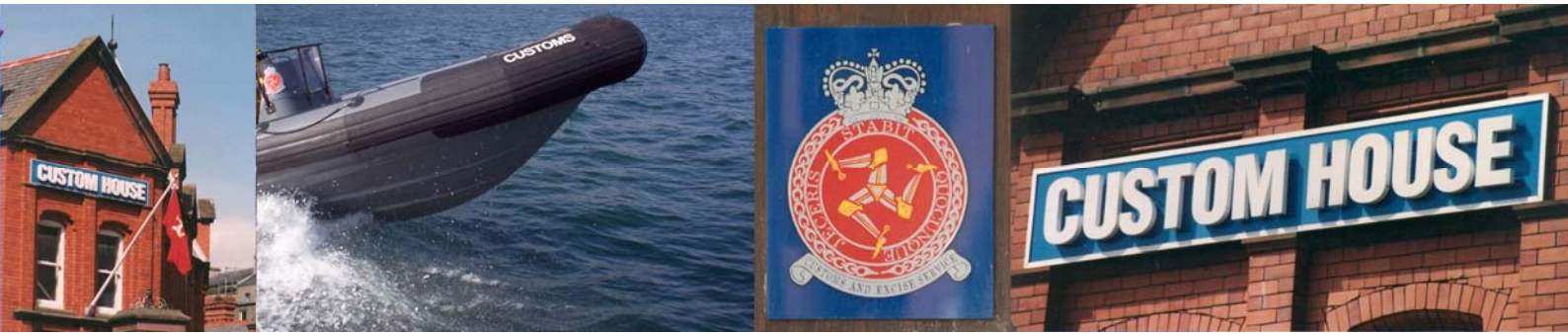
Treasury
Customs and Excise Division

Notice 1008 MAN

Proliferation and Proliferation Financing Risks



August 2016
(updated to 30 November 2017)

Isle of Man Government
Reiltys Ellan Vannin

Contents

Isle of Man Government

Reiltys Ellan Vannin

Introduction

This Notice has been published by the Customs and Excise Division of the Treasury to highlight potential risks to businesses in the Island from -

- proliferation; and
- proliferation financing.

Its aim is to raise awareness of the issues and to provide some assistance to businesses in complying with the requirements of the legislation involved, as well as providing guidance on which agencies may be consulted, or to which any suspicions should be notified.

The Notice is intended as a general guide and has no force in law. Those persons who think they may be affected by the new provisions are advised to seek legal advice.

The information in this Notice was up to date at the month shown on the cover.

The terms "proliferation" and "proliferation financing" are defined below.

After reading this Notice and considering your own business's current procedures and possible exposure to the risks you may wish to consider measures such as -

- improved staff training;
- implementation of new policies and procedures or adaptation of existing ones;
- undertaking risk assessments, or enhanced risk assessments, of clients, customers, suppliers, end-users and third parties involved in particular areas of your business; and
- employing enhanced due diligence procedures to any higher-risk transactions or entities.

Other guidance that might assist you and which is available from Customs and Excise include the following -

- Notice 279 MAN on export licensing controls;
- Notice 279T MAN on trade control licensing (of the trafficking and brokering of certain goods between third countries and involving persons in the Island);
- Notice 1000 MAN on trade-based money laundering and trade-based financial crimes;
- Sanctions Notice 22 on UN and EU sanctions concerned with combatting terrorism financing;
- Sanctions Notice 26 which contains general information about financial sanctions including terrorist financing and proliferation;
- Sanctions Notices 23 and 24 which are concerned with sanctions prohibitions and restrictions affecting North Korea and Iran respectively.

In April 2017, the Royal United Services Institute (RUSI) published what it described as an introductory guide for financial institutions on countering proliferation finance[1]. See paragraph 61C below.

What is "proliferation"?

1. Proliferation is the manufacture, acquisition, possession, development, export, transhipment, brokering, transport, transfer, stockpiling or use of Chemical, Biological, Radiological or Nuclear (CBRN) weapons (weapons of mass destruction or WMD) and their means of delivery and related materials (including technologies and dual-use goods), in contravention of either, or both domestic law and/or international obligations. The term "proliferation" encompasses the acquisition, supply and use of technology, goods, software, services or expertise.

2. The technology, goods, software, services or expertise may have a legitimate use as well as being capable of use in proliferation (and hence the term "dual-use" might be used). Hence it is important to take a holistic approach when conducting any review or risk assessment, and bear in mind that goods, technology etc may have a potential use for both a legitimate purpose or in proliferation. This means that any goods involved may not be included on any international or national control list.

3. Proliferation can therefore take many forms, but ultimately it commonly involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems - which may involve sophisticated technology, such as in long range missiles; or it may involve a relatively simple, or even crude, device (to produce, for example a "dirty bomb"). See Annex B for more information on "dirty bombs" and other improvised devices.

4. Proliferation poses a significant threat to global security. If appropriate safeguards are not established, maintained and enforced for sensitive materials, technology, services and expertise, they can -

    a. become accessible to unauthorised or undesirable individuals and entities seeking to profit from acquiring and selling them on;

    b. be used in weapon of mass destruction (WMD) programmes; or

    c. find their way into the hands of terrorists.

4A. It is important that proliferation and proliferation financing may not be only in one direction. The country or organisation that would appear to be a recipient can also be a supplier. For example, North Korea obtained much of its expertise for use in its nuclear programme covertly from Pakistan (and the so-called "A Q Khan Network"), in return it has exported both missiles and liquid-fuelled missile technology to other countries in the Middle East.

---

1 https://rusi.org/publication/other-publications/countering-proliferation-finance-introductory-guide-financial

What is "proliferation financing"?

5. Proliferation financing can be -

   a. terrorism financing - where it provides financial support to terrorist organisations that would want to acquire and/or use an WMD; or

   b. financing from a state, or a state-controlled or state-sponsored entity with the aim of providing a state with a WMD, or to enhance, improve or replace an existing one.

   Proliferation financing is an important element in both of these and, as with international criminal networks, proliferation support networks use the international financial system to carry out transactions and business deals. Unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology and expertise, providing seemingly legitimate front organisations or acting as representatives or middlemen. It facilitates the movement and development of proliferation-sensitive goods which, in turn can contribute to global instability and may ultimately result in a loss of life. Involvement in proliferation or proliferation financing, even if inadvertent, carries the risk of severe reputational damage to institutions (and to the Island and its business community as a whole). Consequences can include the threat of companies and individuals being included on US and other sanctions lists, or being denied access to banking and other services due to a perceived greater risk. Thus measures to prevent, detect or mitigate potential involvement are important from a business and commercial perspective, as well as to achieve non-proliferation objectives.

6. In 2010, the Financial Action Task Force (FATF) provided the following definition of proliferation financing -

   > "Proliferation financing" refers to: the act of providing funds or financial services that are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.
   >
   > *FATF, Combating Proliferation Financing: A Status Report on Policy Development and Consultation, 2010*

Isle of Man Government Proliferation and Proliferation Financing Risk Policy Protocol

6A. In May 2017, the Isle of Man Government published a Proliferation and Proliferation Financing Risk Policy Protocol (Notice 1009 MAN, available on the Customs and Excise webpages). This contained the following -

IMPORTANT NOTE

The Isle of Man Government does not, and will not, tolerate the use of the Island, its company and business structures, or other facilities for the purposes of proliferation and proliferation financing.

This Protocol applies to ALL public servants, including office-holders. Each has a responsibility to be aware of the risks involved, and of the need to prevent and detect illegal activity, and to report it to the appropriate authorities, namely the Financial Intelligence Unit.

Anyone with any evidence or suspicions about activity connected to proliferation or proliferation financing MUST report it as soon as is practicable.

Similar requirements also apply to persons in business in the Island, and these are set out in Notice 1008 MAN on the Customs and Excise website.

The Protocol supplemented the Isle of Man Government's AML/CFT National Strategy 2016-2018 and its Strategy to Counter Terrorist Financing.

Why can it be difficult to identify activity linked to proliferation, or proliferation financing?

7. You can be faced with a number of problems in attempting to identify proliferation financing -

   a. the purchase and sale of elementary components, as opposed to complete manufactured systems. The individual elementary components may also have legitimate uses (and may even be described as being "dual-use" goods), making their identification for illegitimate purposes even more problematic[2].

   b. dual-use goods are difficult to identify, requiring specialist knowledge and can be described in common terms that denote many innocent uses (e.g. they might be described by an innocuous and generic term such as "pumps").

   c. networks through which proliferation-sensitive goods may be obtained tend to be complex. This, combined with the use of false documentation, allows for such sensitive goods, the entities involved, associated financial transactions and the ultimate end-user to avoid suspicion and detection. Front companies, agents and other false end-users are often used to cover up the true movement of the finance and goods, and the ultimate end-user.

   d. as a state may be involved in seeking the goods, the source of funds may appear (or be) legal, but the true end-user, and the end-use, of the goods involved is obscured, making identification of such activities difficult.

---

2 It was reported in 2016 that the UN Panel of Experts on Iran noted that only 10% of the items it was investigating were mentioned on export control lists.

What are the relevant international obligations in respect of proliferation and proliferation financing?

8. In April 2004, the UN Security Council adopted Resolution 1540 ("UNSCR 1540"), which placed obligations on all UN member states to both have and to enforce appropriate and effective measures against the proliferation of nuclear, chemical and biological weapons, their delivery systems.

9. It also required all member states to adopt and enforce appropriate effective laws and introduce domestic controls which -

   (a) prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use CBRN weapons and their means of delivery, in particular for terrorist purposes, as well as attempts to *engage* in any of the foregoing activities, participate in them as an accomplice, assist or finance them; and

   (b) prevent illicit trafficking.

10. The primary focus of UNSCR 1540 was the implementation of export controls (for more information on the export control licensing regime under Isle of Man law see Notice 279 MAN).

11. It is important to note that export controls include coverage of "dual-use" items, which can have both a legitimate civilian and a military or WMD-related use, and that such dual-use items can be open to misdescription to disguise their true use (e.g. a centrifuge could be one for normal medical use, or for use in a nuclear weapon development programme).

12. In addition, a number of jurisdictions implemented targeted financial sanctions in order to meet the finance-related obligations contained in UNSCR 1540.

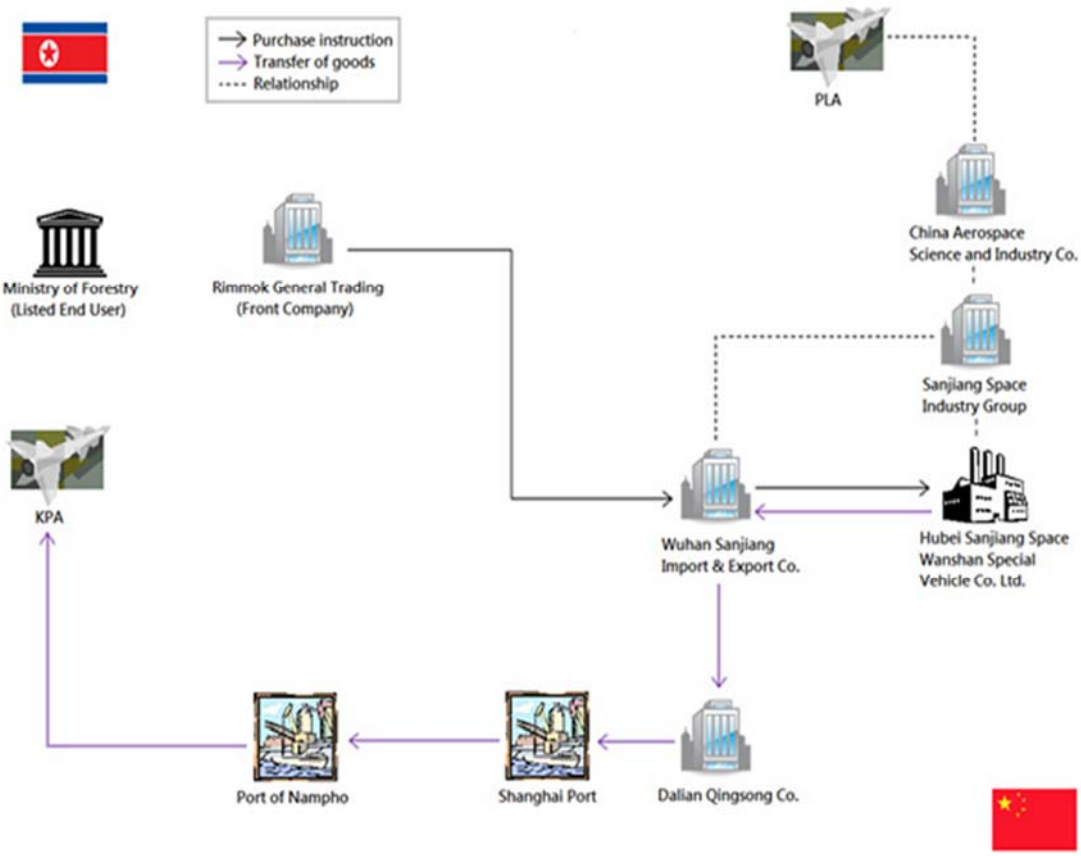
13. Other specific UNSCR were concerned with targeted sanctions against countries known or suspected to be engaged in seeking to obtain or develop WMD and their delivery systems - namely -

   - Iran

   - The Democratic People's Republic of Korea (North Korea)

   Since January 2016, the full array of UN sanctions concerning counter-proliferation only applies in respect of North Korea. However, targeted sanctions affecting Iran, and persons and entities in that country, remain in place.

   How North Korea acquired Chinese Transporter-Erector-Launchers (TEL) ballistic missile launchers



http://www.nti.org/analysis/articles/north-koreas-procurement-network-strikes-again-examining-how-chinese-missile-hardware-ended-pyongyang/

14. The Isle of Man, through the UK, also is bound by commitments under such international treaties and agreements as the Chemical Weapons Convention, the Biological and Toxic Weapons Convention, the Australia Group, the Missile Technology Control Regime and the Wassanaar Arrangement.

15. Furthermore, FATF, which sets the recommendations and issues guidance on combatting money laundering and the financing of terrorism, has since 2012 included combatting proliferation financing in its recommendations and guidance, and has updated its standards to include measures on the implementation of targeted financial sanctions related to proliferation. It had previously issued guidance papers on the risks in 2007, outlining actions that might be taken in respect of UN sanctions affecting Iran and North Korea, with a further paper on Iran in 2008. Also in 2008, FATF issued a more detailed typologies report on proliferation financing, and followed this in 2010 with a status report on its work in CPF (countering proliferation financing).

16. FATF Recommendation 7 requires countries to implement targeted financial sanctions to comply with the UNSCR relating to the prevention, suppression and disruption of proliferation of WMD and their financing.

17. Furthermore, Immediate Outcome 11, which is one of a number of objectives published by FATF and intended to assist in assessing compliance with, and

effectiveness of, a jurisdiction's AML/CFT systems, includes reference to proliferation -

> Targeted financial sanctions are fully and properly implemented without delay; monitored for compliance and there is adequate co-operation and co-ordination between the relevant authorities to prevent sanctions from being evaded, and to develop and implement policies and activities to combat the financing of proliferation of WMD.
>
> *FATF, Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems, 2013, p.117.*

18. Hence, when jurisdictions have their AML/CFT systems assessed by FATF and other international bodies to the FATF standards, proliferation financing is a key issue that will be addressed. This was the case in 2016, during the Moneyval evaluation of the Isle of Man.

19. In 2016, the UK established the Counter Proliferation and Arms Control Centre (CPACC), which brought together expertise from the Foreign and Commonwealth Office, Ministry of Defence and other Government Departments and agencies, including the Export Control Organisation. Based in the Ministry of Defence, it began operations in July 2016.

What proliferation and proliferation financing offences can be found in Manx law?

(a) Proliferation

20. There are offences in Manx law specifically relevant to the development, production, acquisition, retention and transfer of nuclear, biological and chemical weapons. Those offences may also apply in respect of acts performed outside the Island by British nationals normally resident in the Isle of Man and bodies incorporated or established under the law of the Isle of Man.

21. For example, Part VI of the Anti-Terrorism and Crime Act 2003 ("ATCA") is concerned with various offences involving WMD, and section 49E with assisting or inducing certain weapons-related acts outside the Island. Under section 49E, a person who aids, abets, counsels or procures, or incites, a person to do a relevant act outside the Island is guilty of an offence. A relevant act is an act that would constitute an offence under -

- section 1 of the Biological Weapons Act 1974 (offences relating to biological agents and toxins) (of Parliament), as that Act has effect in the Island;
- section 2 of the Chemical Weapons Act 1996 (offences relating to chemical weapons) (of Parliament), as that Act has effect in the Island; or
- section 49B of ATCA itself (use etc of nuclear weapons).

22. Article 6 of the Export Control Order 2008, as applied in the Island, prohibits the export or transfer of goods, software or technology, including dual-use goods, software and technology that may be used in part or in their entirety for WMD

purposes to a place outside the EU unless the subject of the appropriate licence, or after being satisfied that they would not be used for WMD purposes (after "making all reasonable enquiries").

23. The Export of Radioactive Sources (Control) Order 2006, as amended and as applied in the Island, may also be relevant.

24. The penalties for breaches of the legislation can be severe. For example, contravening article 6 of the Export Control Order 2008 could lead to an unlimited fine or up to 10 years imprisonment (under article 34 of that Order).

25. The involvement in activities that contravene any relevant UN or EU sanctions, such as the EU counter-proliferation sanctions measures imposed in respect of Iran and North Korea, would also be serious offences rendering one liable to penalties including imprisonment and/or fines.

(b) Proliferation financing

26. Proliferation financing may be treated as a contravention of -

    a. any relevant UN or EU sanctions;

    b. the anti-money laundering and counter-terrorism financing provisions of the Proceeds of Crime Act 2008 (POCA) and the relevant AML/CFT Codes; or

    c. Part III of ATCA.

What reporting obligations apply: who should I tell?

27. The acquisition, possession, use, transfer, concealment or retention of assets that are the proceeds of unlawful conduct, or are intended for use in unlawful conduct (including the offences mentioned above) may constitute a money laundering offence under POCA.

28. Similarly, Part III of ATCA 2003 contains potential offences that are similar and which relate to terrorism and terrorist finances.

29. Failing to report knowledge or suspicion of money laundering is an offence under POCA.

30. The raising of funding for the purposes of terrorism is an offence under ATCA.

31. A defence is available to banks and other businesses if a suspicious activity report (SAR) is filed with the Financial Intelligence Unit (FIU) within a reasonable time. A SAR should be made if there is the knowledge or suspicion of money laundering or the financing of terrorism, including proliferation financing.

32. Anyone should also make a report to the FIU where they know or have reasonable grounds to suspect someone has committed an offence under ATCA.

33. In addition, the provision of funds, economic resources or specified goods to a person, subject to UN or EU sanctions legislation imposed due to concerns about

proliferation, may be an offence under the relevant sanctions legislation. Reports on potential or suspected breaches of sanctions should be made to the Sanctions Officer at the Customs and Excise Division of the Treasury, as well as to the FIU.

Whilst Customs and Excise co-operates closely with the FIU in sanctions controls, anyone who has knowledge or suspicion of proliferation financing should also submit a SAR to the FIU without delay.

How can proliferation and its financing be targeted?

34. There are two recognised mechanisms by which proliferation can be targeted -

    a. export controls; and

    b. financial measures.

35. For details of export controls and export licensing requirements please refer to the Public Notices listed in the Introduction to this Notice.

36. Note that export control law applies to an "Island person", and this is defined in the Export Control Order 2008 (as it has effect in the Island) as meaning -

    a. A British citizen, a British overseas territories citizen, a British National (Overseas) or British Overseas citizen who is resident in the Island;

    b. A person who under the British Nationality Act 1981 (of Parliament) is a British subject who is resident in the Island;

    c. A British protected person within the meaning of the British Nationality Act 1981 (of Parliament) who is resident in the Island;

    d. A body incorporated under the law of the Island; or

    e. A limited liability company registered in the Island,

    and that export, trade control and sanctions legislation may have extra-territorial effect (i.e. may effect actions of such persons even if taking place outside the Island). It should also be noted that UK law may also apply to the above persons under the provisions of the Export Control Order 2008 and its sanctions and other legislation.

Why are financial measures important?

37. Financial measures supplement effective export controls, and seek to counter the financial activity associated with proliferation. Like international criminal networks, proliferation networks use the international financial system to carry out transactions and business deals. Institutions should therefore be alert to the possibility that their customers may be engaging in, or facilitating, proliferation activities and for proliferation financing.

38. In a Working Group Report of 2010, FATF suggested there are three areas where institutions might have responsibilities in relation to proliferation financing -

a. Risk assessing customers and products;

b. Applying enhanced due diligence to high-risk transactions and entities; and

c. Paying special attention to trade finance and insurance products.

Risk assessments

39. Introducing proliferation financing into current risk assessment practice should be proportionate to the overall proliferation risk of the activities undertaken by the institution. For example, an institution operating internationally or with an international client base will generally assess a wider range of risks, including proliferation risks, compared to a smaller domestically-focused institution.

SIPRI guidance published in September 2016 recommended checks being undertaken on -

a. existing and new customers;

b. the physical aspects of the transaction, including the exporter, collection and delivery addresses and the importer;

c. suppliers, such as subcontractors, airlines and handling companies;

d. business partners and associates; and

e. employees.

It recommended "whole of supply chain compliance".

40. The following risks may be relevant to formulating a proliferation focussed risk assessment -

a. Country or geographical risk

41. The most immediate and obvious indicator will be that there are links to a country that is subject to sanctions imposing restrictions on the movement of military goods, and remembering that sanctions measures requiring specific action against proliferation have been applied in respect of Iran and North Korea.

42. Other indicators may be that a country:

- presents an ongoing and substantial money laundering and terrorist financing risks or have strategic deficiencies in the fight against money laundering and the financing of terrorism (e.g. being identified as such by FATF);

- is an "embargoed destination" listed in Part 1 or 2 of Schedule 4 of the UK's Export Control Order 2008 (extracts of the Order are available in Notice 1002 MAN on the Customs and Excise website). Details of such embargoed destinations may also be obtained from the Foreign and Commonwealth Office at https://www.gov.uk/guidance/sanctions-embargoes-and-restrictions;

- has strong links (such as in providing funding or other support) with terrorist activities. For example, countries designated by the US Secretary of State as state sponsors of terrorism; and those physical areas identified by the US in its annual report entitled "Country Reports on Terrorism" as being ungoverned, under-governed or ill-governed where terrorists are able to organise, plan, raise funds, communicate, recruit, train, transit and operate in relative security because of inadequate governance capability, political will, or both; or

- has higher levels of organised crime linked to arms dealing.

b. Customer risk

43. Specific categories of customer whose activities may indicate a higher risk are -

- those on national lists concerning high-risk entities (e.g. the Iran WMD End-User List published by the UK Department of International Trade and its Export Control organisation https://www.gov.uk/government/publications/iran-list) may involve higher proliferation financing risks;

- where a military or research body is connected with a higher-risk jurisdiction of proliferation concern; or

- where a customer is involved in the supply, purchase or sale of dual-use, proliferation-sensitive or military goods.

c. Risks presented by certain products or services

44. The following may suggest higher risks -

- the delivery of services subject to sanctions (e.g. provision of correspondent banking services affected by UN or EU sanctions measures);

- project financing of sensitive industries in higher risk jurisdictions;

- trade finance services, transactions and insurance products involving higher risk jurisdictions; or

- the delivery of high volumes of dual-use, proliferation-sensitive or military goods, particularly if to a higher risk country.

45. As well as risk factors, mitigating factors should also be considered. For example, whether a customer or client is aware of proliferation risks and has systems and processes to ensure their compliance with export, trade control and sanctions obligations and can provide copies of export control or other licences required.

Enhanced due diligence checks on higher-risk transactions and entities, or customers or clients with exposure to them

46. You should apply, on a risk-sensitive basis, enhanced customer due diligence measures in any situation which by its nature can present a higher risk of money laundering, the financing of terrorism or proliferation financing.

47. It is a matter for you to determine the enhanced due diligence measures to be applied.

48. Lists compiled by national authorities can be a useful resource, as they provide information on individuals who may pose a proliferation concern. The persons, individuals, companies and entities may be referred to as "restricted parties".

49. In individual cases, where proliferation financing is a risk or concern, institutions may also wish to consider whether banks, applicants or beneficiaries of letters of credit, or freight companies and shipping lines moving the goods, appear on such lists.

50. Where a regulated entity provides services to a trading company or any business vehicle that itself has links to higher risk countries, from a proliferation perspective, development of a strategy will assist in responding to any proliferation risks. Such a strategy may call for systems to be put in place to monitor trading activities.

What about checks on the goods involved?

51. Identifying whether a particular item is a dual-use item or otherwise poses a proliferation concern, is acknowledged to be difficult. Therefore, in higher risk scenarios where the customer is importing, exporting or otherwise trading goods, you should be alert to the need to mitigate against inadvertent proliferation financing. Where you believe goods may be subject to export licensing, this can be achieved by asking the customer for the following:

- valid export licences; or
- "licence not required" letters that are less than three months old.

51AA. Radioactive and radiological materials can be obtained from a wide range of sources and/or have a wholly legitimate use - in science, medicine or industry. Even the production of phosphate fertiliser can, as a by-product, produce useable uranium. In fact, in the 1990s some 20% of US uranium production was said to have been from phosphate fertiliser by-products, and during the 1980s Iraq secretly produced 109 tonnes of uranium at a fertiliser plant. Phosphate rock ore can be mined in many countries, the world's largest reserves being in Morocco, but with sizeable reserves in a number of North African and Middle East states - and according to research published in 2017[2] uranium produced as a phosphate fertiliser by-product was a major factor in weapon programmes in the past, as well as having been pursued as a nuclear energy fuel source in a number of countries.

51A. Goods that are considered to be controlled or sensitive because of a potential end-use application are listed by various international bodies -

The Nuclear Suppliers Group (which provides good practice guides[3])

2 https://www.sipri.org/publications/2017/eu-non-proliferation-papers/phosphate-fertilizers-proliferation-relevant-source-uranium

3 Good Practices for Corporate Standards to Support the Efforts of the International Community in the Non-Proliferation of Weapons of Mass Destruction http://www.nuclearsuppliersgroup.org/en/national-practices

The Missile Technology Control Regime (MTCR)

The Wassenaar Arrangement

The Australia Group

The Zangger Committee

The EU dual-use control regime (see paragraph 52 below) incorporates these export control regimes.

52. The EU lists items for which it requires export licensing controls because of their dual -use nature in Council Regulation (EU) No 429/2009. It also provides more information on the dual-use export control at -

http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/index_en.htm

53. The Export Control Organisation in the UK also has an online tool called goodschecker that might assist in identifying if the goods involved may be subject to export licensing under UK or EU law - https://www.ecochecker.bis.gov.uk/spirefox5live/fox/spire/OGEL_GOODS_CHECKER_LANDING_PAGE/new

54. If a customer is unable to provide the information about the goods, then an alternative is to ask that the customer provide evidence, by reference to export control and import control requirements in the relevant jurisdiction, that the goods do not require a licence in either the country of departure or arrival (or end-use).

What about trade finance and insurance products?

55. A significant proportion of proliferation financing activities are said to utilise trade finance as a vehicle. Special attention should therefore be given to certain trade finance and insurance activities.

56. These are -

- direct loans or general credit facility to facilitate export transactions;
- the purchase of promissory notes or bills of exchange issued by foreign buyers to exporters for the purchase of goods and services, freeing up cash for the exporter;
- factoring - the purchase or discounting of a foreign account receivable for cash at a discount from the face value;
- the provision of guarantees to or by financial institutions on behalf of exporters such as pre-shipment guarantees and performance guarantees; or
- the provision of insurance against certain risks in the trading process.

57. In its thematic review in 2013 into how UK financial institutions dealt with financial crime risks in trade finance, the Financial Conduct Authority implied that it was good

practice for banks etc to consider checks on or for dual-use goods involved in transactions.

Are there any particular "red flags" to be aware of?

58. The customer -

- is involved in the supply, sale, delivery or purchase of dual-use, proliferation-sensitive or military goods, particularly to higher risk jurisdictions;
- has a name, title or address which is the same or similar to one of the parties found on publicly available lists (which may be compiled by the UN, EU or international bodies or national authorities) - this also applies to any counter-party which may be involved in the transaction(s);
- is a military or research body connected with a higher risk jurisdiction of proliferation concern;
- has activity that does not match the business profile;
- is vague, particularly about end-user and the end-use of the goods, provides incomplete information or is resistant to providing additional information when sought[4];
- is a new customer and requests a letter of credit from a bank, whilst still awaiting approval of its account; or
- uses complicated structures to conceal their involvement - such as the use of layered letters of credit, front companies, intermediaries and brokers[5].

The FATF report on proliferation typologies in 2008 suggested the use of behaviour-based red flags that could indicate proliferation activity, such as the shipment of goods to a country with a technical level consistent with the sophistication of the goods, or shipping to or through countries with weak export control laws or poor enforcement. Such an approach may be better suited to complex proliferation networks that may involve legitimate operators and dual-use goods.

In September 2016 the Stockholm Institute for Peace Research Institute (SIPRI) published a series of good practice guides for the transport sector, including one guide dealing with "Proliferation Red Flags and the Transport Sector"[6].

59. The transactions/orders -

---

4 Proliferators may make use of a network of middlemen and agents located overseas to procure necessary materials. This means that it is not immediately obvious that these agents have any connection to the true end-user. They may also make use of one or more transhipments through other countries to disguise the eventual destination.

5 UN SCR 2270 of 2 March 2016 commented on the use by North Korea of "complex, opaque ownership structures for the purpose of violating measures imposed in relevant [UN] Security Council Resolutions

6 https://www.sipri.org/publications/2016/red-flags-good-practice-guide

- concern dual-use, proliferation-sensitive or military goods, whether licensable or not;
- involve an individual or entity in a foreign country of proliferation concern;
- demonstrate a link between representatives of companies exchanging goods (e.g. the same owners or management), in order to evade scrutiny of the goods exchanged;
- appear to involve disproportionate freight or associated costs;
- the use of a residential, hotel or other unusual delivery address, or the use of a transport company as the consignee or recipient;
- involve a circuitous routing of goods or financing;
- involve the shipment of goods inconsistent with normal geographic trade patterns (i.e. where the country involved does not normally export or import the types of goods concerned); or
- involve orders placed by firms or individuals from foreign countries, other than the country of the stated end-user.

60. The jurisdictions (countries or territories) involved -

- are countries with weak financial safeguards and which are actively engaged with a country subject to sanctions or other embargo;
- have the presence of an industry that produces dual-use goods, proliferation-sensitive items or military goods;
- are known or thought to have weak import/export control laws or poor enforcement (or are otherwise considered a higher risk for corruption);
- do not have the required level of technical competence, or the need for, the goods involved;
- appear to be deliberately inserted as extra links into the supply chain (e.g. diverting shipments through a third country).

61. Others include -

- where the final destination or end-use or end-user are unclear;
- in any project financing or complex loans, there is a presence of other objective factors such as an identified end-user;
- there appears to be a declared value of shipment under-valued in relation to usual shipping costs;
- there are inconsistencies in information contained in trade documents and

financial flows (e.g. names, addresses, final destination);

- there appears to be the use of fraudulent documents and identities (e.g. false end-use certificates and forged export or re-export certificates);
- the use of facilitators to ensure the transfer of goods avoids inspection;
- where there is innocuous commercial wording on customs declaration/export licence (e.g. "pump"), without further explanation of purpose or use;
- where a freight forwarding firm is being listed as the product's final destination;
- where the wire transfer instructions, or payment from or due to entities, is not identified on the original letter of credit or other documentation;
- one of the parties involved has a history of non-compliance with customs, export or similar requirements;
- possible front or "shell" companies are involved between the supplier of goods and services and the eventual end-user or recipient; or
- the use of cash payments, indirect or unusual payment methods, or a pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.

61A. The Annex to this Notice contains summaries of typologies reported to the UN Sanctions Panel on Iran as examples of attempts to circumvent controls on the financing of proliferation and financial sanctions imposed on Iran.

61B. The Interim Report of the Study of Typologies of Financing of WMD Proliferation[7] by Kings College London in February 2017 identified 4 means of identifying the financing of proliferation which could be used by banks and others -

1. Using sanctions lists to screen current or potential customers, clients and transactions - but warns that the involvement of those not included in lists means commonly available commercial screening systems may not prove of use.

2. Using the information available on documents connected to a transaction to screen the goods and materials involved - using lists of sensitive or controlled goods and material published for the purposes of export control or by organisations such as the Nuclear Suppliers Group and the Missile Technology Control Regime (MTCR).

3. Where the institution has intelligence or other information that indicates that the financing of proliferation is involved; and

7 http://projectalpha.eu/wp-content/uploads/sites/21/2017/02/Project-Alpha-Study-of-Typologies-of-Financing-of-Proliferation.pdf

4. Identifying patterns or characteristics in the transaction(s) that matches those included in typologies or example cases, in the same way that an institution might do so in order to reveal potential money laundering or fraud.

The Interim report also identified similarities and differences between proliferation financing, terrorist financing and money laundering. The comparisons generally showed similarities between the three seemingly different types of activity (albeit that in terrorist financing and proliferation financing the amounts of money involved may be lower than in criminal money laundering).

However, a significant difference was that for proliferation financing for state actors, and for terrorist financing (which might involve seeking to obtain WMD and delivery systems), the money trail was described as "linear". In other words, unlike criminal money laundering, where the intention was the benefit (or at least the bulk of it) to eventually end up with the criminals who generated it, in the other activities the money was (or may be) used for another purpose - such as to obtain goods and materials required.

The Final Report Typologies of Proliferation Finance[8] was published by the Project Alpha Team on 13 October 2017 and includes 60 case studies based on analysis of a variety of official data.

61C. In April 2017, the Royal United Services Institute (RUSI) published what it described as an introductory guide for financial institutions on countering proliferation finance[9]. This guidance paper was aimed at financial institutions that had carried out little or no concerted thinking on proliferation finance as distinct from other forms of financial crime. The stated purpose was to raise awareness of the risk, and to create a baseline policy for mitigating the threat to the institution. The guidance paper placed emphasis on risk assessment, on reviewing the institution's KYC processes and not just rely on screening using sanctions lists or other sources.

61D. In September 2016 the Stockholm Institute for Peace Research Institute (SIPRI) published a series of papers providing good practice advice for the transport sector - including for freight forwarders, as well as red flags for the transport sector and providing details of information sources[10].

Contact details

62. **Isle of Man Customs and Excise**
Export Licensing and Sanctions enquiries:
PO Box 6, Custom House, North Quay, Douglas, Isle of Man, IM99 1AG
Tel: (01624) 648136
Fax: (01624) 661725
Email: customs@gov.im
Website: http://www.gov.im/categories/tax,-vat-and-your-money/customs-and-excise/

8 http://projectalpha.eu/final-report-typologies-of-proliferation-finance/
9 https://rusi.org/publication/other-publications/countering-proliferation-finance-introductory-guide-financial
10 https://www.sipri.org/research/conflict-and-peace/transport-and-security/transport-service-providers

63 **Export Control Organisation, Department for International Trade**
Export Control Organisation, Department for International Trade, 1 Victoria Street, London, SW1H 0ET
Tel: (020) 7215 4594
Fax: (020) 7215 2635
Email: eco.help@bis.gsi.gov.uk
Website: https://www.gov.uk/government/organisations/export-control-organisation

64. **Financial Intelligence Unit**
PO Box 51, Douglas, Isle of Man, IM99 2TD
Telephone: 01624 686000
Email: fiu@gov.im

Amendments to this Notice

14 November 2016	New paragraph 61A inserted and Annex containing sample typologies added.
26 January 2017	Paragraph 1 amended to insert reference to WMD; and paragraph 2 amended to insert mention of use of the term "dual-use".
6 February 2017	New paragraph 61B inserted re the interim report of the Kings College London study into proliferation typologies.
2 March 2017	Diagram of supply of Chinese missile launchers to North Korea added to paragraph 13 and new Annex B added re dirty bombs (RDD) and improvised nuclear devices (IND).
25 April 2017	New Annex C containing certain terms in Korean and Russian script added.
9 May 2017	New paragraphs 6A (Isle of Man Government Proliferation and Proliferation Financing Risk Policy Protocol) and 64 (FIU contact details) inserted.
11 May 2017	Introduction and paragraphs 2, 5 and 58 amended, and a new case study included in Annex A. New paragraphs 4A, 51A and 61C inserted.
15 May 2017	The case study involving Chinpo Shipping in Annex A updated in the light of the appeal before the Singapore High Court.
23 May 2017	Reference to SIPRI good practice guides concerned with proliferation and the transport sector in paragraph 58 and new paragraph 61D. Paragraph 48 amended to add reference to restricted parties. Paragraph 39 amended to mention SIPRI recommendations. Paragraphs 58 and 59 amended.
5 June 2017	New paragraph 51AA inserted re the potential production and use of uranium obtained as a phosphate fertiliser by-product.

13 June 2017	Footnote added to paragraph 7(a) and paragraph 58 amended to mention use of behaviour-based red flags.
30 November 2017	Paragraph 61B amended to include mention of the Final Report Typologies of Proliferation Finance which was published by the Project Alpha Team.

Data Protection Act 2002

Customs and Excise collects information in order to administer the taxes for which it is responsible (such as VAT, excise duties, air passenger duty), carrying out its other functions, and for detecting and preventing crime.

Where the law permits, it may also get information about you from third parties, or give information to them, for example in order to check its accuracy, prevent or detect crime or protect public funds in other ways. These third parties may include the police, other government departments and agencies.

Annex A

Example Typologies of the Financing of Proliferation

The following were provided to the UN Sanctions Panel on Iran by governments and the private sector and were published on the UN website:

- A national authority described an example of a transaction involving intermediaries in multiple countries. A purchase order was placed by a designated entity, Atomic Energy Organisation of Iran and forwarded through a front company in Iran. Payment was initiated by a second front company in Iran through another designated entity, Bank Sepah which transferred funds through an Iranian company in the food business to a non-UN sanctioned Iranian bank. From there, the transfer was made via a bank in another country A to a bank in a third country B. The purchase order itself was also routed via intermediary companies in countries A and B to disguise its origin. Eventually, both the order and payment were received by the manufacturer in country C.

- A foreign national set up a trading company in another Middle East State and opened a series of accounts on behalf of the company at an international bank in that country. These accounts were denominated in local currency and in euros, UK dollars, and other foreign currencies. Monitoring by the bank showed that the trading company's account received funds in local currency from only one source (a second company set up by another foreigner). These local currency funds were then quickly switched into foreign currencies and transferred overseas. This activity triggered investigations by the bank, which indicated that the owners of the companies involved had links to Iran. The bank suspected the funds were coming from Iran and being channelled through the trading company into the global financial system.

- A foreign national set up a trading company in another Middle East State and opened an account on behalf of the company at an international bank in that country. Monitoring by the bank showed a high turnover of funds, and money-laundering was suspected. Investigations by the bank showed that the foreign national's stated employment was as a member of staff in the second company, which had the same telephone number as the trading company. Further investigation revealed that this telephone number was the same as that belonging to two other companies previously identified by the bank as having Iranian shareholders and involved in Iranian business. The bank therefore suspected the trading company was being used as a front for Iranian business.

- A national of a Middle East country set up a company in that country in partnership with a foreign national as a minority shareholder, and opened an account on behalf of the company at an international bank there. Multiple large payments were made from this account to several companies at the same address in a European country, and also to a second set of companies sharing an address in a second European country. The bank's monitoring identified this pattern as possible money-laundering, and further investigation revealed that the Middle East national was also a manager of another company that did business with Iran.

- A payment of freight charges named two logistics companies but which made no reference to Iran. At the request of the financial institution, an invoice was provided. This was found to contain a bill of lading reference number. Upon tracking this bill of

lading, the final destination of the shipment was found to be Iran.

- A payment was identified to a company in a country neighbouring Iran: the policy of the financial institution was to conduct enhanced due diligence where companies in this particular country were concerned and, as a result, this company (the beneficiary of the payment) was found to be located in Iran. The address in the neighbouring country was false.

- An import Letter of Credit (LC) covering a shipment of goods: the goods originated in country A in South Asia, ostensibly to be shipped from a country B neighbouring Iran (B) to country C in North Africa. The financial institution investigated the LC which showed that the shipment was conducted by a third party company, which was Iranian. The beneficiary of the LC in the neighbouring country B was acting as front company to the Iranian one, which was the actual beneficial owner from the LC.

- Payment was identified covering goods shipped from a country A in North Africa to country B which bordered Iran: a review by the international financial institution of related shipping documents revealed that the goods were in fact in transit to Iran.

- Company A in Iran entered into an agreement with company B located in another Middle East country under which company B agreed to accept or process payments on behalf of company A. Company B had a bank account at a non-Iranian financial institution. Company A informed its customers to direct their payments to company B and informed beneficiaries to expect payments from company B's bank. It is not known how the financial transaction between company B and company A in Iran was conducted.

- An Iranian with an established business in Iran selling goods domestically and abroad, moved out of Iran and continued to own and receive income from his business in Iran. The income was received in the form of wire transactions from small financial institutions located in neighbouring countries. The accounts in these financial institutions from which the wires originated were affiliated with companies located outside Iran (hawala methods may have been used to transfer value between the business in Iran and these companies).

- A non-Iranian company A located outside Iran attempted to send a payment to a company B inside Iran. Company A sent the payment to a specific account purportedly belonging to company B at a bank inside Iran. The payment was rejected by an international financial institution and a report filed with the authorities. Company A then arranged a second payment for a similar amount, to a beneficiary company C located outside Iran. The beneficiary account number was the same account number as the original company B. It is not known if/how this second attempted payment would have reached company B and no connection between the Iranian company B and the beneficiary company C located outside Iran was revealed by open source searches.

- In its guidance paper "Countering Proliferation Finance: An Introductory Guide for Financial Institutions[1]", RUSI provided a summary of the case involving the detention in Panama of a North Korean vessel operated by Ocean Maritime Management Ltd.

1 https://rusi.org/publication/other-publications/countering-proliferation-finance-introductory-guide-financial

Some of the costs connected with the voyage were paid by Singapore-based Chinpo Shipping Company (Private) Limited. That company was subsequently charged with, and convicted of, financing proliferation in connection with a wire transfer of $72,016 paid from a Bank of China account to a Panama Canal shipping agent. Evidence was produced which showed, amongst other things, that the same business address, employees and email account was shared with North Korean entities, and that the North Korean embassy used the business as a postal address. Accounts at other banks in Singapore had been closed previously due to suspicious transactions some years before. The Singaporean company had had dealings with North Korean shipping concerns since the 1980s (North Korea has had a great many business connections in or with South-East Asia, particularly Malaysia and in Singapore), and had made payments on behalf of the North Korean concerns for various charges, and between different North Korean shipowners. These activities were kept separate from the company's own chandelling and ship agency work, with 605 remittances made over a 3-year period, involving over $40 million (despite it having no money remittance licence - for which it was also charged and convicted). No mention of the North Korean vessel names (or other identifying details) were used in remittance forms or email correspondence. Once a year a North Korean diplomat was allowed to withdraw up to $500,000 in cash to take out of Singapore.

Bank of China (which subsequently closed the Singapore company account in 2013) was said to have queried only one remittance - asking for details of the cargo, the consignee in Cuba and the bill of lading. These details were provided.

The RUSI summary makes the point that additional checks, including due diligence and KYC ones would have thrown up "red flags" earlier. The Bank should have regarded the company as high risk, because it dealt with North Korean vessels, and the change to non-declaration of the vessels involved in transactions, as well as the regular withdrawal of large sums of bulk cash, should have alerted the Bank.

On 12 May 2017, an appeal to the Singapore High Court against the proliferation conviction was allowed, and the money transmission conviction upheld. The proliferation conviction was quashed because the prosecution had failed to prove beyond all reasonable doubt that the surface-to-air missiles involved (said to be for use in defending ballistic missile and nuclear sites) could be said to reasonably contribute to the nuclear weapons programme. The missiles involved were "conventional" weapons, but the authorities had chosen not to use the part of the statute concerned with conventional weaponry.

Despite the partly successful appeal, it should be noted that involvement in the shipment of the missiles involved, had it involved an Island person, could have given rise to charges under the Export Control Order 2008, as it has effect in the Island (see Notice 279T MAN).

Annex B

"Dirty bombs" and improvised nuclear devices (IND)

The International Atomic Energy Agency (IAEA) ranks radioactive sources in 5 categories.

- Category 1 - the most dangerous because they can pose a very high risk to human health; an exposure of only a few minutes to an unshielded Category 1 source may be fatal.

- Category 5 - the least dangerous; but these sources could give rise to doses in excess of the dose limits if not properly controlled.

Note that the system is based on safety concerns, not "area denial" consequences that would be more relevant for use in a military context.

"Dirty bombs" combine a conventional explosive with radioactive material that is dispersed when the device explodes, so as to cause maximum contamination, damage and panic[1].

The effects of a dirty bomb (a.k.a. radiological dispersal device or RDD) can vary depending on what type of radioactive material is used and how effectively it is dispersed. In addition to damage and injury caused in the explosion, there would be a public health concern from the risk among exposed individuals of developing cancer.

The consequences of an RDD may be localised or affect a larger area, but economic losses may still be considerable, depending on the chemistry and form of the radioactive material, the means of dispersion, and the target area[2].

An "improvised nuclear device" (or IND) differs from a RDD. An IND uses highly-enriched uranium or plutonium to actually generate a nuclear explosion, and its use would cause hundreds of thousands of casualties over a much larger area. It also would produce potentially lethal radioactive fallout, capable of contaminating a very large area, depending on location, wind and other weather conditions.

An IND would therefore likely result in large loss of life, destruction of infrastructure, and contamination of a very large area. The economic losses are almost incalculable.

An RDD is technically much easier to construct than an IND, and the materials required are more readily available. Therefore, in evaluating the comparative risks represented by the use of an IND or RDD, the National Threat Initiative Radiological Security Progress Report of 2016[3] said that most experts have concluded that the risk of an RDD attack is much higher than that of an IND attack.

Source: National Threat Initiative Radiological Security Progress Report of 2016, published by the NIT in March 2016.

---

1 See the US Nuclear Regulatory Commission factsheet https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fs-dirty-bombs.pdf

2 The cost of cleaning an affected area could be huge. The cost of safely disposing of a single pallet or container of contaminated goods detected by UK port screening systems, for example, can run into tens of thousands of pounds.

3 http://nti.org/6512P

Annex C

Certain terms in Korean and Russian script[1]

Item	*Korean*	*Russian*
Vacuum pumps	真空泵	Вакуумный насос; or Вакуумные насосы (plural)
Spark gap plugs	火花间隙插头	Искровой промежуток пробки
Spark gap	火花间隙	Искровой промежуток
Plug	插头	Пробки
Maraging steel[2]	马氏体时效钢	
Carbon fibre –	碳纤维	
Single strand		Углеродное волокно
Composite		углепластики; or карбон
Autoclaves[3]	高压灭菌器	Автоклавы

1 For more information on the use of search terms etc, see "OP#27: Searching for Illicit Dual Use Items in Online Marketplaces: A Semi-Automated Approach" (James Martin Center for Nonproliferation Studies (CNS) Middlebury Institute of International Studies) http://www.nonproliferation.org/op27-searching-for-illicit-dual-use-items-in-online-marketplaces-a-semi-automated-approach/

2 Carbon-free iron-nickel alloys with additions of cobalt, molybdenum, titanium and aluminium. The term maraging is derived from the strengthening mechanism. A special class of low-carbon ultra-high-strength steels.

3 A strong, heated container used for chemical reactions and other processes using high pressures and temperatures.

Published by:
Isle of Man Customs & Excise Division
PO Box 6
Custom House
North Quay
Douglas
Isle of Man
IM99 1AG

Telephone: (01624) 648100

Email: customs@gov.im
Website: www.gov.im/customs

This document can be provided in large print or audio tape on request

Isle of Man
Government
Reiltys Ellan Vannin