ANNEX C

REQUIREMENTS FOR THREAT, VULNERABILITY AND RISK ASSESSMENT (TVRA)

1 Introduction

1.1 The TVRA is a systematic process to identify and analyse risks associated with attacks against the identified critical assets of a building. Although numerous methodologies have been developed, the principles of conducting risk assessments are generally similar in nature. The end objective is to provide a prioritised list of risks to facilitate the Responsible Person's (**RP**) decision on the mitigation measures to be adopted.

2 Key Elements

2.1 In the conduct of TVRA, the following key elements are generally considered:

a. Introduction to the building;
b. TVRA methodology;
c. Identify critical assets;
d. Define threat scenarios;
e. Assess threat probability;
f. Analyse vulnerability;
g. Analyse consequences / Impact of successful attack;
h. Evaluate risk; and
i. Explanation of implications of risk assessment/conclusion.

2.2 Conducting the TVRA is an iterative process where the RP needs to work closely with the Competent Person (**CP**) to agree on the risk assessments. The RP will endorse the final report and submit to MHA for review.

2.3 The report should comprise the above key items in separate chapters and should generally follow the order of the key items above.

3 TVRA Methodology

3.1 There is no preference for any particular methodology as long as it is relevant to the nature of the assessment to be done and the CP is able to clearly demonstrate ability and experience in applying the methodology. As a general guide, the methodology employed should be able to express the risks faced by the assets in terms of, minimally, the threat considerations, the impact of a successful attack, the relative importance of the defined assets, the attractiveness of the target and assets, and any site-specific weaknesses that may be exploited. The methodology should also allow for the clear and concise presentation and prioritisation of risks. A description of the TVRA methodology adopted including the assumptions made should be documented.

3.2 The risk analysis shall **NOT** merely be a building-level analysis. Instead, various types of plausible threat scenarios[1] within the building shall be developed and assessed. For each threat scenario, a robust and soundly supported assessment of the risks faced by the assets using its proposed methodology shall be made. In assessing each threat scenario, consideration should be taken on the typical security features found in the type of building being studied or features that have been incorporated in the building's design[2]. For threat scenarios involving Improvised Explosives Devices (IEDs) and explosive weapons, analysis should be supported with the relevant facts, figures, quantitative and qualitative data as derived from calculations, computer simulations, actual tests, and literature review, etc. in order to assess the risk of each scenario.

4 Identifying Critical Assets

4.1 The first step of a proper TVRA is to identify the critical assets within the building. These critical assets will then become the focus for the rest of the assessment process.

4.2 Critical assets are generally defined as assets which are vital for the building to perform its roles. When identifying assets, the RP needs to consider what are the critical functions / services that the building provides as well as the infrastructure and equipment required to support these functions / services. Critical assets should be defined in consultation with the RP.

4.3 For large buildings with high public footfall, the focus would be in preventing mass casualties in areas of mass congregation.

4.4 For critical asset identification, the following can be addressed:

a. Are there any interdependencies between the assets?
b. What are the existing countermeasures?
c. What are the consequences if asset is damaged?[3]
d. Are there any effective redundancies[4] available; and
e. Where are the critical assets located?[5]

4.5 Given that the identification of critical assets is such a crucial step, the RP may wish to seek comments from MHA before the CP proceed with the rest of the analysis for the TVRA, to avoid abortive work.

[1] This represent threat scenarios at the various locations within the building where the critical assets may be at risk. For example, a VBIED at the vehicle drop-off point, a chemical and biological attack using the ventilation system at a particular air intake point, etc.
[2] For example, the CP should take into account the envisaged operational flow of the building, e.g. whether it is open to public access, whether there will be screening conducted on vehicles or persons entering the building, and whether there will be security clearance for personnel working in the building etc.
[3] This should include expected downtime if the asset is damaged and whether they can be restored.
[4] To assess if redundancies are effective, CP should check to ensure that these redundancies will not be concurrently damaged by a single threat scenario.
[5] The location of the critical assets should be clearly indicated on a layout plan.

5 Defining Threat Scenarios

5.1 The baseline threat list is controlled and disseminated to the RP[6].

5.2 Where applicable, the CP should include cases of previous attacks conducted on similar facilities within the report.

5.3 The CP are also expected to study and include threats which are not within these threat lists but specific to the building being assessed in their study.

5.4 To conduct proper threat scenario identification, the CP should address the following:

a. Have all threats based on the baseline threat list been considered? If not, are justifications provided for omission?
b. Are threats specific to the building[7] considered?
c. Are threats considered for assessment in different threat periods?
d. Are specifics of threats considered in line with MHA's baseline threat lists?
e. Are specifics of threats, such as conveyance method, included in threat consideration[8]?
f. Are there different modus operandi for the same threat on the critical assets / points of the building identified?

6 Threat Probability

6.1 In this phase, the probability / likelihood of terrorists attempting a threat is typically computed as a score. Different methodologies have a different scoring range e.g. 1 to 5 or 1 to 10 etc., normally with 1 being low and 5 or 10 being high. This must be conducted at the asset level where applicable.

7 Vulnerability Analysis

7.1 Vulnerability analysis[9] estimates the likelihood that the terrorist / adversary will be successful in executing a specific attack mode at the building.

7.2 The CP shall consider the following factors:

a. The asset's visibility (ease of obtaining building information in public domain or through reconnaissance);
b. Existing/baseline security measures and Standard Operating Procedures (SOPs) that can (or aid to) detect, delay, deny the threats; and
c. Geographical / site disadvantage e.g. lack of standoff distance due to site constraint etc.

[6] RP should ensure that CP is security cleared before disseminating the threat list.
[7] For example, criminal threats, escape / rescue (detention facilities), water-borne threats, etc.
[8] For example, conveyance method of biological attack (via ventilation ducts, etc), ramming/stationary VBIED, internal/external IED, etc.
[9] If there are varying levels of security for the building, different vulnerability assessments may be needed for the different time periods.

8 Consequence / Impact Analysis

8.1 Consequence analysis[10] estimates the impact of a successful attack on the building. The CP shall minimally consider the following factors:

a. Loss of lives / injuries;
b. Loss or damage to building / critical assets; and,
c. Loss of primary service / output capability (downtime).

8.2 For blast effects, quantitative analysis should be used to determine the consequence / impact. This analysis, which is sometimes called the Blast Effects Analysis, may be contained in a separate annex to be submitted together with the main qualitative TVRA report. The CP can provide qualitative assessments at the TVRA stage (and provide quantitative assessments with detailed calculations thereafter in the Structural Resiliency Study (SRS)) if the conclusion is that additional mitigation is required.

9 Evaluation of Analysis

9.1 This phase of the assessment generally relates the ratings for threat with vulnerability and consequence to achieve a risk rating. The figure is then used for prioritising or ranking the risks to carry out risk management proposals or countermeasures. This is important to the RP as it helps them make decisions on the risks that need to be addressed critically and which risks can be managed with existing measures.

10 Implications of Risk Assessment / Conclusion

10.1 The broad implications of the analysis should be presented as a conclusion. This should include:

a. A clear listing of risks which are deemed to be acceptably low enough for additional mitigation measures not to be taken; and

b. A broad description of the types of mitigation measures[11] which would be undertaken, and/or further analysis which will be conducted to propose suitable mitigation measures.

[10] If there are varying levels of consequences for the building, different consequence assessments may be needed for the different time periods, e.g. whether building is hosting high-signature events for MICE venues.

[11] Examples include "full height steel jacketing for columns directly exposed to potential blasts in the atrium will be explored and its specifications elaborated upon in the SRS", and "laminated tempered glass in the auditorium will be explored and its specifications elaborated upon in the SRS".