not classify as being of potential interest to a wide range of individuals and businesses.

Suggested solution: Clarification is needed on what will constitute '*wide range of individuals and businesses*'. It may be in the form of a note explaining the intent and purpose of adding this criterion in the text of Category 8A502 or corresponding Category 5 Part 2 of the Wassenaar Arrangement List of Dual-Use Goods and Technology.

APPROACHES TO CONTROLLING CRYPTOGRAPHIC INFORMATION SECURITY

Information security products that incorporate encryption technology for certain functions are subject to the controls specified under the WA. The way the signatory countries implemented the export control restrictions flowing from the WA, remained a subject of national legislation. Resultantly, there are different approaches undertaken by various jurisdictions to control export of items that perform cryptographic functionality.

Many countries incorporate relaxed licensing requirements in their export control laws for cryptographic information security products which range from mere record-keeping requirements to reporting requirements. Moreover, in many jurisdictions, the government authority responsible for issuing the export licence, provides for guidance and advisory opinions to clarify classification queries by the industry on a case-to-case basis. The various approaches to controlling cryptographic information security can be categorised in the following 4 ways:

1) Individual Export Licences;
2) Bulk Licences/General Licences;
3) Licence Exceptions; and
4) Periodic revision of dual-use list.

(1) Individual Export Licences

Here, exporters of controlled items, software or technology are required to obtain an individual export licence, irrespective of the end-use of the item/software being exported. The exceptions for requiring an individual export licence are restricted to the ones given under the WA List of Dual-Use Goods and Technology itself. India primarily follows this regime for export of items, software and technology falling under Category 8A5 Part 2 of the SCOMET List. Other jurisdictions following this approach include Mexico, South Korea and South Africa.

(2) Bulk licences/General Licences

This category of jurisdictions includes the ones which typically incorporate a system of bulk licences. This option of bulk licence is available for export of eligible items, software, or technology; and for the rest, the usual individual licence regime applies. There are certain variations in the way these bulk licences would operate.

For example, In the UK, export of items that contain general purpose cryptography are eligible for an Open General Export Licence (**OGEL**), under special circumstances. OGELs are bulk licences with set terms and conditions, which permit, without further authority involvement, export from the UK and remove the need to apply for an individual export control licence. Each OGEL covers a different activity that is controlled, for example, cryptographic development OGEL specifies the items allowed to be exported under that OGEL, the end-users and the destinations where items can be exported to.

Specifically for export of cryptographic information security items/technology, there are two types of OGELs available in the UK:

a. Open General Export Licence - Information Security Items;[3] and
b. Open General Export Licence - Cryptographic Development, this is specifically for intra-company transfers or established supply chain transfers for cryptographic product development activities.[4]

Under both these OGELs, exporters are subject to strict export record keeping obligations, technical data submission obligations, compliance audits by the government, and certain other conditions, as the case may be. The record keeping may be also done in a more general way, if agreed with the responsible authorities, in the form of semi-annual reporting, such as, [insert name of software] has been exported multiple times between [X-Y date] from location 1 to location 2. Such general reporting is especially beneficial for software transfers because record keeping of every single software export are very difficult.

In Singapore, besides Individual export licences, bulk permits can be obtained for the export of controlled goods, known as, 'Strategic Goods'. The bulk permit eliminates the need for an individual licence and is valid for a period determined by Singapore Customs. Eligible exporters are required to have good compliance records, have achieved a certain milestone under TradeFirst and implement an effective Internal Compliance Programme (**ICP**).[5] This is a general bulk licence, including but not limited to, items performing cryptographic information security only.

Singapore is not a member to the WA. Category 5 Part 2 (Information Security) of the List of Dual Use Items issued under the Strategic Goods Control Act[6] in Singapore is identical to Category 8A5 Part 2 of the Indian SCOMET list. Items that incorporate information security for data confidentiality require a licence by Singapore Customs for exporting such items out of Singapore, subject to the exceptions under notes and technical notes given in Category 5 Part 2 (Information Security) of the list of Dual Use Items.

In addition to UK and Singapore, other jurisdictions that follow a bulk licence approach, whether or not specifically for information security items, software, and technology, include Australia, Japan and most European countries like Germany, Netherlands, France, Belgium etc.

(3) Licence Exception

The third category includes jurisdictions which do not require a licence for export of certain controlled items, software, or technology. The United States of America (**US**) is one such jurisdiction,

[3] Open General Export Licence – Information Security Items, Department for International Trade, Government of UK, available at: https://www.gov.uk/government/publications/open-general-export-licence-information-security-items (Last accessed on 30 September 2021).

[4] Open General Export Licence – Cryptographic Development, Department for International Trade, Government of UK, available at: https://www.gov.uk/government/publications/open-general-export-licence-cryptographic-development (Last accessed on 30 September 2021).

[5] Information on Bulk Permit, Singapore Customs, available at: https://www.customs.gov.sg/businesses/strategic-goods-control/permit-and-registration-requirements/bulk-permit-export-transhipment-and-intangible-transfer-of-technology (Last accessed on 30 September 2021).

[6] Strategic Goods Control Order 2020, available at: https://sso.agc.gov.sg/SL-Supp/S786-2020/Published/20200915?DocDate=20200915#Sc- (Last accessed on 30 September 2021).

which regulates export of cryptographic information security items, software, and technology in a unique way. An exporter of US-origin encryption products from the US is required to classify the export items, either via self-classification or by submitting a request to the US BIS. Confirmation of self-classification of a software/encryption item can be achieved with a formal ruling request from the US BIS. Thereafter, subject to certain conditions, such items may be exported either under a licence exception or, if required, after acquiring a licence from the US BIS. A licence exception allows export or re-export, under stated conditions, items subject to the US export control laws, without requiring an export licence.

Licence exception Encryption Commodities, Software, and Technology (**ENC**) specifically applies to items that implement cryptography. It provides a broad set of authorisations depending on the item, end-user, end-use and destination.[7] Most encryption products can be exported (except to sanctioned countries) under licence exception ENC, i.e., without requiring an export licence, once the exporter has complied with applicable reporting and classification requirements. If an item is designed to use cryptography or contains cryptography, and does not fall under the cryptography note, then subject to certain other conditions, it may be exported without requiring an export licence.

For example, a software/encryption item may be determined to be eligible for export without requiring an export licence through a self-classification process, however, if the software/encryption item falls within any of the following, then an export licence may be required:

1. Item is designed to use cryptography or contains cryptography;
2. Item is not a publicly available source code;
3. Item uses cryptography for data confidentiality, in excess of 56 bit of symmetric key length;
4. Cryptographic capability is usable without activation or has been activated; or
5. Item does not fall under the cryptography note or any other exceptions.

(4) Periodic revision of dual-use list leading to relaxed controls

Member countries to the WA are obligated to revise their national control lists of dual-use items to implement changes to the periodic changes to the WA List of Dual-Use Goods and Technologies, as is decided in the annual plenary meetings. More recently, relaxing export controls over encryption items has been seen. For example, in the 2018 and 2019 WA Plenary Meeting, some of the agreed changes to Category 5 Part 2 of the WA List of Dual-Use Goods and Technologies include:[8]

- the scope of exclusions was expanded by removing limitations on the range and number of connections specified for a 'personal area network'. Consequently, any item using only published or commercial cryptographic standards where the information security functionality is limited to personal area network functionality is excluded from control regardless of the range or number of connections. Personal area network refers to the connection of devices within a user's immediate area, such as, connection between a smartphone and a printer, Bluetooth earphones, tablet etc.

[7] Encryption and Export Administration Regulations, available at: https://bis.doc.gov/index.php/encryption-and-export-administration-regulations-ear (Last accessed on 30 September 2021).

[8] Summary of Changes 2019, List Of Dual-Use Goods & Technologies And Munitions List, Wassenaar Arrangement, available at, https://www.wassenaar.org/app/uploads/2019/12/Summary-of-Changes-to-the-2019-Lists-web-version.pdf (Last accessed on 30 September 2021).

- 'Gateways' in addition to relays, switches or routers, were added to the list of exclusions, where the information security functionality is limited to operations, administration or maintenance tasks implementing only published or commercial cryptographic standards.
- The scope of exclusion was expanded by adding certain connected end-point devices that are designed for a connected civil industry application other than information security, digital communication, general purpose networking or computing. For example, a smoke detection alarm installed inside a house; it securely collects and communicates temperature-related data over a private network.[9]

India notified implementation of these changes to the SCOMET list in June 2020.[10] The EU notified implementation of these changes in October 2020.[11] The US published amendments to the Commerce Control List in March 2021.[12]

While taking the international route to implement changes to encryption items is one way, countries can also take the national route to introduce changes to their national export control laws. Relaxations in controlling export of encryption have been observed in some jurisdictions, over and above what has been agreed to at the WA level. For example, The US notified elimination of certain email notification requirements for publicly available encryption source code and self-classification reporting requirement for certain 'mass market' encryption products in order to reduce exporters' regulatory burdens in the US.[13] Another example is the introduction of OGEL in the UK for export of certain low risk information security items deploying encryption to a wide range of destinations.[14]

Moreover, the EU Regulation (EC) No 428/2009 (**EU Dual-use Regulation**) has been replaced with the new EU Dual-use Regulation from September 9, 2021.[15] The key revisions include: introduction of a new Union General Export Authorisation for encryption items; new rules to authorise restrictions on exports of items that could be used to support human rights abuses, such as, cyber-surveillance items; expansion in information sharing and cooperation between EU Member States regarding controls of certain items impacting public security including with respect to antiterrorism and human rights issues; and requiring exporters using or applying for global export authorizations to implement a formal Internal Compliance Program.

[9] Summary of Changes 2018, List Of Dual-Use Goods & Technologies And Munitions List, Wassenaar Arrangement, available at, https://www.wassenaar.org/app/uploads/2019/consolidated/Summary-of-Changes-to-2018-Lists.pdf (Last accessed on 30 September 2021).

[10] https://content.dgft.gov.in/Website/Noti%2010%20dated%2011.06.2020%20-%20SCOMET%20update_0.pdf (Last accessed on 30 September 2021).

[11] 2020 Update of the EU Control List of Dual-Use Items, European Commission (October 7, 2020), available at: https://trade.ec.europa.eu/doclib/docs/2020/october/tradoc_158973.pdf (Last accessed on 30 September 2021).

[12] Federal Register, Export Administration Regulations (March 29, 2021), available at: https://www.federalregister.gov/documents/2021/03/29/2021-05481/export-administration-regulations-implementation-of-wassenaar-arrangement-2019-plenary-decisions (Last accessed on 30 September 2021).

[13] Federal Register, Export Administration Regulations (March 29, 2021), available at: https://www.federalregister.gov/documents/2021/03/29/2021-05481/export-administration-regulations-implementation-of-wassenaar-arrangement-2019-plenary-decisions (Last accessed on 30 September 2021).

[14] Open General Export Licence – Information Security Items, Department for International Trade, Government of UK, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/989662/Open-General-Export-Licence-Information-Security-Items-from_December_2019.pdf (Last accessed on 30 September 2021).

[15] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0821 (Last accessed on 30 September 2021).

THE WAY FORWARD FOR EXPORT CONTROLS IN INDIA

It is worthwhile to explore if there are approaches from other countries which can be adapted by India, given our early stage in the export control regime as applicable to cryptographic information security.

It is important to re-emphasise that, today encryption technology is widely used for civil (non-military) purposes and incorporated in items/software of civil-use, for example, in the banking industry, educational institutes, hospital industry, automotive industry etc. Most times, software incorporate standard encryption libraries that are widely available and are sometimes open source. Information and Communication Technology today is a software-dominated industry where agile deployment of software with short release-cycles (typically, 2 weeks from the date of receipt of order to the date of deployment) is expected to remain competitive in the market. In such an environment, any additional steps that consume time, drive significant costs. Obtaining a SCOMET authorisation in such timelines is a challenge. This is mainly because individual licences have to be applied for, there is lack of transparency in the authorisation process, the licencing authority undertakes long and cumbersome verification activities etc. Customers are not willing to wait for more than two weeks from the time of ordering the software till the time of deployment, quoting the efficient home country process of bulk licensing/licence exceptions without the need for direct verifications by the government with the customer. Therefore, harmonising the implementation of India's export controls with other jurisdictions, so as to reduce processing times, is paramount for companies operating in India to have a level-playing field with the rest of the world.

The objective of the WA list of dual use goods and technology is not to create unnecessary restrictions on trade of items of civil-use, but to ensure non-proliferation of dual-use items. Accordingly, there is a need to ease compliance obligations when exporting less-sensitive items incorporating encryption technology for civil-use only.

In the above context, we propose the following:

(1) Introduction of bulk licence for cryptographic information security

Suggestion to introduce a licencing regime in the nature of bulk licences, to ease the compliance burden on the industry for export of controlled cryptographic items, software, and technology. Recently, a similar bulk licence regime has been introduced by the Department of Defence Production, Ministry of Defence, for certain technology transfers and export of certain parts and components under Category 6 (Munitions) of the SCOMET list. We suggest that a similar regime be introduced for SCOMET Category 8A5 Part 2 items. Appropriate safeguards in the forms of documentation proofs, post-reporting requirements, audits and implementation of Internal Compliance Programme may be put in place to ensure no misuse of the bulk licence regime.

(2) Helpdesk for classification queries

Irrespective of whether bulk licences will be introduced for cryptographic information security, there is need for clarity on various terms and phrases used in Category 8A5 Part 2 of the SCOMET list. In this regard, we suggest that a SCOMET helpdesk may be set-up within the Directorate General of Foreign Trade (**DGFT**) to address industry's classification queries in a prompt and consistent manner. This is necessary for avoiding mis-classification and even non-classification mistakes that can potentially lead to penalties upon the exporting company.

Such helpdesks are available in many countries. For example, in the US, commodity classification requests can be placed before the US BIS, after providing certain information about the item sought to be classified, such as, technical details, brochures, pictures, descriptive information and even potential Export Control Classification Numbers.[16] In Singapore, the determination of whether an item requires a licence can be done by seeking advice by Singapore Customs on the product.[17] Singapore Customs also releases a list of products with categorisation for reference. This ensures that all ambiguities among exporters regarding interpretation of various terms and phrases of the List of Dual Use Items are effectively addressed by Singapore Customs.

(3) Complete Digitisation of SCOMET licensing procedures

A new SOCMET application portal has been put in place by the DGFT effective from August 5, 2021. This portal has simplified the format for filling in application details and introduced the feature of raising tickets for technical issues with the portal. This is a positive step in terms of streamlining the licence application process for the industry. However, certain improvements in this portal will go a long way in reducing the turn-around time for a licence application and making the portal comprehensive by capturing all compliances:

- Show real-time status of the application: this is needed to show the application status along with information whether the application is pending due to inaction by the applicant. This will help in making the process transparent and enable prompt response to queries, if any. Currently, the application status is reflected in a spreadsheet format that runs into thousands of line items; it does not have transparency on where the application is pending and the reason for such delay; it is available in the public domain which makes an exporter's application details visible to all entities (even those that may not be a party to the export transaction).

- Automate the document submission and concordance process: The portal should have the facility to submit all required documents and proofs, such as the End-User Certificate (**EUC**), purchase order, contracts, technical details etc. These documents should then be centrally available and any verification to be done should be caried out through the portal. Once the licence application is disposed-off (whether licence granted or not), all relevant information and documents should be archived for future reference purposes. This will help in making the process efficient and obviate the need for submitting the same documents again, for example, at the time of revalidation of licence.

- Enabling dialogue between authority and applicant: an option for query-response mechanism between the licencing authority and applicant regarding the application must

[16] US BIS, Classification Request Guidelines, available at: https://www.bis.doc.gov/index.php/licensing/commerce-control-list-classification/classification-request-guidelines (Last accessed on 30 September 2021).

[17] Determination of Strategic Goods, Singapore Customs, available at: https://www.customs.gov.sg/businesses/strategic-goods-control/strategic-goods-control-list-2/determination-of-strategic-goods (Last accessed on 30 September 2021).

be added in the portal. This will enable a dialogue between the authority and applicant about the application and may help in timely resolution of problems or filling gaps in the application, if any.

- Publish a detailed set of Frequently Asked Questions (**FAQ**) to assist the applicant in using this portal.

Such end-to-end digitised and integrated licencing portals are available in many countries. For example, there is Simplified Network Application Process – Redesign (**SNAP-R**) available in the US for the submission of license applications, commodity classification requests and certain other notifications;[18] and the SPIRE portal is available in the UK for the application of export licences for 'strategic' goods.[19] Both these portals are supplemented by detailed FAQs or user-guide for guidance on how to use the portal.

In conclusion, a combination of amendments in India's export control regime is required to revamp the implementation of export controls in India. This will go a long way in easing the compliance burdens on the industry and thus enabling seamless exports. The abovementioned proposals will contribute to the improvement of export control laws in India as well as assist the industry in complying with export control obligations.

[18] Simplified Network Application Process – Redesign, US BIS, available at: https://www.bis.doc.gov/index.php/licensing/simplified-network-application-process-redesign-snap-r (Last accessed on 30 September 2021).

[19] SPIRE, Department for International Trade, Government of UK, available at: https://www.spire.trade.gov.uk/spire/fox/espire/LOGIN/login (Last accessed on 30 September 2021).

NASSCOM®

ADDRESS

Plot 7 to 10,
Sector 126, Noida – 201303
Uttar Pradesh, INDIA

CONTACT

Email: policy@nasscom.in
Website:
www.nasscom.in