Hostile Vehicle Mitigation Installers Scheme

Index

Page

Guiding Principles

The HVMIS aim is to promote a competent and professional approach to installations of temporary and permanent vehicle security barriers (VSB's). Through the HVMIS Government and Industry will work collaboratively to ensure that protection measures are suitable, commensurate and correctly implemented to protect against Vehicle As a Weapon (VAW) attack and Vehicle Borne Improvised Explosive Device (VBIED).

Members of the scheme will be expected to be clear, open and honest with their customers and ensure a suitable level of competence and quality in their works.

A Register will be kept, operated and administered by the Perimeter Security Suppliers Association (PSSA), utilising a database model used to record companies involved in the manufacture and / or installation of VSB's and their Nominated Security contact details.

The scheme will be open to all manufacturer and installer companies to join (not just PSSA members) with an annual administration charge payable by each member company.

The PSSA will chair an Independent Advisory Group, comprised of scheme members and key strategic partners, who will set the scheme's high level objectives, output & requirements.

The PSSA will be responsible for monitoring the registration and compliance with the scheme.

The PSSA in will disseminate best practice guidance from UK Government, scheme members and other partners.

The guidance is designed to support the Code of Practice (CoP) on page 4 which sets out the requirements expected of those wishing to join the HVMIS. Organisations wishing to join the scheme must commit to meeting the requirements of the CoP and have in place a plan demonstrating how this has or will been achieved.

The scheme will be auditable and copies of all sign off documents will be held by PSSA and randomly checked for accuracy and compliance.

Non-compliance with the CoP could lead to the exclusion from the scheme.

The Scheme will deliver wider benefits for industry and the general public.

As a general note, the CoP will act as support to the expected new Protect Duty Act and will be reviewed / amended accordingly when new legislation is enacted to support members.

Benefits to Industry

An organisation's Corporate Social Responsibility (CSR) duties will include; protecting the public, its customers and assets. By joining the HVMIS an organisation will be demonstrating that it takes security and its CSR responsibilities seriously.

Benefits of HVMIS membership include:

- Helping to keep defined assets, events and the public safe from vehicle borne attack

- Protecting the Organisation's reputation

- Corporate Social Responsibility

- Competitive advantage

- Improved professionalism within the business

- The scheme will help organisations assess their security risks and take appropriate actions

- Crime reduction

- Enhanced Staff training

- Professional image

- Continuous improvement in standards

HVMIS Code of Practice (CoP)

Each member shall;

Appoint a Recognised Security Contact (RSC) for the business and (where practical) a deputy.

Ensure that product specific installation training (Annex D) has been undertaken by all relevant operatives involved in the installation works.

Check that the client / operator has a clear operational requirement and has this been compiled in conjunction with advice from CPNI / NaCTSO and open source information.

Confirm that the product being installed is in an "as rated" format and if not ensure that the client / operator has been made aware (in writing) if this is not the case.

Check the status of client / operators CT insurance (if any) and note status on handover form (Annex G).

Based on the operational requirement or tender specification, the member company should ensure that appropriate security equipment is being utilised and notify the client / operator (in writing) of any concerns. Examples of concerns should include but not limited to:

- Does the equipment need supervision / guarding to stop removal (for temporary solutions)?
- Are automatic barrier controls in secured locations?
- Has full operational training been given?

On installation completion, a formal hand over document (Annex G) including details of all equipment installed, operating and maintenance information and any non-compliance / concerns regarding the installation must be signed by the client / operator with a copy held by the installer.

Members' staff are expected to support law enforcement counter terrorism and communications campaigns such as ACT and share data and information with law enforcement agencies where it can be done so lawfully and consistent with data protection requirements.

Data Protection Act (DPA) and the General Data Protection Regulation (GDPR) 2018. The member company will ensure staff have sufficient training in regard to the DPA and GDPR

Non-compliance with the CoP

It should be noted that failure to demonstrate that you have met the requirements of this code could invalidate your application/ registration and could lead to your exclusion from the scheme.

Supporting Guidance - Completing a Security Plan

As part of the application registration (see Annex B) you need to confirm that you have completed the Security Plan Proforma that can be found at Annex C.

The pro-forma (a copy of which you should retain) is intended to demonstrate how the company has (or will) meet the requirements of the CoP. The pro-forma should form the basis of a security plan which you should develop and which, in due course, may be subject to assurance checking by PSSA.

PSSA can assist in the development of the security plan and additional guidance can be found on the Centre for the Protection of the National Infrastructure (CPNI) and NaCTSO websites.

Guidance for completing the security Plan is outlined below:

Appointment of a Recognised Security Contact (RSC)

- The Registered Company (RC) will appoint a Recognised Security Contact (RSC) and, where practical, a deputy within the organisation. These persons will act as the focal point for the dissemination of counter terrorism security advice and procedures on the company's behalf.
- The RSC will actively utilise and share National Counter Terrorism Security Office (NaCTSO) and Centre for Protection of National Infrastructure (CPNI) online material and engage with National Counter Terrorism Police Headquarters (NCTPHQ)/PSSA on any relevant law enforcement related activities.
- The RSC will ensure that they are up to date with security training (such as ACT e-learnings or other training products supplied by their CPNI / NaCTSO and, where appropriate, that supplied by other sources.
- The RSC (or a nominated person) should ensure that all staff receive the required levels of security training to enable them to fulfil their roles.
- The RSC will act as the point of contact between the organisation and PSSA/Law Enforcement agencies and will be the person that receives security related communications.
- The RSC should ensure that, on an as appropriate basis, security related messaging is displayed at the place of business.
- The RSC should ensure that staff are undertaking the necessary checks (as outlined in the Code of Practice).

Training

Training staff to identify and report suspicious behaviours

The Registered Company (RC) should ensure that counter-terrorism guidance is available to staff and ensure they trained in customer verification procedures to help build a culture of vigilance.

All staff involved in the installation of VSB's should have completed the ACT (Action Counters Terrorism) awareness course (https://ct.highfieldelearning.com/) and certificates submitted to PSSA by the RSC in support of the RC registration.

The RC will have in place a mechanism for reporting suspicious behaviours to the relevant law enforcement authorities and ensure that company procedures and management processes incorporate the use of this mechanism where appropriate. If no procedures are in place to identify and report suspicious activities/behaviours, CPNI have existing guidance on increasing employee vigilance this can be found at https://www.cpni.gov.uk/employee-vigilance

Support law enforcement reporting and communications campaigns

The RC will agree to support Government counter terrorism reporting and communications campaigns where the material is relevant and suitable, one example of this being the current Action Counters Terrorism (ACT) campaign.

Where practical the RC will support the campaign by displaying the logo on the company website and at their place of business.

Staff Training

As part of the organisation's recruitment and retention process, staff should be trained to enable them to undertake their role. Part of this training should include, where appropriate, recognising suspicious behaviours and awareness of the company reporting process.

The RSC will also train staff to ensure that customers are provided with the most suitable VSB to meet their requirements (this may offer an opportunity for identifying suspicious behaviours).

Data Protection Act and the General Data Protection Regulation.

The RC will also ensure all relevant staff have sufficient training in regard to the Data Protection Act and the General Data Protection Regulation (GDPR) 2016/679 so that in the event of a law enforcement request, staff understand their overall obligations and whether they are able to share data when requested.

Supporting information resources

CPNI Security Systems Management and Risk Assessment Advice

The Centre for the Protection of National Infrastructure (CPNI) is the Government authority for protective security advice to the UK national infrastructure. Its' role is to protect national security by helping reduce the vulnerability of the national infrastructure to terrorism and other threats.

CPNI produce a number of guidance documents which can assist organisations in drawing up security plans. These are available free of charge on the CPNI website. The following products may be of particular assistance:

- https://www.cpni.gov.uk/principles-risk-assessment Provides guidance on the principles of risk assessment

- https://www.cpni.gov.uk/content/mitigate-your-risks Provides guidance on how to mitigate risks that may affect you organisation

- https://www.cpni.gov.uk/secure-4-assessing-security-culture Outlines why it is important to get a security culture right

- https://www.cpni.gov.uk/security-planning outlines the need for effective security planning

- https://www.cpni.gov.uk/hostile-vehicle-mitigation-0 An introduction to vehicle borne threats

- https://www.cpni.gov.uk/hvm-impact-rated Impact rated products

https://www.cpni.gov.uk/cse-chapter-hvm-delay-rated Delay rated products

https://www.cpni.gov.uk/insider-risk Review security risks associated with personnel

Annex A: Hostile Mitigation Installers Scheme: Code of Practice Declaration

In order to be included on the Hostile Vehicle Mitigation Installers Scheme register the Manufacturer / Installer Company should complete the declaration which can be accessed by the following hyperlink. https://TBA An example of the declaration can be found below.

We (insert company name)…………………………………………………… agree to adhere to the requirements set out in the Code of Practice set out above.

Signed*

   (Company Proprietor, Partner or Director (Please indicate)

Date:

* Note: by signing this declaration you agree that you have completed and retained the Security Plan Proforma (Annex C) and to have your security measures audited/assured by PSSA.

Once complete you should send this form along with your registration application (see Annex B) to PSSA using the following link admin@pssasecurity.org.

Annex B: Hostile Vehicle Mitigation Installers Scheme: Registration

In order to be included on the Hostile Vehicle Mitigation Installers Scheme register the registered Manufacturer / Installer should complete the application which can be accessed by the following hyperlink https://PSSA/???????? An example of the application can be found below.

Applicant details

1. Business name:

2 .Principal place of business:

3. Website:

4 Nature of business (a brief description of the main activities of your business):

 Contact details

5. Proprietor/Partner/Director (please indicate) :

Forename   Surname

Direct email Direct telephone:

6. Recognised Security Contact (if different from above):

Forename   Surname

Direct email Direct telephone

7. Deputy Recognised Security Contact (if different from above):

Forename   Surname

Direct email Direct telephone

8. Are you a member of the following organisations?

PSSA, BSIA, ADS

HVMIS
HOSTILE VEHICLE MITIGATION INSTALLERS SCHEME

Annex C: HVMIS Security Plan - Proforma

Please complete the proforma below outlining how you meet [or intend to meet] the requirements of code (please refer to the Code of Practice and supporting guidance when completing this form):

Does the organisation meet the requirements of the CoP?

CoP Ref	Gaps identified?	Actions taken	Sign off/date
1. Appointment of a Recognised Security Contact (RSC) and deputy.			
2. Do you have a skills matrix detailing operative name and specific product training they have received? Is the matrix continuously updated? Do you use matrix to ensure that only properly trained operatives are used on installations?			
3.Do relevant operatives (site managers?) understand threat and risk assessments? Do you have a process for checking that the client / operator has undertaken threat and risk assessments in conjunction with CTP (CTSA / CT SecCo). Do you have a suitable and traceable method of recording this information?			
4. Do you have installation specific product information including the "as rated" information? How is this information communicated to installation teams? Are the installation team leaders trained in identifying proposed installations that are not "as rated"? Do you have an auditable document process to ensure that the client / operator is aware of the compliance status of the proposed installation and has accepted any non-compliances?			

5. Do installation team leaders understand the importance of CT insurances for the client / operators? Is there an auditable document process to confirm the status?			
6 How will your installation team leaders be trained in the review of the assessments of threat and risk? How will the installation teams ensure that appropriate security is being utilised? Is there an auditable document process to notify the client / operator (in writing) of any concerns?			
7 Do you have an auditable hand over document including details of all equipment installed, operating and maintenance information and any non-compliance / concerns regarding the installation? How will you ensure that the document is signed by the client / operator?			
8.Have you signed up to the ACT campaign? Do you encourage regular CT training using CPNI available resources?			
9 Will you agree to share data and information with law enforcement agencies where it can be done so lawfully and consistent with data protection requirements?			
10. How will you ensure that staff have sufficient training with regard to the DPA and GDPR? Will you ensure that your staff have sufficient training to understand the principals and their ability to share data when requested?			

Annex D – Training Matrix M-Mandatory R-Recommended	Recognised Security Contact (RSC)	Deputy RSC (DRSC)	Project Manager (PM)	Installation Team leader (ITL)	Installation operative (IOP)
General training requirements					
Understanding of impact test standards (IWA14-1, PAS68, ASTM F2656 and VADS)	M	M	M		
Impact / VAW test attendance (ideally both)	R	R	R		
Completion of relevant CT Courses from NaCTSO and/or UK Government'. Eg ACT	M	M	M	M	R
Manual handling	R	R	R	M	M
Appropriate Health and safety training	M	M	M	M	M
First aid	R	R	R	M	R
Road closure completeness checking (please note that it is envisaged that traffic management and road closures will not form part of the installation)	R	R	R	M	
Project management	M	M	M	M	
Site management	R	R	M	M	
Product specific training					
Understanding of impact test results of each product being installed including vehicle type, weight, impact speed, impact angle, penetration and debris disbursement where applicable	M	M	M	M	
Understanding of foundation / ground conditions of impact test for each product being installed	M	M	M	M	
Understanding of as tested configuration for each product being installed	M	M	M	M	
Installation and assembly process for each product being installed	M	M	M	M	M
Operation of moveable equipment being installed	M	M	M	M	M
Maintenance requirements for each product being installed	M	M	M	M	
De-commissioning and removal process for each product being supplied	M	M	M	M	M

Annex E - Manufacturer handover information

For each tested product, the installer must be issued with:

1. Product marketing information – sales literature or similar
2. Impact test report including
    -   Formation of rated VSB/ quantity / size / connections / configuration / orientation
    -   Test parameters (vehicle type, size, speed etc.)
    -   Impact test standard used
    -   Test house used
    -   Test date
    -   Test result (penetration. Debris disbursement (if known), vehicle disabled?)
    -   Foundation information and / or ground conditions
    -   Impact test video (real time full video)
3. Product technical information
    -   Dimensions
    -   Weight
    -   Ground fixing type, size and quantity used (if any)
4. Assembly / dis-assembly instructions
    -   Drawings
    -   Assembly fixings
    -   Training video (ideally)
5. Other information
    -   Operation manual
    -   Maintenance manual and checklist
    -   Product drawings
    -   Foundation drawings where applicable
    -   Rebar drawings where applicable
    -   Rebar schedule where applicable

Ideally the manufacturers should host regular installation training courses on the implementation of their products to ensure that installers are kept up to date at all times

Annex F - HVMIS process document

Starting point

Most of the VSB installation projects will be designed at a much earlier stage than the installer scheme covers and we are not recommending that installers are used to produce an Operational Requirement, threat assessment, vehicle dynamic assessment or protective scheme design. This is not to say that some installers are not capable or competent in undertaking this work but is a restriction on the scheme, to focus on the deployment of the protective measures.

Where products cannot be deployed in their exact tested and rated formation due to site constraints, the installers experience in deploying HVM should help to provide a risk based solution within both physical constraints and the client's budget. Any changes to the solution recommended by the installer must be further verified by an independent third-party review.

General process

Tender Stage

- RFQ (or Tender) is received showing the protective measure requirements
- RFQ is reviewed by the installer for obvious errors / conflicts etc. and client clarification requested.
- If RFQ protective measure design seems to have major weaknesses check for involvement of NaCTSO (inc. CTSA's and or CT SecCos) / CPNI in the design and if none, recommend their engagement.
- Site visit (wherever possible) to review conditions and layout proposals
- Quotation issued clearly showing:
    - Client responsibilities (eg. layout design, site specific H&S / environmental requirements, safe access for loading / unloading, road closures both temporary and permanent, traffic management)
    - Installer responsibilities (eg. Installation risk assessment and method statement, delivery, offloading, assembly and installation of equipment, derig and collection of equipment)
    - List of equipment being provided with impact test information (including units / sizes tested, test result string, foundation / ground condition for test and layout design)
    - Details of any areas of non-compliance with as-tested design as a result of site visit or RFQ review
- Order issued to installer
- Order checked by installer and acceptance confirmed

Preparation stage

- Preparing an installation / deployment Risk Assessments (RA's) and Method Statement (MS) and operational / removal RA's and MS's if relevant (incorporating start date and installation program, clients' safety requirements and emergency procedures where applicable) for issue to and for acceptance by the Client.
- Check that client has Counter Terrorism insurance in place and if not, whether this should be considered.

- Equipment ordered and delivery / installation arranged including transport arrangements, road closures and timing plan.
- Once confirmed by the client, issue RAMS and Method statement to relevant site personnel and ensure they are fully understood.

Site works

- Pre-start handover meeting between installation project manager and client's representative. Use checklist and notes to confirm all items noted.
    - Check that the client has a clear operational requirement.
    - Check that all agreed road and pedestrian access closures are in place and being suitably managed.
    - Confirm that the products being installed are in "as tested and rated" configuration
    - and advise of any non-compliant areas.
    - For non-compliant areas, ensure that the client understands the ramification of this and accepts the consequent liability.
    - Confirm any requirement for the equipment to be supervised / guarded to stop removal (for temporary solutions). Check that controls for any automatic barriers are in secured locations.
    - Identify site Installation Supervisor / Project Manager to clients representative.
    - Check and confirm that RAMS and method statement are still correct and relevant and adjust if required.
    - Client representative to identify all staff needing training in operation and / or maintenance of the systems. These should be noted on the checklist.
- Pre-start checklist form with notes to be signed by both the clients representative and the installation supervisor / project manager with a copy issued to each. Pre-start Toolbox talk by Installation supervisor / project manager and all installer operatives to review the RAMS and method statement and ensure they are all fully understood.
- General health and safety check including but not limited to PPE, tools and equipment, environment and site surroundings.
- Photograph work areas before installation commencement – subject to security restrictions and client approval.
- Installation works undertaken
- Photograph work areas after installation completion– subject to security restrictions and client approval.
- Provide operational / maintenance training to client / operator staff as advised at pre-start handover as well as any others subsequently added to the training requirement (details of all those trained and training given be recorded on the handover document) - this is a mandatory element of the process and cannot be excluded. CPD updates regarding installation processes will be provided for a period of 12 months from handover.
- Installation completion handover document from the installation supervisor / project manager to the clients' representative must be completed and include:
    - Confirmation of products installed
    - Identification of those products installed that are not in "as tested" format including explanation of the variance from original impact test.
    - Operation and maintenance manuals where applicable handed over
    - Any other notes or points for concern

- Handover document with notes to be signed by both the client's representative and the installation supervisor / project manager with a copy issued to each.

De-rig of installation (temporary solutions)

- Issue de-rig RAMS and method statement.
- Pre-start Toolbox talk by Installation supervisor / project manager and all installer operatives to review the de-rig RAMS and method statement and ensure they are all fully understood.
- General health and safety check including but not limited to, tools and equipment, environment and site surroundings
- Check that all agreed road and pedestrian access closures are in place and being suitably managed.
- Photograph work areas before derig commencement – subject to security restrictions and client approval.
- De-rig works undertaken
- Photograph work areas after derig completion– subject to security restrictions and client approval.
- De-rig completion hand over document from the installation supervisor / project manager to the clients' representative must be completed and include:
  - Confirmation of products removed including notes of any damage (with photographs).
  - Confirmation of all waste removed and site left good.
  - Return of operation and maintenance manuals where applicable
  - Any other notes or points for concern
  - De-rig completion document with notes to be signed by both the clients representative and the installation supervisor / project manager with a copy issued to each.

Annex G – Handover Form

HVMIS Handover Document				
Installer Company Name				
Installer handover Manager				
Client				
Rated Product being installed	**Manufacturer**	**Product**	**Qty**	**Installed as Rated Y/N**
Installation handover date				
Have all relevant installation operatives been given product specific installation training	Y/N			
Has the installer received the handover information from the manufacturer as set out in Annex E of the Scheme	Y/N			
Is there a clear operational requirement document in place	Y/N			
Has the installer been shown the operational requirement document	Y/N			
-If Yes, has the scheme been compiled in consultation with NaCTSO/CPNI	Y/N			
Is the equipment being installed commensurate with the operational requirement	Y/N			
-If No, has the client/operator been advised of any concerns in writing (Submit a copy of this to PSSA with the handover document copy)				
Is the product installed "as rated"	Y/N			
-If No, has the client/operator been advised of variances in writing (submit a copy of this to PSSA with the handover document				

Does the Client/Operator have valid CT insurance	Y/N		
Has operation and maintenance training been given to the satisfaction of the Client/Operator	Y/N		
Have operation and maintenance manuals/documentation been issued to Client/Operator	Y/N		
Other Comments/Concerns raised			
	Name	**Signature**	**Date**
Signed by Installer			
Signed by Client/Operator			
Checked by Installer RSC			