ACAMS

ACAMS International Sanctions Compliance Task Force Submission to FATF

Draft Guidance on Proliferation Financing Risk Assessment and Mitigation

FRIDAY, APRIL 9, 2021

The role of ACAMS and the Global Sanctions Program

ACAMS is the largest international membership organisation dedicated to enhancing the knowledge, skills and expertise of AML/CTF, sanctions and other financial crime prevention professionals through training, best practices and professional development. ACAMS is present in over 175 countries and regularly works with global think-tanks and other like-minded organisations.

Through our **Global Sanctions Program**, ACAMS convenes international experts to enhance thought leadership, producing Masterclasses, Monthly Updates, bespoke training, certifications available in a number of languages and holding issue-specific roundtables. In early 2020 we established the International Sanctions Compliance Task Force with the aim of facilitating dialogue by bringing together sanctions specialists from a wide array of sectors. As a high-level inter-industry forum, one of the key priorities of the Task Force is to enable and support cross-industry dialogue on global sanctions compliance topics.

This submission has been prepared in collaboration with our International Sanctions Compliance Task Force ***Counter Proliferation Financing*** workstream; this workstream aims to enhance global knowledge of proliferation financing and assist effective implementation of regulations and best practices. Through this group, we have facilitated dialogue across a number of ACAMS members to better understand the practical implication aspects related to the draft consultative guidance issued by the FATF. We have additionally drawn upon our wider experience on advancing counter proliferation financing matters, specifically:

- **Proliferation Financing National Risk Assessment Roundtables:** Hosting public-private roundtables to advance individual country level proliferation financing (PF) national risks assessment (NRA). Discussions included identification of PF threats and capacity of the private sector in relation to a major global financial centre. Broader themes included the limitations of tools available to combat PF, challenges in understanding the complexities of goods, and challenges arising from a lack of PF knowledge.
- **Maritime Sanctions Compliance - Enhancing Cross Industry Cooperation and Implementation:** Under another, closely-linked, International Compliance Task Force workstream – ***Maritime, Energy, and Commodities*** – a paper was issued in **October 2020** identifying key priorities for public-private sector engagement. This paper drew on a number of cross-industry and public/private roundtables with wide-ranging attendance, and covered PF relevant aspects such as risk identification, knowledge gaps, and taking a risk-based approach.
- **Global Counter Proliferation Financing Survey:** In February 2020, ACAMS and RUSI published the results of a **joint survey** of sanctions professionals from across the global financial industry on proliferation finance. This report is based on 366 unique survey responses received between November 7, 2019 and January 6, 2020, and surveyed individuals based all over the world, and in different levels of seniority. The survey identified a number of notable elements, including information and knowledge gaps as well as training deficiencies. A summary of the key findings from this survey are set out in Annex 1.

Our purpose in submitting this response is to offer a framework for advancing cross-industry dialogue, including the identification of key priorities for public-private sector engagement. To advance this ACAMS would be willing to host some dedicated roundtables with the Financial Action Task Force (FATF) Secretariat to further explore the themes in this paper.

Key observations and areas requiring future public-private sector dialogue

To help shape FATF's thinking, ACAMS have identified a number of areas where further dialogue and clarification would be welcome. The following section sets out in further detail these observations. However, in brief we would highlight the below key themes that should be considered as a priority area of focus:

Ability for financial institutions, and other private sector actors, to detect illicit activity based on goods alone

It has long been recognised that goods-based screening controls alone will offer limited effectiveness in the detection and prevention of items of proliferation concern. This is particularly relevant given that most international trade happens through open account wire-based transactions and therefore identification is considerably less reliant on itemizations of the underlying good. Additionally, there are specific limits in the extent that FIs, and other private sector actors, are able to verify the underlying goods being transferred. It is further noted the potential PF risks arising from the use of credible falsified documents, this is especially the case in respect to more sophisticated actors. Consequently, our Task Force members highlight the importance of ensuring the accuracy of underlying documentation, including beneficiary and originator information as a more readily available tool in the detection of potential anomalies indicative of proliferation activity.

We propose that further public-private sector dialogue should be undertaken on proportionate risk-based approaches in the enhancement of opportunities to detect the movement of sensitive/dual-use goods. Such a dialogue would provide the opportunity for industry to offer specific examples of the challenges encountered when seeking to ensure the accurate representation of goods being traded and the extent to which partnerships between FIs, governments (e.g. custom authorities) and other private sector companies (e.g. shipping companies) could potentially enable more effective scrutiny of international trade.

Expanded focus on sensitive technologies and controlled goods with manufacturers and suppliers

Our Task Force members highlight the importance of ensuring identification and engagement with those involved in the manufacturing and supply of sensitive technologies and strategic/controlled goods. We believe this should be a first line of defence in counter proliferation financing efforts. We propose the guidance sets out further clarity on how government agencies and the private sector can work together to ensure a clear basis for risk assessing those involved with manufacturing and supply of sensitive technologies and strategic/controlled goods.
It would furthermore be useful for the guidance to state that countries should ensure continuous engagement and awareness of manufacturers/traders/exporters of sensitive technology/goods. This issue appears to be a gap within the current draft guidance, we additionally draw attention to the need to include relevant aspects associated with intangible technology transfer.

Effective public-private information sharing

As a prefix to concerted and appropriately targeted efforts to identify, disrupt, and respond to proliferation financing is the need for effective information sharing mechanisms. As identified by the ACAMS-RUSI 2020 global survey only one-fifth of respondents felt they received sufficient guidance from their government to support understanding and identification of proliferation finance risk. Our Task Force has further elaborated on this finding with the view that in order to establish a proliferation finance connection will often rely on information not readily available to the private sector, including geographical ties. As such, ensuring the successful implementation of Recommendation 1 (R1) will require more concerted government communication on assessing and understanding "proliferation financing risks", including how to apply these measures, training for small-medium enterprises producing specialized parts, and identification of key countries, industries and entities of concern.

Updating of risk indicators

Our Task Force welcomed a number of the risk indicators and noted they provided a good framework to approach risk assessment. However, when considering the reference to Customer Risk Indicators, it was noted that in practice these were not specific enough to conclusively identify proliferation financing risk and some of them were instead more aligned to wider money laundering risk assessment. We would additionally highlight a range of wider indicators that are of relevance, including those recently produced for the maritime sector. We would recommend that a public-private dialogue is advanced across the industries to further expand the concept of updated proliferation financing risk indicators. Furthermore, challenges posed by shell companies/shadow directors may undermine the effectiveness of some indicators, and further addressing of these challenges within the guidance would be welcome.

Ensuring sufficient clarity between mandatory and non-mandatory obligations

We note the non-binding nature of the draft guidance and the aim not to restrict the freedom of national authorities and private sector entities in determining how best to conduct their proliferation financing risk assessments. Our Task Force members did, however, note that the guidance - whilst stressing there is no one-size-fits-all approach – at times appeared unclear on which proposals set out were mandatory, versus what should be implemented on a risk-based decision basis. To ensure proportionate implementation of obligations, we would urge that further clarification is provided between the mandatory and non-mandatory aspects set out within the guidance. This will be particularly important for ensuring efforts are well targeted, that appropriate exemptions can be utilized and that such efforts do not undermine complementary objectives such as financial inclusion.

The need for expanded and targeted training

Discussion among the Task Force noted the continual importance of effective PF training and understanding public/private training needs. As identified in the RUSI-ACAMS 2020 global survey, 80% of those in mid to junior level position agreed they needed further education about proliferation finance risk and typologies in order to implement effective proliferation finance controls. This was 70% for senior management and 64% for executive leadership. Task Force observations on specific training needs included that it would be beneficial to include identified manufacturers/suppliers of sensitive goods. We recommend that further public-private dialogue is advanced on priority areas for expanded training, as well as identification of where that training is most needed.

Detailed issues requiring clarification and/or further dialogue

From discussions and observations, we would also draw attention to the following:

Lack of information in relation to goods

Throughout the guidance there are multiple references to goods and the subsequent detection of dual-use/military items. A clear explanation of financial institutions (FIs) responsibility in such transactions, as opposed to that of the importer/exporter, would greatly assist in clarifying the expectations on FIs. There are inherent challenges for FIs, and other private sector actors, to detect what could be a sensitive or dual-use good, as they will not necessarily have the engineering or military background to determine this (for example the Nuclear Suppliers Group and Wassenaar Arrangement lists are not readily comprehensible to non-experts). FIs could potentially identify possible dual-use goods relevance, but even this would likely require additional data from customers or export authorities. Additionally, whilst overt military goods (such as weapons and ammunition) can often be readily identified, it can be very difficult to identify goods, such as component parts, associated with WMD which have no overt military or WMD related application. We propose the need for further discussion with the FATF on methodologies for how FIs, and other relevant private sector actors, can identify the goods associated with WMD.

Alongside challenges around identification, the limited effectiveness of screening controls in dealing with goods is a longstanding issue. As mentioned above, in order to improve effectiveness, engagement would be required with those manufacturers/suppliers involved in the trade of these goods/components, or identification of high-risk manufacturers/suppliers would enable PF to be included in an FIs risk assessment of such clients and the correct level of due diligence to be applied. As such, those engaged in the manufacture of dual-use goods/strategically controlled goods could be included in the list of stakeholder firms in para. 26 of the guidance. Robust supply chain compliance controls which engage manufacturers/suppliers is needed to tackle PF. Furthermore, it would be beneficial to be able to factor in what countries can produce/have the relevant raw materials or components, and where that information may be available. We propose that the topic of how to screen relevant manufacturers and suppliers, in a manner which avoids generating extensive false-positive alerts and aspects such as disruption to legitimate business, is something that we would wish to undertake follow-up dialogue with the FATF on.

We would further highlight that most open account transactions (wire-transfers) related to PF are unlikely to be captured by FI transaction monitoring systems unless they present some anomalies (e.g. very high amount being paid and not in line with the customer behavior), and they are likely to be identified/reviewed after the transaction has already occurred. Unless a specific and timely lead from law enforcement is forthcoming attempting to identify and disrupt a transaction in flow is generally very difficult and therefore will normally occur post event. In such scenarios, identified suspicions of the transaction/parties involved would be reported to the relevant competent authority. Consequently, the tools/capabilities to identify and prevent potential proliferation activity will ultimately rely on governments having the ability to investigate and take appropriate actions.

Documents which FIs rely on

FIs might receive trade documents and export licenses, but frequently do not have the ability to interpret the information or verify whether these are original or not, as such documents can be extremely technical. In many cases, FIs and other private sector actors will be reliant on the clients confirmation on the end usage, which can be difficult to verify. Additionally, end user certificates do not always go as far as the final user. We propose that this issue should be explored further including through the opportunity of public-private information exchange.

Linked to this are issues around falsification of documents, whereby identification of PF risks is impacted by limitations on obtaining external information from others. For example, this can include the client's counterparty or other legs of the transaction. In many scenarios FIs and other private sector actors will have limited, or no, visibility on the wider aspects of a specific transaction.

Risk indicators

With regards to the risk indicators contained within the draft guidance[1] discussions indicated these were welcomed, particularly that there is the inclusion of a specific focus on maritime risk indicators. Within the Customer Risk Profile Indicators, it was highlighted that the indicator concerning a person lacking a technical background for a complex equipment in which they are dealing is a key useful indicator.[2] We have also noted that the indicator relating to the customer appearing in negative news is of limited usefulness in relation to R1 and Recommendation 7 (R7), as UN sanctioned Iranian/DPRK entities and individuals are unlikely to have news coverage, and PF networks often use shell companies/shadow directors with a limited online presence.

However, our Task Force discussed areas where the indicators could go further and other areas which could be covered – for example, in dealing with shell companies. More generally, it was observed that the provided risk indicators have limited usefulness beyond FIs, for example in the case of the maritime sector, and it can be impractical to expect such a high level of detail with the realities of the maritime industry.

It was also observed that there is little specifically dealing with PF within the risk indicators, and it would be beneficial for this to be built out with more specific information.

Finally, it was suggested that the provided risk indicators could be considered in line with wider risk indicators which have been provided by various competent authorities, such as the advisories by the US government (such as the list of red flags included within the **US Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities**).

Distinguishing mandatory requirements from best practice

As mentioned above, a number of Task Force members also noted a lack of clarity within the guidance between where the FATF is identifying something as mandatory to implement under obligations to Recommendation 1 & 7, as opposed to best practice. Much of the language is that of 'could' or 'should', and further clarity is needed on what is actually required. For example, it is not clear as to where FIs have sanctions compliance programmes and client due diligence programmes, whether this would be considered a reasonable mitigator of PF risk, or where additional factors need to be considered.

Scope of PF

Additionally, discussions included a lack of clarity within the guidance with regards to the scope of PF itself. Given that the guidance itself is limited to R1 and R7, and therefore entities/individuals linked to UN designated DPRK/Iranian individuals and entities, there seems to be a lack of consistency as to whether sections are referring to PF only in the scope of R1, or the wider PF scope. It should be noted than many FIs will take a much broader definition of PF than R7 and use wider risk indicators, which will not necessarily match up with FATF's recommended risk assessment. It would therefore be helpful for FATF to clarify the exact scope of this guidance.

Wider issues

We would also suggest further dialogue on the following key headline points:

- Through our discussions, it was also noted that FIs may not always have a dedicated PF team, and as such clearer expectations for what an organization is expected to do would be helpful.
- Greater clarity could be provided on who is being addressed through the document – there is a section for FIs and a section for countries, but beyond this it can be unclear.
- It would be beneficial for training for FI staff to be rolled into existing sanctions training, so it is more easily comprehensible.
- Fictitious examples would be useful for illustrating what should be looked for.

[1] Pg. 13-16
[2] Pg. 13

- The guidance references countries of concern, and it would be helpful if these could be identified by FATF in relation to PF, or if the guidance could clearly set out the combination of factors which would pose a higher risk.

Conclusion

In conclusion, we thank the FATF for the opportunity to submit this response. We would welcome the opportunity for further dialogue and would be more than happy to facilitate a detailed discussion with our Task Force members on the above points.

Annex

Annex 1 - Key findings from the ACAMS and RUSI Global Survey on Counter Proliferation Financing

The 2020 RUSI-ACAMS global survey is available **here**. Some notable findings of the survey are outlined below:

- Lack of familiarity with PF risk, with the percent of respondents stating they are likely to be familiar with PF risk being 57% at international banks, 34% in regional banks, and 32% in national banks (as well as 35% for non-banking respondents)
- Nearly two-thirds of respondents located in national banks agree that money laundering controls will detect most proliferation financing transactions (64%), which is more than double compared to respondents in international banks (31%).
- 81% respondents think proliferation finance is primarily about the procurement and financing of nuclear, chemical and biological weapons, rather than primarily about the proliferation efforts of specific state actors or non-state groups.
- A majority of respondents work for an organisation with a compliance function that incorporates proliferation finance (60%). Based on received responses, international banks appear most likely to have a compliance function that incorporates proliferation finance (76%), in comparison to national banks (63%) and non-banking institutions (46%).
- Three quarters of respondents believe that training workshops/courses specifically focusing on proliferation finance would be useful. 51% of respondents had not been to any workshop or event where proliferation finance was a topic in the last 12 months. Only 9% had been to 3 or more.
- From a list of proliferation finance risks, respondents indicated they are most concerned about detecting payments related to goods that can be used in a weapons of mass destruction programme (selected by 83% of respondents), and least concerned with implementing targeted financial sanctions on Iran and North Korea (selected by 63%).
- Over three-fifths agree it is challenging to incorporate lists of dual-use goods into transaction monitoring programmes.

Justine Walker, Head of Global Sanctions and Risk, ACAMS

Sam Cousins, Sanctions and Risk Associate, ACAMS

April 9, 2021

www.acams.org/sanctions