Department for Transport

Light Rail Security
Recommended Best Practice

June 2014

The Department for Transport has actively considered the needs of blind and partially sighted people in accessing this document. The text will be made available in full on the Department's website. The text may be freely downloaded and translated by individuals or organisations for conversion into other accessible formats. If you have other needs in this regard please contact the Department.

Department for Transport
Great Minster House
33 Horseferry Road
London SW1P 4DR
Telephone 0300 330 3000
Website www.gov.uk/dft
General email enquiries FAX9643@dft.gsi.gov.uk

Cover photo acknowledgements

Clockwise from left:

Manchester Metro © Transport for Greater Manchester / TfGM

Safer Travel Team with Centro tram © Centro

Sheffield Supertram © South Yorkshire PTE/SYPTE

Newcastle Metro CCTV monitoring © Nexus

Images reproduced with kind permission of Transport for Greater Manchester / TfGM, South Yorkshire PTE/SYPTE, and Nexus.

Contents

Foreword 5

Executive summary 6

1. Introduction 7
Background 7
How to use this guidance 8
Sources of advice and further guidance 8
DfT contact details 10
DfT Light Rail Security Network 10

2. Organisational security culture 11
Building and embedding a security culture 11
Personnel security 12
Security training 12
Administrative staff 13
Training records 13
Contingency (emergency) plans 14
Security exercises 15

3. Handling threats and incidents 17
Received threats 17
Firearm incidents 18
Response to unattended and suspicious items 18
Response to suspicious behaviour 19
Discovery of 'white powders' 19
Responding to a cyber incident 20

4. Security of light rail carriages and vehicles 23
Rolling stock design 23
Searches and checks 23
Securing vehicles and carriages not in service 24
Control of passengers boarding and leaving 24
Baggage reconciliation 24
Security awareness measures for passengers 25
High visibility clothing 25
On board Closed Circuit Television (CCTV) 25
Security enhancements at times of increased threat 27

5. Security of light rail stations, termini and interchanges 28
Security in Design of Stations (SIDOS) and Hostile Vehicle Mitigation (HVM) 28
The Safer Tram Stop Award 29
Searches and checks 29
Construction work at a station 30
Links to other public transport systems 31
Control of access to public / non-public areas 32
Visitors and contractors 33
High visibility clothing 33
Areas of concealment 34

Waste management 35
Bicycles 36
Equipment boxes 36
Public toilet facilities 37
Post boxes 37
Tenants and cleaners 37
Security awareness measures for passengers 37
Closed Circuit Television (CCTV) 38
Left luggage facilities 38
Car parks / park and ride facilities / car rental facilities 39
Commercial developments at stations 39
Security enhancements at times of increased threat 40

6. Security of depots and maintenance facilities 41
Physical protection 41
Control room security 41
Rolling stock on site 42
Closed Circuit Television (CCTV) 42
Staffing / patrolling 42
Passes: recording and issuing 43
Motor vehicle access and parking arrangements 43
Security awareness measures 44
Security controls 45
Control room security 45
Security enhancements at times of increased threat 45

Annex A - Bomb / Threat Report Form 47

Annex B - Marauding Active Shooter guidance 50

Annex C - Suspicious items - using the HOT protocol 54

Annex D - Quick reference security checklist 56

Annex E - General online resources 62

Annex F - Closed Circuit Television (CCTV) specific publications 64

Annex G - Vehicle search routine for entry to depots 65

Annex H - Glossary of terms 66

Foreword

On 18 October 2010 the Government published its National Security Strategy which reiterated that the international terrorist threat to the UK is a tier one risk. This makes it part of a group of the highest priority risks for UK national security looking ahead, taking account of both likelihood and impact. Therefore work in protecting the travelling public will be essential for the foreseeable future.

Terrorists continue to target railway services across the world. The Madrid commuter train attacks on 11th March 2004, London attacks on 7th July 2005 (three of which occurred on the Underground) and suicide attacks in Volgograd railway station on the 29th and 30th December caused death, injury and disruption. These are clearly very rare events, but potentially high impact, hence there is a need to plan, and to remain vigilant. Along with physical attacks, the transport network has also been disrupted by telephone threats, unattended items and hoax devices.

The constantly changing nature of the risks and threats has necessitated a refresh of the original guidance published by the Department for Transport (DfT) in 2007. This 2014 document assembles the latest best practice security measures, and we hope that it helps your operations and staff to run a safe and secure network. This guidance covers the 7 light rail systems (Blackpool Tram, Croydon Tramlink, Manchester Metrolink, Midland Metro, Nottingham Express Transit, Sheffield Supertram and Tyne & Wear Metro) and can be used to help new networks ahead of commencing operations, for example the Edinburgh Tram. We encourage you to make full use of this guide.

Executive summary

1. An effective protective security regime must take account of the prevailing threat and likelihood of a security incident, the vulnerability of potential targets and the potential consequences of an attack. Together these identify the risk to the operators and infrastructure and to those using them and working on them.
2. The open nature of the environment around light rail stops and stations presents a greater challenge than some other transport modes where access can be more readily restricted to certain areas and screening and searching regimes are in place. Nonetheless, the opportunity exists to embed systems for effectively managing risk, and this guide shows you how to do that.
3. Security measures will generally be a proportionate combination of "front line" physical and procedural security measures (e.g. screening, searching, physical barriers, patrolling) and "secondary" measures (e.g. background checks, security vetting and training), depending on the prevailing threat.
4. A "multi-layered" approach to security is more robust, acknowledging that no single security measure is either fool-proof or capable of mitigating every type of threat. Security measures should therefore be commensurate to the risk, effective, holistic, practicable and sustainable. The aim is to deter would be perpetrators, detect prohibited articles and respond to any potential threats. Your security regime should also provide reassurance to passengers.

1. Introduction

Background

1.1 The Department for Transport (DfT) sets and enforces counter terrorism security measures on a number of transport modes. This includes aviation, maritime, the national and international rail network, London Underground, the Docklands Light Railway (DLR) and Glasgow Subway. One of the recommendations flowing from a comprehensive review of railway security undertaken after the 2004 Madrid train bombings was that the DfT formalise its relationship with the other light rail networks through the development of specific best practice security regimes. This was because of the continuing serious nature of the terrorist threat and the integral nature of these systems to the wider rail network.

1.2 Since 2007, the seven light rail systems in Great Britain (Blackpool Tram, Croydon Tramlink, Manchester Metrolink, Midland Metro, Nottingham Express Transit, Sheffield Supertram and Tyne & Wear Metro) have therefore been covered by an advisory regime of recommended best practice. However, if this advisory approach proves to be unsatisfactory, Ministers can exercise their powers under the Railways Act to issue such security instructions as they consider appropriate to provide protection against acts of violence.

1.3 This guidance replaces the Light Railway Security Recommended Good Practice published in January 2007, to reflect developments in the terrorist threat and associated security advice. It has been developed to help operators devise and maintain a range of best practice security measures. It covers depots, stops and stations, rolling stock and infrastructure used for operating light rail systems along with generic security issues such as personnel security. The measures outlined are based on experience gained in developing and putting in place effective, proportionate, viable and sustainable security measures for other transport areas, and on some good practices that various light rail operators already have in place.

1.4 This guidance is generic, although it is recognised that the light rail systems across the country are quite different from each other in several respects. Some recommendations therefore may not fit with a particular environment or set of circumstances. It should however enable you to gain a good understanding of the issues to consider and provide a range of options that could be implemented, including basic measures, together with suggested enhancements which can be draw on at times of heightened concern (e.g. if there is a bomb threat, or if the country moves to a higher threat level). More information about threat levels is

on the Security Service website[1]. We suggest checking the website regularly for changes.

1.5 We have developed the updated guidance in discussion with a range of stakeholders including the light rail networks, the Confederation of Passenger Transport UK (CPT), the Passenger Transport Executive Group Safety and Security Group (PTEG S& SG), Scottish and Welsh devolved administrations, the Home Office, the Centre for the Protection of National Infrastructure (CPNI), the police and the National Counter Terrorism Security Office (NaCTSO). The revised guidance has been welcomed by the stakeholders involved in updating it. This guidance is available on the gov.uk website.

How to use this guidance

1.6 This guidance is for operators of light rail and owners/managers of light rail stations and depots. Sections 1, 2 and 3 are generic and relevant to all, 4 to light rail rolling stock (vehicles and carriages), 5 to light rail stations and termini, and 6 to depots. We suggest that you draw on this guidance for the development and implementation of your own security regimes, tailored to your respective operations. The Quick Reference Checklist at Annex D can help you do this.

1.7 We also recommend building these measures into your contingency planning (see Section 2).

1.8 We have also produced a Passenger Rail Security DVD training aid (free to operators on request) which complements this guidance. Details of how to obtain the DVD are given at the end of this section.

1.9 Following this guidance will help you to strengthen security, reassure your passengers and increase public confidence in using light rail services and facilities generally. It can also offer positive benefits in helping to reduce the risk of crime and anti-social behaviour.

1.10 The three key elements underpinning the advice throughout are:

- Establish a security regime;
- Check that this is operating as it should; and
- Be vigilant beyond the formal measures.

Sources of advice and further guidance

1.11 Whilst this guidance and the Passenger Rail Security DVD are important sources of advice, they should not be seen as the only available reference.

Police forces

1.12 Police forces are a good source of free advice, and will be able to provide guidance to assist you in determining suitable security measures. Additionally, specialist police advisers known as Counter

[1] https://www.mi5.gov.uk/home/the-threats/terrorism/threat-levels.html

Terrorist Security Advisors (CTSAs) promote awareness of the terrorism threat and develop relationships with partner agencies and site owners to encourage a co-ordinated approach. CTSA contact details can be found on the British Transport Police (BTP) (www.btp.police.uk) and National Counter Terrorism Security Office (NaCTSO) websites (www.nactso.gov.uk).

1.13 The policing of the networks is organised as follows:

Network	Police force
Blackpool Tram	Lancashire Constabulary
Croydon Tramlink	BTP
Edinburgh Tram	Police Scotland
Manchester Metrolink	Greater Manchester Police
Midland Metro	BTP
Nottingham Express Transit	Nottinghamshire Police
Sheffield Supertram	South Yorkshire Police
Tyne & Wear Metro	BTP

1.14 Whilst the majority of light rail operators receive police assistance from local constabularies, the BTP can provide specialist advice tailored to the rail environment. They can help you to build in a range of preventative measures and contingency planning considerations. The BTP has extensive knowledge of working with operators, and balancing the requirement of keeping the railways moving, with keeping them safe and secure. The BTP also provides a range of rail specific security training, more of which is detailed in Chapter 2 of this guidance.

Centre for the Protection of National Infrastructure (CPNI)

1.15 The Centre for the Protection of National Infrastructure (CPNI) protects national security by providing protective security advice. (http://www.cpni.gov.uk/about/#sthash.rdGDIbO2.dpuf) CPNI provides advice on physical security, personnel security and cyber security/information assurance. Most importantly, they explain how these components combine together and reinforce each other. A useful introduction is their booklet entitled 'Protecting Against Terrorism', which offers general protective security advice for businesses and other organisations[2].

[2] http://www.cpni.gov.uk/documents/publications/2010/2010002-protecting_against_terrorism_3rd_edition.pdf

Office of Rail Regulation (ORR)

1.16 The ORR (orr.gov.uk) have a remit to secure the proper control of risks to the health and safety of employees, passengers and others who might be affected by the operation of Britain's railway systems.

Local Authorities

1.17 Local authorities prepare emergency planning guidance as a requirement under the Civil Contingencies Act (2004) and may be able to provide assistance on some aspects, e.g. contingency planning. They can also assist regarding the positioning of street furniture such as litter bins or cycle racks.

Other Operators

1.18 You may find it helpful to contact other operators and infrastructure owners/managers (i.e. those who own and/or manage light rail stations and depots) to consider sharing best practice. Also, if you own or run a light rail station adjoining a railway station, the station manager should already be in touch with you, but if not, we recommend that you contact them to discuss and implement mutually beneficial security measures. Refer to paragraph 5.10 for more information on links to other public transport systems.

DfT contact details

1.19 Should you wish to know more, or have any questions about light rail security, please e-mail your enquiry to landsecurity@dft.gsi.gov.uk. You can also write to the Domestic Land Transport Security Team at :

Great Minster House, 33 Horseferry Road, London SW1P 4DR

DfT Light Rail Security Network

1.20 The DfT has established a Light Rail Security Network, (LRSN) which is an informal group sharing advice and best practice amongst operators. Those Light Rail Operators who have not already joined are encouraged to. If you would like more information or are interested in joining the network, please write to landsecurity@dft.gsi.gov.uk .

2. Organisational security culture

2.1 Security measures will generally be a combination of ‘‘front-line’’ physical and procedural security measures (e.g. searching, physical barriers, patrolling) and ‘‘secondary’’ measures (e.g. emergency planning, background checks, briefing/training). A ‘‘multi-layered’’ approach to security is more robust, acknowledging that no single security measure is fool-proof or capable of mitigating every type of threat.

Key actions:

- Effective pre-employment screening checks for job applicants (e.g. ID checks);
- Regular staff security briefings and training;
- Establish or review your emergency plans and test them regularly; and
- Contact your police force to obtain advice on protecting your network.

2.2 The CPNI and NaCTSO have produced guidance on building organisational security culture and on personnel security measures. These are designed to help organisations manage the risk of staff or contractors exploiting their legitimate access to their premises, information and staff for unauthorised purposes. The text at paragraphs 2.4 to 2.7 and 2.9 below is taken from that advice:

Building and embedding a security culture

2.3 Developing a security culture within an organisation is about encouraging staff to respect common values and standards towards security whether they are inside or outside the workplace. It is important therefore that somebody within your organisation has a clear responsibility for security, and works to build a security culture throughout the organisation.

2.4 The awareness of security amongst staff – their vigilance when conducting everyday routines, for example – is an essential part of an organisation’s protection and staff training: regular exercise and internal communications play an important part. Equally important is the manner in which a business reinforces its words through its actions.

2.5 If an organisation wants its employees to act appropriately, it must provide an environment that sets an example. For instance, if staff are required to keep paperwork securely locked away but they are not

provided with sufficient storage (or broken locks are never repaired), they may question the management's commitment to security. Likewise, staff ID passes should be worn at all times and a culture of enforcement established.

2.6 A security culture is about more than facilities and procedures – it is also about creating an environment that is focused and proactive about identifying and reducing risk, for everyone's benefit.

Personnel security

2.7 Personnel security is a system of policies and procedures that seek to manage the risk of an 'insider threat'. This is the threat from individuals working somewhere within the industry and abusing their access for malicious purposes. Personnel security measures offer some protection against the use of insiders by terrorists, criminals or the media. Good personnel security ranges from proportionate but thorough pre-employment screening to the provision of ongoing care (once the job applicant is employed). The latter is to protect against existing employees who may foster a grudge against their employer, develop terrorist sympathies, or who may have been coerced out of loyalty to a family member or friend to do harm to their organisation.

2.8 Although many organisations regard personnel security as an issue resolved during the recruitment process, it is a discipline that needs to be maintained throughout a member of staff's time in employment: through appraisal procedures, communication programmes, incentive schemes and even management attitudes and relationships. It should include a formal process for managing staff leaving the business.

2.9 When consistently applied, personnel security measures not only reduce operational vulnerabilities – they can also help build a hugely beneficial security culture at every level of an organisation.

2.10 Further guidance on personnel security can be found on the CPNI[3] and NaCTSO websites[4].

Security training

2.11 We recommend that any staff (e.g. drivers, cleaners, security staff, CCTV operators, customer service / information desk staff and other front lijne staff) whose duties or tasks include the following, be briefed regularly (and if possible be given appropriate training) to ensure that they are aware of their security responsibilities and how to respond appropriately:

- Searching or checking rolling stock;
- Passenger luggage reconciliation;
- Searching or patrolling a station or other public area;
- Controlling access into a non-public area;

[3] http://www.cpni.gov.uk/advice/Personnel-security1
[4] http://www.nactso.gov.uk/managing-the-risks

- Searching by hand or screening by x-ray or other detection equipment baggage being placed in a left luggage or lost property facility; and
- Issuing passes for access to a non-public area

2.12 We also suggest that training be given to those appointed as or acting in the capacity of:

- Security managers;
- Directors and other senior staff whose appointments involve executive, operational or administrative responsibility for light rail security; and
- Managers and supervisors who have no direct responsibility for security operations or staff, but who control operations, premises or staff.

2.13 You may wish to use the free Passenger Rail Security DVD (see Section 1) as part of your front-line staff training, along with Project Argus[5] and Project Griffin[6] Training. Project Argus is a NaCTSO initiative aimed at managers to explore ways to prevent, handle and recover from a terrorist incident and Project Griffin is a police initiative to provide public facing staff with practical awareness of the CT threat and associated matters. This training is delivered by police CTSAs. Contact your police force for further information.

Administrative staff

2.14 Telephonists, receptionists, and other staff who may receive threat warnings should be briefed before taking up their duties. The responses required from them should be incorporated into appropriate staff instructions and they should be provided with checklists to remind them of the steps to take should they receive a threat warning. Their supervisors should be similarly aware of the response required, and of the need to handle information about bomb or other threats in accordance with local police advice – see Section 3.

Training records

2.15 Where your staff are given specific training, we recommend that you maintain training records that include:

- The date that each staff member took up a security related post
- The initial / refresher training given to each member of staff; the date or dates on which it was given; and

[5] http://www.nactso.gov.uk/our-services
[6] http://www.projectgriffin.org.uk/

- The signature of each staff member to confirm that they received that training

Contingency (emergency) plans

2.16 If you have not already done so, you should consider establishing plans to deal with any situation affecting your business and which is likely to prejudice public safety or disrupt your ability to operate normally. You will be aware that disruptive events cover a wide range of scenarios and include terrorism, fire, adverse weather, loss of service (power, fuel etc.) and loss of staff. Make sure that these also consider possible terrorist acts. For example, what would you do if there was a bomb threat to your premises – where could you relocate to in such an event, and how would you direct passengers, staff and vehicles there?

2.17 The five golden rules of contingency planning are:

- Think about it;
- Plan for it;
- Tell staff about it;
- Test it; and
- Keep it up to date

Developing the Plan

2.18 A plan may cover a whole network, but operators should consider carefully where it would add value to support it with individual plans for distinct sections of the network e.g. a train depot, a large station, or one where the light rail system interfaces with heavy rail or buses/depots, the control room etc. Your Local Authority Emergency Planning Officer can help in the development of risk assessments and contingency plans tailored to your network.

2.19 A contingency plan should cover the response action required in the event of:

- Threats against stations/vehicles/depot/other infrastructure and facilities;
- Discovery of a suspect or prohibited article;
- A breach of security;
- Times of heightened security; and
- Anything that reduces usual security regime e.g. staff absences.

2.20 In addition to dealing with an immediate response the plan should also provide for continuity of security as an integral element of business continuity.

2.21 Contingency plans should take account of the need for co-ordination between the various agencies involved. They should detail the

responsibilities of operators / infrastructure providers in respect of station facilities, trains, passengers, staff and any other relevant assets; the police (who have primacy in dealing with any act of unlawful interference against the railway); other operators in locations where facilities are shared; and local authorities. Plans should also detail contact information for the DfT in the case of a security incident, (TICB@dft.gsi.gov.uk Telephone 020 7744 2870) or in a cyber security incident (see Chapter 3 for more information on cyber incidents, and who to contact if they occur).

Disseminating the Plan

2.22 The plan should be accessible at all times and staff should know where to find it if required. It is also recommended that the responsibilities and the actions outlined in it are covered in staff instructions and staff training programmes. Copies should also be held by a recognised security contact within the company, and the police.

Reviewing the Plan

2.23 The plan should be reviewed and updated at least once every 12 months. The review should take into account:

- The findings from exercises - there is great value in exercising contingency plans on a regular basis - at least annually. The exercises may be by drill or by table top simulation;
- Operational information - data on unlawful interference, security occurrences and breaches of security should be collated and analysed. This will help pinpoint the development of further measures to prevent a recurrence;
- The outcomes arising from activation - if the Plan is called into action then lessons learnt need to be identified and the Plan amended as required;
- Changes in circumstances - the Plan should be amended during the year as and when changes in circumstances arise, but it is a good idea to schedule in a review of factors such as development work around a station, new tenants, new postholders / contact numbers etc.

Security exercises

2.24 Exercising enables you to:

- Test existing plans, procedures and systems;
- Allow staff to practice their agreed roles in a simulated and safe environment; and
- Evaluate the exercise and make any amendments to the plans as required.

2.25 Exercises give everyone an opportunity to practise arrangements with a wide range of people and to identify any gaps in contingency plans,

against a variety of scenarios to ensure they are sufficiently robust and that your staff are familiar with them. We suggest that, where appropriate, you involve the emergency services and local authority in rehearsals and exercises. You may also join in with exercises organised by the emergency services or other transport operators. Your Local Authority Emergency Planning Officer can help you identify the correct contacts.

3. Handling threats and incidents

Key actions:

- Print out the threat report form (Annex A);
- Put it in a prominent place near to publicly advertised phone lines;
- Talk about it with staff who may receive a threat call; and
- Use the Marauding Active Shooter Guidance (Annex B) and HOT Protocol (Annex C) to brief your staff.

Received threats

3.1 Threats may be received by light rail staff, station staff or anyone connected to light rail operations. Most threats are made anonymously by telephone, (although they may be written, emailed or posted on social media). They may be received directly from the people issuing the threat or via the police or through intermediaries (e.g. the media, press agencies etc.) Recipients should try to obtain as much information as possible about the threat in order to help the police to assess it and identify the person issuing it.

3.2 Threats are usually hoaxes. Hoax telephone calls or written messages are intended to cause a nuisance, however they must be taken seriously and assessed properly, as a small number have been genuine and have preceded a terrorist or criminal act. In the first instance, we suggest you contact your police force on how to handle any threats received. Any event assessed as a deliberate hoax (physical or otherwise - see paragraph 3.6 on unattended and suspicious items) is a crime and requires investigation by police.

3.3 We recommend that any recipient of a call or message completes the Threat Report form at Annex A (which is based on the standard police threat report form) and passes it without delay to their supervisor. The supervisor should inform the police. Recipients of a written threat should keep the message and pass it to their supervisor with precise information about its discovery. Staff who are likely to receive a threat (such as customer services and sales staff), should be briefed on the possibility and what to do on taking up their duties. Supervisors should be similarly aware of what to do and of the need to relay information about any received threat to the police. These briefings should be repeated on a regular basis to maintain staff knowledge and awareness. (See Section 2 – Organisational security culture).

Firearm incidents

3.4 The BTP has developed a guidance note for the rail industry (based on advice prepared by NaCTSO) detailing what to do if there is a marauding terrorist firearms attack or active shooter incident affecting the network. This could be by a co-ordinated group of terrorists as in Mumbai, India (2008), Westgate Shopping Centre, Kenya (2013) or by a lone gunman (Norway 2011). This is not, however, a rail specific issue as it concerns any public crowded place.

3.5 The parts of the guidance most relevant are offered at Annex B for you to use if you wish, as best suits the needs and circumstances of your operation. For example, you could make it available to your staff in its entirety, or use it as a basis for staff briefings.

Response to unattended and suspicious items

3.6 Lost property is an inevitable consequence of mass transit travel. In contrast to most of the unattended items encountered daily, a small number may cause a concern because of their physical appearance, their placement, or other circumstances associated with their discovery. A suspicious item, therefore, is one that exhibits unusual characteristics (appearance or placement) and for which a legitimate purpose cannot readily be established.

3.7 Staff should have established procedures to follow for dealing with items assessed and confirmed as suspicious. The HOT protocol, developed by the BTP and described at Annex C (also see searches and checks, Chapter 4) is one example of how to assess unattended items in a safe and efficient manner. Some examples of what staff should be briefed to look out for would include unusual packages, bags or other items in odd places, or carefully placed (rather than dropped) 'heavy' items in rubbish bins. Please refer to Annex C for full details of dealing with suspicious items using HOT.

3.8 As well as hoax telephone calls or written messages, operators may also discover a hoax item. A hoax item is any object constructed or placed deliberately in such a way as to cause concern and anxiety on the part of the finder (see Annex H for a full definition). Producing a hoax device is a serious offence (and may only become apparent after police or bomb disposal action at the scene of an item declared suspicious). However, any item believed to have been placed maliciously should always be reported to police. As noted in relation to anonymous threat message scenarios and overreaction to lost property, when such incidents cause disruption and attract media coverage, they can also generate imitative behaviour (i.e. copy-cat activity).

3.9 Once an item is assessed and confirmed as suspicious, people must be moved away from the scene, out of line of sight, and police advice sought urgently. If an immediate threat to life is perceived, evacuation distances are likely to be measured in hundreds of meters.

Response to suspicious behaviour

3.10 Suspicious behaviour can be defined as any behaviour that would be perceived by a reasonably prudent individual as of a kind that ought to be investigated by a person with security responsibilities. It is important that your staff know what to do and who to report their concerns to should they notice someone behaving suspiciously or have concerns about any suspicious items. Report suspicious behaviour to supervisors and the police.

3.11 Staff should be briefed to look out for any actions which may possibly indicate potential hostile reconnaissance/activity by criminals or terrorists. This might for instance include people showing unusual interest in sensitive, important or less accessible areas and specific interest in security regimes/features.

3.12 CPNI have produced a short film entitled 'Personnel Security: Eyes Wide Open'. The film explains how to spot people acting in a suspicious manner and how to deal with the situation. To access this, and for more information on hostile reconnaissance please contact CPNI or visit www.cpni.gov.uk .

Discovery of 'white powders'

3.13 A 'white powder incident' is a phrase often applied to the discovery of a substance (solid or liquid) where the finder cannot eliminate the possible presence of a chemical or biological hazard. (Not all such hazards are white, or powders). An example of the concern is the series of Anthrax attacks in the US in 2001. That event caused a small number of deaths and large-scale disruption (because of the need for extensive decontamination).

3.14 The majority of white powder incidents in the rail environment (and elsewhere) have related to benign substances and were not accompanied by any kind of threat information. Examples of risk aversion have included concerns about spilt flour (from a shopping bag); spilt plaster (dropped by a builder); salt (spilt on a canteen table); liquid soap (found under a soap dispenser in a staff bathroom); white powder (found after the discharge of a powder fire extinguisher). In the absence of a specific threat, or any other credible reason to believe such discoveries are suspicious, the scenario should be dealt with under normal housekeeping arrangements.

3.15 Where the discovery is believed to be malicious (e.g. a threatening letter, observed suspicious behaviour, a face-to-face threat received by staff or passengers), it should be investigated by police, who will also give specific risk management advice. In the unlikely event of people having been exposed to a genuine hazard, any uncoordinated evacuation will spread the hazard further, contaminate more people and delay effective medical intervention. In the absence of people becoming unwell, evacuation should be limited to adjacent rooms/carriages and people kept near the scene. In the event of a small scale contamination, the blue light services (police first point of contact) should be called. If the

substance is deemed toxic, the police will launch an initial operational response, drawing in colleagues from the other emergency services as appropriate.

Responding to a cyber incident

3.16 Any electronic or cyber incident, which affects any critical engineering assets or engineering assets that perform a safety function should be reported to the Department for Transport (TICB@dft.gsi.gov.uk Telephone 020 7744 2870) and Office for Rail Regulation (Telephone 020 7282 3910), in a timely manner. Incidents reaching the threshold of 'Level 0 - Exceptional Occurrence' as defined in the Centre for Cyber Assessment (CCA) Cyber Incident Coordination Plan (CICP) should be reported immediately to CERT-UK by telephoning 01242 709311 or by emailing (Unclassified to: enquiries@govcertuk.gov.uk ; and Restricted / Official Sensitive to: enquiries@govcertuk.gsi.gov.uk).

3.17 This does not preclude you from consulting the CERT-UK were you unable to manage the consequences of an attack alone.

Incidents that should be notified:

- Deliberate or accidental destruction, alteration, disruption, or disclosure of asset software or data, resulting from device connections;
- Successful unauthorised access or alterations to assets. (Unsuccessful attempts should be recorded locally for audit purposes and only notified if they are repeated or persistent);
- Malware infection of assets. (Blocked infection attempts, e.g. detected and blocked by anti-virus software and procedural controls, should be recorded locally for audit purposes and only notified if they are repeated or persistent);
- Theft of assets and asset data (including disclosure by social engineering) that may be used to further compromise the asset base, including engineering laptops, engineering asset user account credentials, engineering documentation. (Unsuccessful attempts should be recorded locally for audit purposes and only notified if they are repeated or persistent).

What does not constitute an electronic or cyber Incident:

- Random hardware failure of asset;
- Design flaw or design error (failure of intention to implement the correct design);
- Installation or manufacturing flaw or error (failure of intention to install or build the correct design).

The Modes of Attack

Cyber systems used on UK railways may be subject to unauthorised access through various means:

- Remotely, via the internet, or open non-secure telecom networks.
- At close hand through direct contact with infrastructure (e.g. through a USB port).
- Locally, through unauthorised access to physical infrastructure, or insider threat (infiltration).

The Vulnerabilities

- Use of unauthorised devices
- Use of unauthorised software
- Unsecured configurations for hardware and software
- Lack of vulnerability assessment and remediation
- Lack of malware controls, or controls that are poor quality or obsolete
- Poor control of application software security
- Poor control of wireless devices.
- Poor data recovery capability.
- Lack of skilled employees.
- Unsecured configurations for network devices.
- Ineffective limitation and control of network ports, protocols, and services.
- Poor control of administrative privileges.
- Poor boundary defence.
- Poor maintenance, monitoring, and analysis of security audit logs.
- Poor access control.
- Insufficient account monitoring and control.
- Inability to effectively prevent data loss.
- Insufficient incident response capability.
- Unsecure secure network engineering.
- Lack of security system testing.

Investigating persons should look for one or more of the following:

- Coincidence with another security breach, perhaps physical
- Records indicating the connection of an unauthorised media or data storage device
- Instructions issued from unexpected sources internally
- Instructions issued from unknown or suspicious sources externally
- Abnormal, illogical or otherwise obviously suspicious instructions being issued from any source.
- Recently imported data
- Recent activation of unknown software or script
- Unauthorised disabling of firewalls, or security software
- Unauthorised deletion or alteration of data
- Drops in light levels in fibre-optic cables

4. Security of light rail carriages and vehicles

Rolling stock design

4.1 Even before new vehicles are introduced to your network, you can be designing in security considerations. DfT has recommendations on incorporating security into rolling-stock design. For further information contact landsecurity@dft.gsi.gov.uk

Searches and checks

4.2 There are a number of common sense searches and checks that can be conducted on vehicles. Operators should visually check inside their vehicle at the start and end of a route before the next journey to ensure that nothing has been concealed or left behind. Checks should include underneath seats and any storage areas, e.g. for pushchairs, bags etc. within the carriage. Drivers or other crew should ensure any overhead luggage shelves are also included in a vehicle check. These basic visual checks should only take a few minutes to complete. Examples of existing good practice include the issue of crib / prompt cards to staff on security awareness and what to do if an unattended item is found – you may wish to consider introducing something similar for your own operation.

Image: Undertaking the security search © First Group

4.3 Should staff find an unattended item, whether as part of a security check or during the course of their duties, it is important that they know what to do. One example for doing this is to apply the ‘‘HOT’’ protocol (at Annex C). This has been designed by the BTP to assist rail staff in determining

whether an item or bag found is a genuine item of lost property or if it is something more suspicious. HOT has proved effective in minimising delays caused by unattended items and by identifying those which may represent an immediate hazard.

4.4 Almost all property that is left on the network is lost property, and it is important to have arrangements in place to return lost property to its owners. However some items may be malicious and it is important that these are dealt with correctly to protect your staff and your customers.

4.5 Whilst it is a useful tool, HOT may not be suitable for all environments – particularly where there is no active security presence, CCTV, search regime etc. (see Section 5 on Security at light rail stations, termini and interchanges). It is important that you have discussions with your police force to establish a system to enable unattended items to be reported and dealt with appropriately by your staff. Further advice is available from the BTP.

Securing vehicles and carriages not in service

4.6 Drivers should ensure that doors are closed when carriages are left unattended (e.g. at the start and end of a journey, during a comfort break or whilst parked at termini, depots or stations). This is to protect against someone entering the vehicle and potentially leaving an item on board, or engaging in other forms of criminal activity such as theft or vandalism. Where possible, doors should be locked and, if appropriate, windows secured.

Control of passengers boarding and leaving

4.7 At the end of a route, where a security check is carried out, passengers should not be permitted to board until it is completed.

Baggage reconciliation

4.8 It is recommended that you develop appropriate procedures that minimise the risk of someone placing an item of luggage on the vehicle without boarding, or of a disembarking passenger leaving baggage behind (See Section 1 for further details).

4.9 Reconciling passengers and their luggage is important because it:

- Acts as a deterrent to potential terrorists seeking to plant a bomb;
- Special attention should be paid to any luggage that appears suspicious, or is handled in such a way as to raise suspicions;
- Reassures passengers that you, the operator, have appropriate security measures in place; and
- Minimises potential for items of baggage to be left behind and associated delays this can cause.

Security awareness measures for passengers

4.10 Passengers can help act as your eyes and ears, and awareness messages are useful in promoting vigilance and providing reassurance. You could display security posters in your vehicle to remind passengers not to leave bags unattended and on what to do if they find any unattended or suspect packages or are concerned about suspicious behaviour, e.g. by reporting to a member of staff or a police officer. Where vehicles are fitted with electronic messaging or TV screens, these can be used too. If practical, voice announcements can be made from time to time on public address systems, where fitted. You should establish clear procedures and points of contact to deal with passenger reports.

High visibility clothing

4.11 The public are reassured by seeing your staff. This is particularly the case at times of heightened security (as indicated by the DfT, or by the National Threat Level, available from the Security Services website[7]). Those planning or who are intent upon criminal activity, may also be deterred by a clear staff presence on your network. You should consider whether your on board staff (drivers, revenue collectors etc.) should wear high visibility clothing during these times. This adds to their visual deterrent and identifies them as a point to report suspicious behaviour and items to. However, the legitimacy of wearers of high visibility, or branded company clothing, should not be automatically assumed. Staff should be encouraged to challenge anybody they do not recognise posing as staff, for instance if somebody is not wearing a pass in a non-public area, and / or is acting suspiciously.

On board Closed Circuit Television (CCTV)

4.12 CCTV has a useful deterrent value, and can be a valuable source of evidence for use in the detection and investigation of crime. The Surveillance Camera Code of Practice[8] issued under S30 of the Protection of Freedoms Act 2012 contains guidance on the overt use of CCTV in public places in England and Wales. The purpose of the code is to ensure that individuals and wider communities have confidence that surveillance cameras are deployed to protect and support them, rather than spy on them. It sets out 12 guiding principles which are intended to ensure the use of CCTV is necessary, proportionate, transparent, and effective in meeting a stated purpose and meets all legal requirements. In general terms, local authorities and the police are specified as relevant authorities who must have regard to the code when exercising any functions to which the code relates. Other CCTV system operators are encouraged to adopt the code on a voluntary basis. The Surveillance Camera Commissioner has been appointed to encourage compliance

[7] https://www.mi5.gov.uk/home/the-threats/terrorism/threat-levels.html

[8] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

with the code, review its operation and provide advice about it. That advice will include information about the relevant operational, technical, quality management and occupational competency standards which are available for a system operator. CCTV system operators can then consider these standards in determining how best to meet the purpose of their surveillance camera system whilst meeting legal obligations, making effective use of it, and safeguarding privacy considerations.

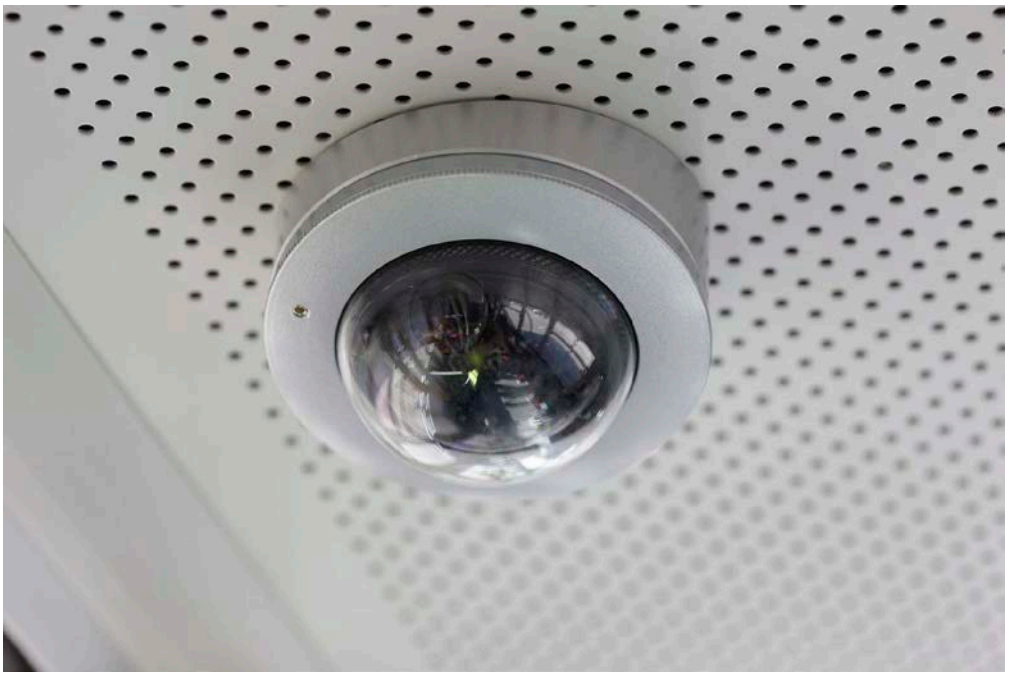

Image: On board CCTV © Metro

4.13 In the specific context of on board security, if CCTV has been fitted, at least one camera should provide identifiable quality images of everyone entering the vehicle, i.e. a clear image of the face plus characteristics of clothing, items carried etc. CCTV cameras positioned for identification purposes (i.e. for determining who is involved in an activity) should be able to produce an image size of not less than 100% standard definition screen height and ideally run at a minimum of 6 IPSPC (images per second per camera). Cameras positioned for recognition purposes (i.e. for determining what is happening) should be able to produce an image size of not less than 50% standard definition screen height and should record at a minimum of 2 IPSPC.

4.14 The system should be able to quickly export video and stills onto a removable storage medium, such as a CD or DVD, with the time and date integral to the relevant picture. Exported images should include any software needed to view or replay the pictures or be able to be replayed on a standard computer system with no additional software.

4.15 We recommend that if possible, recordings be retained for a maximum of minimum of 31 days, unless the evidence is being used in further proceedings, before recording media are reused, and made available to police on request. A log should be maintained to provide an audit should recordings be required by the police or other law and order agency.

4.16 As with any technological system, things can go wrong and it is essential that good maintenance arrangements are in place so that any faults can be repaired as quickly as possible. If current CCTV systems are to be replaced, digital systems are recommended. The Home Office has published comprehensive guidance for organisations who wish to install or upgrade CCTV systems, in its CCTV Operational Requirements Manual 2009[9], which concentrates on how best to determine your requirements and ensure that the system you use meets these as closely as possible. Information can also be found on the CPNI website[10].

Security enhancements at times of increased threat

4.17 There are a number of simple, common-sense security enhancement measures which can be employed at times of increased threat:

- Increase frequency of checks on rolling stock;
- Tighten controls on passengers boarding and any luggage reconciliation;
- Increase frequency of passenger security announcements / display security posters; and
- Deploy revenue control officers / other staff to travel on network, wearing high-visibility jackets / tabards.

4.18 Enhanced security may attract public attention. The measures employed should therefore be consistent with the threat and implemented in such a way as to reassure passengers and not to arouse anxiety. (This observation also relates to the use of awareness posters).

[9] http://nactso-dev.co.uk/system/cms/files/127/files/original/28_09_CCTV_OR_Manual2835.pdf
[10] http://www.cpni.gov.uk/advice/Physical-security/CCTV/

5. Security of light rail stations, termini and interchanges

5.1 Stations, termini and interchanges can be crowded places, making them a potential terrorist target. (Consult the NaCTSO website for guidance on protecting crowded places[11]). A range of simple measures can help to create the feeling of a controlled environment; this helps as a deterrent for hostile actors and provides reassurance to customers:

Key actions:

- Contact your police force to obtain free and independent advice on protecting your premises against terrorists and criminals;
- Remind passengers not to leave bags unattended and advise how to report unattended / suspect packages or suspicious behaviour to staff;
- Fit locks / tamper proof seals to cupboards / equipment boxes in public areas;
- Review the area and see what "clutter" you can do without;
- Review your litter management arrangements;
- Access control to non-public areas; and
- Encourage a "challenge culture".

Security in Design of Stations (SIDOS) and Hostile Vehicle Mitigation (HVM)

Protection of passengers and staff who use the rail and underground networks is a priority for government and rail operators. Incorporating physical security measures into stations is one method of mitigating the risk of a terrorist attack and other crime. Incorporating such measures at an early stage in the design of a new or major redevelopment of a station has benefits both in terms of their effectiveness and of minimising costs, and can take account of the needs of the travelling public better. In August 2012, the Department for Transport published its Security in Design of Stations (SIDOS) Guidance[12]. This includes detail of possible Hostile Vehicle Mitigation (HVM) measures which can be employed.

[11] http://www.nactso.gov.uk/crowded-places
[12] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/4345/sidos-guide.pdf

Image: HVM measures at St Pancras Station © Crown Copyright

The Safer Tram Stop Award

5.2 Those involved in the design of stations, termini and interchanges are encouraged to refer to the Safer Tram Stop (STS) Award[13]. Whilst the scheme is largely designed around crime and safety, it has clear benefits for counter terrorist security (sight lines, CCTV, lighting etc.) Speak to your police force for further details.

Searches and checks

5.3 Regular patrols by uniformed staff are a good deterrent, help to reassure passengers, and can be key to finding unattended or concealed items, detecting suspicious behaviour or checking doors are locked to prevent public access to non-public areas. Whilst dedicated and regular security patrols are the ideal, resources may not necessarily permit this.

5.4 Security checks can be shared by a number of staff and incorporated into their duties – for example by those monitoring areas as part of their customer service and safety duties, by cleaners as part of their routine cleaning duties and by ticketing or sales staff in ticket halls or concourse areas. Staff are familiar with their work environment, so are well placed to spot anything out of the ordinary. Checks need not be carried out during the times a station is not accessible to the public or is not open for service, but should be carried out on opening. We recommend that you keep records of these. They need not be overly detailed, but may provide critical information when reviewing incidents that have occurred, particularly when backed up by CCTV.

5.5 We recommend that you involve managers of other organisations (tenancies etc.) occupying premises or carrying out business at the station to ensure all parts of the station security check area are properly

[13] http://securedbydesign.com/professionals/guides.aspx

covered and that effective lines of communication are established. These groups should be included in all security planning, exercising and awareness presentations.

5.6 If properly planned in advance, a security check need not be too time consuming. The key considerations for you and your staff when conducting a check of public areas are:

- **Define the area** - Staff designated to undertake a check should be sufficiently briefed and aware of what is required. Asking someone to "check the station" is not sufficiently detailed: a start / finish point and boundaries need to be established;
- **Plans** - The process can be simplified if laminated plans of areas to be checked are produced. The plans do not need to be particularly detailed but should highlight key features of the areas (such as toilets, emergency exits etc.) to be covered;
- **Thoroughness** - Checks need to be sufficiently thorough in order to be able to detect any concealed item. Staff should pay particular attention to areas that are not in clear public view: low roofs, emergency exits, lavatories etc. Other vulnerable areas include litter receptacles and work sites. There should not be sole reliance on visual checks - doors should be physically checked to ensure they have been properly secured. Any areas beyond doors that are found to be unlocked should be checked before they are secured. It is not considered necessary to lift drains or the covers to other utilities, unscrew access panels or search areas into which unauthorised access is not possible; and
- **Sealing** - Any locations (stores) not in regular use should be secured under lock and key. When this is not possible (for safety reasons etc.), tamper evident seals are a good option. This will eliminate the need to check inside such boxes or cupboards unless the seal is no longer intact.

5.7 In summary, security checks should concentrate on areas of public space – especially those not in clear public view as terrorists do not want their bombs or their actions to be noticed. All checks should be made regularly and if possible recorded.

5.8 Should an unattended item be found, whether as part of a security patrol or during the course of staff carrying out their duties, it is important that there are established procedures to follow. One such example is to apply the HOT protocol (Annex C).

Construction work at a station

5.9 During construction work operators should:

- Consider how they intend to control access to site;
- Ensure ID passes are issued to all contractors and visitors and an audit kept of issue and return;

- Make sure that all works staff receive a security awareness briefing; and
- Consider if and how works affect existing security arrangements and procedures.

Links to other public transport systems

5.10 At locations where light rail systems interface with other transport networks such as heavy rail, underground or bus, operators should jointly discuss what security measures are appropriate, consulting other stakeholders including the police, the local authority, tenants etc. Larger railway stations should already have a station security committee comprising the key stakeholders involved in ensuring an effective security regime; light rail operators should join these. Where light rail stops and termini fall within a regulated rail station[14], the security regime adopted for light rail will usually be equivalent. We will be reviewing the security arrangements at interchanges over 2014-2015 as part of our wider review of the Railway Instructions and National Railway Security Programme. Responsibility for complying with the security regime at interchanges lies with the owner or operator of the relevant asset. If you are in any doubt as to whether or not any of your light rail stations will be affected by this, please contact the DfT for clarification.

Image: Nottingham Tram & Bus © Nottingham City Council

[14] The definition of “station” in Section 83(1) of the Railways Act 1993: "any land or other property which consists of premises used as, or for the purposes of, or otherwise in connection with, a railway passenger station or railway passenger terminal (including any approaches, forecourt, cycle store or car park), whether or not the land or other property is, or the premises are, also used for other purposes".

Key actions:

- Where a light rail station interfaces with a regulated heavy rail and / or underground interchange, jointly discuss what security measures are appropriate with other stakeholders, as a matter of best practice.
- Be involved in the station security committee, in order to understand and contribute to the security arrangements in place.
- Where a light rail station falls within a heavy rail / underground station, the security regime adopted for light rail will usually be equivalent to that of the heavy rail station. If you are in doubt, contact the DfT.

Control of access to public / non-public areas

Non-public areas

5.11 Members of the public should not be able to gain access to non-public areas such as staff rest rooms, store rooms and cleaners cupboards. All doors in public areas leading into non-public areas should be kept locked or controlled to prevent unauthorised access. This can help to minimise areas that need to be searched and patrolled. Ideally, keys for doors should be kept in a secure location controlled by a responsible person and a record kept of who has the key. If access is controlled by keypad, the code should only be given to persons with a legitimate need to know. We recommend that codes are changed regularly (on a frequency to be determined locally), depending on the number and turnover rate of staff with knowledge of the code. Keypad codes should be changed from the factory setting immediately on being installed. Securing your station will reduce the opportunity for criminal, as well as terrorist activity.

Vehicle access

5.12 It is important to be aware of the potential threat from Vehicle Borne Improvised Explosive Devices (VBIEDs). The movement of vehicles around and into stations and termini should be controlled where possible. Ideally, access to all vehicles should be prevented and distance should be provided between drop off points and the operational infrastructure, however where this is unavoidable (e.g. delivery to a retail outlet, access to staff parking areas) we recommend the use of access controls. Measures that can be introduced include:

- A parking permit system for staff and, where appropriate, for vehicles of visitors and contractors;
- Monitoring retail delivery vehicles to ensure that they do not stay on a station for longer than is necessary; and
- Pre-arranged deliveries only.

5.13 Ideally, these measures should be incorporated into stations from the initial design and build stage, using SIDOS guidance (refer to paragraph

5.2). Building HVM measures into new stations / refurbishments will often lead to the most effective and economical outcome.

5.14 It is also important that you consult local police to agree a system for reporting and dealing with any suspicious vehicles, and to liaise regarding evacuation plans.

Visitors and contractors

5.15 All visitors and contractors should be required to report to the station manager or other responsible person to notify their arrival at the station. It is good practice to require them to sign in a log book. This provides important audit information, including sign in/out times and the purpose of the visit, and can be crucial in the event of an emergency evacuation of the premises.

5.16 We recommend that you give visitors a security awareness briefing along the following lines:

- If the person is issued with a visitor pass, it should be displayed prominently at all times when they are on the premises;
- If the person has a vehicle parked on site, any work / parking permits should be displayed prominently in the windscreen;
- Be vigilant when around the premises. Should a suspicious item be found, do not touch it, but contact a member of staff as soon as possible. Similarly, if a person is seen to be acting suspiciously, contact a member of staff; and
- Ensure that all doors are properly closed/locked when you are leaving, particularly those doors that lead to non-public areas. Do not allow anyone to "tail-gate" into non-public areas. If you are leaving a work site, ensure that it is locked and all equipment has been securely stored.

High visibility clothing

5.17 Particularly at times of heightened security, the public are reassured by seeing your staff. This can be an active deterrent to those planning or who are intent upon criminal activity. As regards use of high visibility clothing, the same considerations apply as for staff working away from stations. You should consider whether your members of staff/contractors should wear high visibility clothing during these times. This adds to their visual deterrent and identifies them as a point to report suspicious behaviour and items to. At the same time however, it should not be assumed that wearers of high visibility, or branded company clothing, automatically have a right to be in non-public areas of a station. Staff should be encouraged to challenge anybody they do not recognise posing as staff in these areas or who is not wearing a pass etc.

Areas of concealment

5.18 Undoubtedly, some light rail stations were designed and built without consideration to security. As a result many contain voids and spaces which, if large enough, could be used by a terrorist to conceal an explosive device. In addition, any ‘‘dark corners’’, particularly those that are out of view of staff and members of the public, can be potential areas of concealment and can be a source of crime and anti-social behaviour.

5.19 Whilst it may not be possible to eliminate all areas of concealment some measures can be taken to reduce them. These include:

- Location of equipment - ask yourself if you are going to create a hiding space or if you can remove an existing one;
- Where possible, any grit bins, vending machines or other equipment boxes should be flush to walls so that nothing can be hidden behind or around any sides; tamper evident seals can be fitted to cupboards or equipment boxes that cannot be locked;
- Boarding or sealing up voids that cannot be removed e.g. under vending machines or around equipment boxes;
- Lighting - additional lighting can be installed to improve security and make security checks easier, particularly in any darker areas; and
- Conducting regular checks around the station.

5.20 Those involved in designing or refurbishing facilities at light rail stations (i.e. designers, architects and planners, as well as light rail station operators) can help ‘‘design in’’ security enhancing features from the outset. Clear lines of sight aid search and evacuation procedures. Curved tops on ticket machines, advertising panels and vending machines make it difficult for these to be used to place items on. Fitting them back to back with other machines, or on legs with large gaps underneath, can also make it difficult for someone to attempt to conceal an item without it looking obvious. Similarly, if planters are to be used on a station, they should be designed so as to make it impossible to hide anything underneath (i.e. no gap, or a gap so big that anything can be visible from all sides), and planting should not be so dense that it hinders searches.

5.21 Again, a useful reference tool when designing new major light rail stations, termini, and interchanges is the DfT’s SIDOS Guide (see paragraph 5.2). Whilst this guidance is intended for new major rail stations and rebuilds, it contains good security design principles that are more widely applicable. Other good sources of guidance available online are Integrated Security: A Public Realm Design Guide for Hostile Vehicle Mitigation[15] and Protecting Crowded Places: Design and Technical Issues[16] Of course, also be sure to contact your police force, who will be

[15] http://www.cpni.gov.uk/documents/publications/2011/2011001-integrated_security_v1.0.pdf?epslanguage=en-gb
[16] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97992/design-tech-issues.pdf

able to offer their specialist advice in helping you to design in appropriate and proportionate security measures from the outset of a new scheme.

Waste management

Litter Bins

5.22 Litter bins provide an easy and convenient method of concealment for a device and have been used by terrorists in the past. Certain types of receptacles, such as those made of metal, concrete or plastic, pose a greater risk as they can add to blast fragmentation, which can cause serious injury and structural damage.

5.23 The following bin design recommendations are based on regulated rail requirements but are equally valid here. Litter bins should be of a type that would not contribute to fragmentation if an Improvised Explosive Device (IED) were to explode inside it. A recommended design is a clear plastic sack that is unobstructed from view and suspended from a metal or plastic frame, so as to be easy to inspect visually and to remove if circumstances require. They should not have a lid, unless it is a plastic one, and hoops should be attached to concrete or brick walls, away from flammable structures, or to dug-in, stand-alone wooden posts. Consideration should be given to covering bins by CCTV so that the face of anyone placing an item in the bin would be seen.

5.24 We also recommend these ‘‘do’s and don’ts’’:

Do

- Check and empty bins regularly;
- Place bins near staffed positions (where possible) for deterrent value as well as to ensure that they do not become over-full; and
- Keep the number of bins to the lowest practicable level and monitor usage to identify those that are not really necessary

Don’t

- Allow litter bins to overflow (ideally they should be emptied when no more than half full); and
- Place litter bins near control rooms, evacuation routes, sources of possible fragmentation, such as overhead glass
- canopies, windows, mirrors etc., fire hydrants or electrical equipment

Bulk rubbish containers and compactors

5.25 Large bulk rubbish containers (including wheelie bins, compactors and skips) should be stored in secure non-public areas where possible. However, if they are to be stored in public areas such as in car parks or adjacent to entrances, they should be emptied and checked regularly, be capable of being locked and kept so, and covered by CCTV cameras.

Recycling facilities

5.26 Recycling facilities should not be located on or adjacent to well-populated areas (e.g. station concourse), next to station building walls or next to entrances or exits. Recycling facilities are not classified as bulk rubbish containers but, if placed within a station, should be subject to the same measures as litter receptacles.

Bicycles

5.27 There is a risk that explosive devices could be concealed in bicycles. Bicycle bombs are rare; and many examples have involved IEDs in panniers rather than concealed ‘invisibly’ within the frame tubes. The following recommended measures can be taken to reduce the risk of damage and injury.

Bicycle racks

5.28 Bicycle racks should be positioned with regard to the safety of passengers, staff and facilities, preferably away from crowded parts of the station such as platforms, waiting areas, entrances, concourses and large windows. If this is unavoidable, we suggest the racks be covered by CCTV surveillance. Derelict/abandoned bicycles should be removed once adequate notice of removal has been given.

Bicycle lockers

5.29 Bicycle lockers are increasingly being used to safeguard bicycles from theft. These bring associated risk, as an explosive device could be concealed inside a cycle locker. As with cycle racks, positioning can minimise the risk (see above for recommendations). In addition, we recommend that those using the lockers do not secure them with their own padlocks. Ideally, keys and padlocks for lockers should be controlled and issued by the facility operator, with spare keys retained securely to enable lockers to be checked by staff in the event of a security incident or alert.

5.30 Solid sided bicycle lockers may be used, although lockers with mesh sides or adequate vision ports (that provide good visibility of the interior during low light conditions) are preferable and can assist in checking.

Equipment boxes

5.31 It is recommended that all equipment boxes, such as sand and grit bins, fire extinguisher boxes, first aid equipment etc., are kept shut and secured to prevent anything being concealed inside. One of the best ways of doing this is with a tamper evident seal (e.g. plastic/wire seals, stickers) that can easily be broken in the event of an emergency. A broken seal can also highlight if a box has been tampered with.

Public toilet facilities

5.32 Terrorists have in the past used toilets for concealing explosive devices. When public toilets are checked at a station, particular attention should be paid to potential areas of concealment (such as exposed cisterns). Where old style cisterns are used, a tamper evident seal could be placed on to the cistern. If refurbishment of a public toilet facility is being considered, designs that reduce or eliminate areas of concealment are preferred. Your police force can advise.

Post boxes

5.33 Any post boxes located at a station should be kept locked or otherwise securely closed (apart from any opening used for the posting of mail), except when being emptied by a person authorised to collect the mail within it. The opening should be kept as small as possible to limit the size of items posted to letter format.

5.34 You should obtain advice from your police force if you intend to increase the number of post boxes at a station, particularly if you are considering installing post boxes that take items larger than normal letter/small packet size.

Tenants and cleaners

5.35 Tenants and cleaners have their part to play in overall security. We recommend that you have periodic meetings with them (and indeed with all operators at the station) at which security issues can be discussed. Tenants and cleaners should be made aware of the importance of vigilance and given details of incident reporting procedures (who to report to, what to report etc.). Tenants should also be aware of the need to secure any stock rooms and, where appropriate, monitor and supervise any delivery vehicles. Cleaners should also ensure that they lock cleaning cupboards when not in use and do not leave any cleaning equipment unattended. The importance of adhering to the security regimes in place on the premises should be emphasised – such as the wearing of passes, signing-in procedures etc.

Security awareness measures for passengers

5.36 You should remind passengers not to leave bags unattended and to report any unattended or suspect packages or suspicious behaviour to a member of staff or police officer. You may also wish to produce notices such as 'keep your belongings with you at all times', avoiding any messages which would cause undue alarm or panic. Security messages can be displayed on posters and information screens, and they can be delivered by regular announcements on a public address system during the times that the station is open. Staff should be trained to deal with reports from members of the public and should reassure the person that their concern or information will be taken seriously.

Closed Circuit Television (CCTV)

5.37 CCTV has deterrent value and can be used to cover parts of stations or facilities on stations that terrorists could exploit, such as litter bins, cycle racks/lockers and doors to non-public areas. CCTV also has a mutual benefit in terms of crime reduction (in both recording crimes taking place, and tracing perpetrators, to discouraging criminal activity in the first place). Please refer to Section 4 for further information on appropriate standards for CCTV systems, and Annex F for a list of recommended CCTV publications to consult.

Image: CCTV Control Room Copyright © Centro

5.38 You may wish to consider liaising with other local organisations/ operations (e.g. rail stations, local authorities etc.) to identify whether it would be useful to have compatible systems or whether their CCTV surveillance covers any part of your operation to avoid duplication. It may be possible to agree the positioning of several systems to ensure that there are no potential gaps in coverage.

Left luggage facilities

5.39 Left luggage facilities present an obvious security risk. Where possible Left luggage facilities should be located away from the main concourse or areas of large crowd density. In particular, left luggage lockers are of concern, as there is no control of persons depositing bags or items. Where left luggage lockers are installed we recommend that they are covered by CCTV. Staff should have a means of accessing the lockers –

or enabling the police to do so – to check their contents – for example, in circumstances of a bomb threat. This is also relevant to any other lockers, for example customer collection lockers, at a location.

5.40 We recommend that luggage or other property (other than lost property) be accepted on the condition that the person depositing the luggage or property agrees that it may be searched and/or screened. A record should be kept of the left luggage searched/ screened.

5.41 We recommend that screening be carried out by hand searching items of luggage and their contents, or using x-ray equipment that conforms to DfT standards, if it is available. A Standard Test Piece (available from x-ray machine manufacturers) determines whether an x-ray machine meets these standards in terms of image quality and will help to ensure that performance is maintained. Where it is used, x-ray equipment should be checked regularly to ensure that it is operating correctly and be maintained in accordance with manufacturer's recommendations. Further advice on testing of x-ray equipment is available on request from the DfT Land Transport Security team at landsecurity@dft.gsi.gov.uk

5.42 Left luggage facility operators should encourage their staff to pay particular attention to any bags that appear to be suspicious or are handled in such a way as to raise suspicions. Where a customer refuses permission to search/screen items, staff should not accept these and should notify police immediately.

Car parks / park and ride facilities / car rental facilities

5.43 We recommend that public car parks, park and ride facilities and car rental facilities are monitored to ensure that vehicles near to buildings are not left longer than an authorised time. If public parking is available, e.g. near station entrances or other passenger facilities, a procedure for dealing with suspicious vehicles should be agreed with your police force. Car parks should be included within any security patrolling regime.

Commercial developments at stations

5.44 A number of commercial developments have been seen or are proposed at a stations across the UK. This can range from internet shopping delivery boxes, phone charge lockers, reverse vending machines, flower dispensers etc. Whilst providing a useful service, these developments can have unintended consequences for the security of the station, by importing additional risk, e.g. concealment of an IED. If you are considering such developments at your stations, mitigating controls should be factored in. Location is key and ideally the development should be located away from crowded parts of the station. Station staff and police should also be able to access the interior (e.g. to search it in the event of a bomb threat) and there should be the ability to suspend use of the development at times of heightened threat. Operators should consult their CTSA about each proposed location / development before installation, and DfT can also offer advice.

Security enhancements at times of increased threat

5.45 There are a number of security enhancement measures which can be employed at times of increased threat:

Security enhancements - at times of increased threat

- Carry out more frequent and more thorough security checks of the public areas in a station;
- Remove litter bins or check them more frequently;
- Close bicycle parking facilities within the station area or require panniers to be removed before bicycles are left;
- Introduce/increase frequency of passenger security announcements/display posters;
- All staff on duty in public areas to wear hi-vis jackets or tabards;
- Withdraw luggage or other lockers from use or increase amount of screening of left luggage; and
- Deliveries are to be by prior appointment only. Details of supplier, vehicle and driver to be checked and recorded on arrival.

6. Security of depots and maintenance facilities

6.1 Although depots and maintenance garages are not crowded places in the same way as stations are, application of common sense security measures can help ensure that items are not concealed on board vehicles when in these locations. As with stations and termini, we recommend having clear signage in place to discourage unwanted access by vehicles / people and to facilitate proper egress in an emergency.

Key actions

- Contact your police force to obtain advice on protecting your premises

Physical protection

6.2 In providing physical protection, barriers around the site (fencing, walls, gates etc.) are recommended to control access and objects that could be used as climbing or screening aids e.g. trees should be removed. Reducing the number of access points into depots may lessen vulnerability to unauthorised access. Consideration should be given to permanently sealing (e.g. replacing with fencing) any redundant or unnecessary access points.

6.3 The main entrance should be the only point through which visitors and their vehicles can access a site. Alternative access points should be protected by appropriate physical measures to prevent unauthorised persons gaining access e.g. by tailgating.

Control room security

6.4 Where a control room is critical to the operation of a system, it is recommended that additional physical protection be given to it such as CCTV, exterior fencing and physical protection of the entrance. Careful consideration should be given to who has access rights to this area. It is recommended that a record of those staff who have unescorted access rights be kept, based on a legitimate operational need to access that area. Other staff, contractors and visitors should be allowed access only where they are expected and have been authorised or, preferably, where they are accompanied by a member of staff who has these rights. A

visitor record should also be kept. Further advice on Control room design can be obtained from the CPNI website[17].

Rolling stock on site

6.5 It is recommended that measures are introduced to protect rolling stock within the site if practicable (locking whenever the stock is not being worked on, searching before they leave the depot etc.) Section 4 of this guide covers the security of rolling stock, and gives more detailed information. Such vehicle checks may be done by drivers or by cleaners and a record made of the checks.

Closed Circuit Television (CCTV)

6.6 We recommend measures are introduced to aid the detection of unauthorised persons: either through the use of a monitored CCTV system (at a minimum covering all access points) which could be based on motion detection where activity is not expected, or another equivalent surveillance system, or the use of security patrols. Further information on CCTV can be found in Section 4, and useful CCTV publications are listed at Annex F.

Staffing / patrolling

6.7 We recommend that the main entrance should be controlled. Security guards and regular patrols of the depot compound are options for consideration. Systems for recording site patrols are also recommended.

Image: BTP Police bike patrol alongside Metro lines © Nexus

[17] http://www.cpni.gov.uk/

Passes: recording and issuing

6.8 A system of security passes or identity documents provides a useful control on legitimate access to the depot. Such measures will support the safe and secure movement of staff, contractors and authorised visitors around the site, as well providing a systematic check on vehicles through access points and into the depot.

6.9 We therefore recommend a pass system for staff, visitors and vehicles that need to enter non-public areas of depots. In the case of staff or contractors, their operational need to enter the site should be checked before any pass is issued. For others, the legitimacy of the visit should be checked and verified by a permanent and appropriately responsible staff member where possible.

6.10 Staff and contractors should be provided with passes. Full passes are preferred with photos and an automated or visual means of checking validity e.g. expiry date. These should be checked, either electronically or physically scrutinised, before access is gained to the depot. Passes should be clearly displayed by the pass holder at all times whilst in a depot area. Awareness briefings for staff should encourage them to challenge someone not wearing a pass, and/or who is unfamiliar to them.

6.11 Appropriate arrangements should be in place for receiving visitors into non-public areas. It is recommended that guards should check that the visitors are expected and have a legitimate reason to enter the depot. If this is the case then it is good practice to require them to sign in on arrival and produce appropriate evidence of identity (e.g. work request, driving licence, employer's letter) before issuing them with a pass. Ideally they should be escorted at all times in the depot area. At a minimum they should be required to display their pass at all times and surrender it when they leave.

6.12 Systems should also be in place to record the details of those issued with passes and to ensure they are surrendered when no longer needed (along with any keys, access cards, uniforms etc.) It is recommended that a record be retained of all passes issued to staff, contractors, visitors, and to persons entering the controlled area(s). For staff passes and others where the period of validity is over a day, this should include the date of issue and of expiry of the pass.

Motor vehicle access and parking arrangements

6.13 A similar checking/verification and pass issuing regime can be applied to motor vehicles. Where these belong to staff it can provide an additional safeguard to have a specific 'Staff Vehicle Pass'. All vehicles should display their vehicle passes while they are within a depot.

6.14 Attention should also be given to delivery vehicles. Providing the security guard with an "expected deliveries list" on a daily basis would enable them to verify the legitimacy of the delivery. If it is not expected then the guard should not allow it to enter until a member of staff has confirmed it is required. However, also be suspicious of 'regular' delivery vehicles; don't just waive them through without checking.

6.15 At heightened security levels you should consider implementing a random search regime. Guidance on a search regime for vehicles is included at Annex G.

6.16 For car parking within a depot, you might consider

- Adopting a colour coded parking permit system to distinguish staff, contractor, and visitor vehicles;
- Designating sections of the car park into spaces for staff and visitors. Spaces for visiting vehicles should be situated furthest away from the depot buildings (and the control room in particular);
- Carrying out checks on parking spaces to ensure no vehicles are parked illegally (and a system be put in place to have any such vehicles removed where possible, NOT clamped); and
- Agreeing a system with the police for the reporting of and dealing with any suspicious vehicles.

Security awareness measures

6.17 It is recommended that contractors and visitors are given a security awareness briefing to include, as appropriate the following messages:

- Visitors passes should be worn at all times when in the depot, and an audit kept of their issue and return
- Vehicle/parking permits should be displayed prominently in the windscreen
- The need for vigilance when around the depot. Should you find a suspicious item, please do not touch it, but contact a member of staff as soon as possible
- Similarly, should you see a person acting suspiciously contact a member of staff; and
- Please ensure that you close/lock all doors behind you when leaving, particularly those doors which lead to non-public areas. If you are leaving a work site, please ensure that it is locked and all equipment has been securely stored.

6.18 It is also sensible to provide periodic reminders to depot staff about the importance of good security measures. This could be included in operational briefings. Posters for notice boards can also be used.

6.19 Encourage staff to challenge anybody they do not recognise in the depot area, or who is not wearing an appropriate pass. It should not be assumed that wearers of high visibility, or branded company clothing, automatically have a right to be in non-public areas of a depot or sidings.

Security controls

6.20 All sites where rolling stock is stabled when not in service should be subject to minimum security controls. This can include:

- Physical access barriers around the site such as walls and fences;
- Access control measures at all entrances to prevent unauthorised access;
- Measures to protect rolling stock within the site (securing train/tram doors, regular patrols, or CCTV cameras to detect and monitor any unauthorised access); and
- Systems for recording site patrols, monitoring and checking of visitors and vehicles should be established. Identification passes should be worn at all times.

Control room security

6.21 Where a control room is critical to the operation of a system, it is recommended that additional physical protection be given to it such as CCTV, exterior fencing and physical protection of the entrance. Careful consideration should be given to who has access rights to this area. It is recommended that a record of those staff who have unescorted access rights be kept, based on a legitimate operational need to access that area. Other staff, contractors and visitors should be allowed access only where they are expected and have been authorised or, preferably, where they are accompanied by a member of staff who has these rights. A visitor record should also be kept.

Security enhancements at times of increased threat

6.22 At times of heightened security, consideration should also be given to:

- Closing access points other than the main entrance and thereby channelling all staff access via a main gate (other than staff on board trains as part of their duties);
- Keeping vehicle gates shut and only opening them to allow legitimate access into and out of the depot, so as to give added protection to the entrance; and
- Searching vehicles before permitting them access. Annex G outlines the main areas to be covered by a search.
- Carrying out more frequent and more thorough security checks of the facility;
- Requiring all visitors to report to the facility manager, or other responsible person, on arrival;
- Securing rolling stock when not subject to maintenance work;
- Escorting all visitors whilst they are on site;

- Deliveries to be by prior appointment only;
- Details of supplier, vehicle and driver to be checked and recorded on arrival; and
- Increasing efforts to ensure identification passes are worn at all times

Annex A - Bomb / Threat Report Form

Threat Report Form

To be completed by/with the assistance of the information recipient.
To be forwarded immediately to the supervisor
To be retained for 12 months

Please record all calls if possible: Is this call recorded: YES/NO

Is the threat conveyed by email, social media, etc? If so, ensure it is not deleted and available for police.

For spoken threats - i.e., by telephone or face-to-face

Message: exact words

(continue on extra sheet if necessary)

WHERE is the bomb/threat?

	Company	Location	Details (e.g. vehicle number, route, destination)
Vehicle			
Stop			
Station			
Terminus			
Other			

Did the caller seem familiar with the location described? Why?

If it is a bomb WHEN will it explode?

If moved	After departure	In transit	If opened
Date:	Time:	Day:	Other:

WHAT does it look like?

WHO are you?						
Name or individual: Person's location:	Name of organisation: Other:					
WHY are you doing this?						
Characteristics of the threat-maker (if applicable); Please circle as appropriate						
Sex:	Male/Female					
Age:	Child	Teen	Young Adult	Middle Aged	Old	Unknown
Language spoken:						
Command of Language:	Excellent		Good	Fair	Poor	
Voice characteristics:	Loud Rasping		Soft Pleasant	High pitched Intoxicated	Deep Other	
Speech:	Fast Stutter Other:	Slow Nasal	Clear Articulate	Slurred Hesitant		
Accent:	Scottish London Other:	Irish Geordie	Welsh Birmingham Foreign (specify):	Liverpool West Country		
Manner:	Calm Irrational Deliberate Laughing Concerned		Angry Coherent Emotional Obscene Other:	Rational Incoherent Righteous		
If a telephone threat: Background noise-	Transport (cars trains aircraft public announcements) Domestic (kitchen television/radio music) Workplace (office machines factory) Animals Other voices Other:					
Telephone warning: background details						
Mobile Phone	Payphone	Private Phone	Internal Call	External Call		

Where automatic caller ID available, record number shown:				
Number dialled by caller: Person usually on that number:				
Other details: e.g.	What? Where found? Where stored?	Written note	Text message	e-mails
Recipient's details (must be filled in)				
Name: Phone number: Threat received at: Time: Form passed to Supervisor (name): Signature		Position: Date:		

A completed copy of the form should be sent to the DfT Threats Office at the following address:

Threats, Risk & Intelligence Branch
Department for Transport
2/24 Great Minster House
33 Horseferry Road
London
SW1P 4DR

Telephone: +44 (0) 207 944 2870
Email: TICB@dft.gsi.gov.uk

Annex B - Marauding Active Shooter guidance

B.1 The attacks in Mumbai in November 2008 involved a co-ordinated shooting, bombing and hostage taking spree across the city by a group of 10 terrorists. The terrorists spread out, targeting a number of locations, including a railway terminus, hotels and cafes. A similar armed attack took place at the Westgate shopping mall in Nairobi in September 2013. We have also seen the effects a lone gunman can have in the attacks by Anders Breivik in Norway in July 2011.

B.2 This guidance is intended to complement existing guidance provided on other – more familiar – forms of terrorist attack, by addressing the scenario which emerged in the Mumbai and Nairobi attacks. This document also covers other types of firearms incidents where a gunman is active against multiple targets. This style of attack is potentially attractive to any crowded area, so vigilance by managers and staff everywhere is important.

B.3 We are not asking light rail organisations or staff to put themselves in the line of fire, indeed the opposite. The overall message to staff is DO NOT PUT YOURSELF AT RISK. It explains how staff and managers can help keep themselves and passengers safe, whilst assisting the authorities in dealing with the situation as swiftly and effectively as possible.

B.4 In briefing staff, or responding to staff concerns, you may like to explain:

"This guidance is not being provided in response to any specific intelligence but the current UK threat level is SUBSTANTIAL[18], meaning a terrorist attack is "a strong possibility". Having seen the new style of attack in Mumbai and Nairobi, and more events in the UK and Norway, it is sensible that we consider the scenario, in the same way that we do with other potential (and more familiar) terrorist threats to the transport system.

B.5 An incident of this nature could happen anywhere, particularly if it is a crowded place. A transport system is only one of many possibilities if such an attack were to happen.

B.6 The key message is that staying safe and not putting yourself at risk is paramount. By being aware of the sorts of issues that an attack in this form raises, it will help you know the best things to do in the unlikely event of this happening here".

B.7 Police forces in England, Scotland, Wales and Northern Ireland have been training officers using the "Stay Safe" package in relation to

[18] https://www.mi5.gov.uk/home/the-threats/terrorism/threat-levels.html

firearms attacks and are providing the following advice to the business community utilising the principles of that package:

In the event of an attack consider these actions:

Stay Safe

- **Under immediate GUN FIRE** – Take cover initially but leave the area as soon as possible - if safe to do so, e.g. (if the shooters are no longer a threat to you or others in your vicinity).
- **Nearby GUN FIRE** - Leave the area immediately, if possible and it is safe to do so.
- **Evacuation** – Beware of location and direction of threat and evacuate away from danger. Assist others in evacuating if safe to do so.
- **Leave your personal belongings behind** – Do not delay your evacuation but if possible take a means of communication (i.e. Mobile phone) with you to facilitate the giving/receiving of further safety advice.
- **Do not congregate** or allow the public to congregate at evacuation points or usual Rendezvous points. Dispersal away from the danger area is vital. However try to maintain contact with your supervisor so they are aware of your safety and location.

COVER FROM GUN FIRE (Examples)	COVER FROM VIEW (Examples)
Substantial brickwork or concrete	Internal partition walls
Engine blocks of motor vehicles	Car doors
Base of large live trees	Wooden fences
Earth banks/hills/mounds	Curtains

REMEMBER – Cover from view does not necessarily mean out of danger, especially if you are not in ‘cover from gun fire.’

IF YOU CAN’T ESCAPE - consider locking yourself and others in a room. Barricade the door then stay away from it. If possible choose a room where escape or further movement is possible. Silence any sources of noise, such as mobile phones, that may give away your presence.

See

Pass as much information to the **Police** as possible. Consider using **CCTV** and other remote methods where able. **NEVER** risk your **own safety** or that of others to gain it.

If it is safe to do so, think about the following:

- Type of firearm, long barrelled or handgun
- Exact location of the incident
- Is it automatic fire or single shot?

- Moving in any particular direction?
- Number and description of gunmen
- What else are they carrying?
- Are they communicating with others?
- Number of casualties / people in the area

Tell

Do not assume that others have already contacted Police. Therefore contact **POLICE** immediately by dialling 999 or via your control room, giving them the information shown under '**See**'. Using this information the Police will take the necessary action to ensure where possible trains are stopped entering the affected station.

Use all **forms of communication** available to you – to inform staff, public, neighbouring premises etc of the danger.

Act

Carry out the following actions **if safe to do so**.

Secure your immediate environment and other vulnerable areas

Keep people out of public areas

Move away from the door and remain quiet until told otherwise by **Emergency Services** or if you need to move for safety reasons

Armed Police

In the event of an attack involving firearms a Police Officer's priority is to protect and save lives.

Please remember:

Initially they may not be able to distinguish you from the gunmen.

Officers may be armed and may point guns at you.

They may have to treat the public firmly.

Follow their instructions; keep hands in the air / in view.

Avoid quick movement towards the officers and pointing, screaming or shouting.

Plan

Consider the following when planning for an Active Shooter firearms incident

1. How you would communicate with staff, public, neighbouring premises, etc.
2. What key messages would you give to them in order to keep them safe?
3. Have the ability to secure key parts of the building to hinder free movement of the gunmen.
4. Does your location store NHS Medical Bags for use by paramedics to treat casualties of such an incident? Do your staff know the location of these bags?
5. Think about incorporating this into your emergency planning and briefings
6. Test your plan.

If you require further information then please liaise with your immediate Supervisor, who can take further advice from your local CTSA.

Annex C - Suspicious items - using the HOT protocol

C.1 A suspicious item is one that exhibits unusual characteristics (appearance or placement) and for which a legitimate purpose cannot readily be established.

C.2 To avoid unnecessary disruption of the network and alarm to customers, staff should first try to identify the owner of any unattended item. If no owner can be identified, they should then apply 'HOT'. This helps staff to decide quickly whether an unattended item is typical of lost property or whether it is suspicious. It is designed with staff and customer safety in mind as well as minimising disruption to the network and wider society.

C.3 The HOT protocol has been used in the rail environment since the early 1990s and is reviewed regularly. It is based on research undertaken by BTP that indicates unattended suspicious items are typically:

Hidden - i.e. placed where they will not be readily seen or noticed as unusual

Obviously suspicious (e.g. by physical appearance, by placement, or because of the circumstances in which they have been discovered)

Not **T**ypical of what you would normally expect to find in that environment

C.4 Lost property items are typically:

Not **H**idden - often left where people congregate before moving to do something else

Not **O**bviously suspicious - they do not usually exhibit improvised wiring, timers, putty-like substances etc.

Typical of what you would normally expect to find in that environment - a judgement made best by staff with an intimate knowledge of the area in question

C.5 It is difficult to define comprehensively how items might appear "obviously suspicious" from their appearance. However, from experience, a suspicious item may display one or more of the following features:

a. external wiring;
b. visible batteries;
c. switches;
d. timers;
e. circuit boards;
f. wire passing from one package to another;
g. items secured by plastic adhesive tape;
h. annotations (e.g., ‘ON’, ‘ARMED’, ‘DET’, reference to the time delay);
i. specially modified wooden or plastic boxes;
j. unidentified powders or other putty-like substances; or
k. carefully wrapped in plastic bags.

C.6 While the HOT protocol provides a useful starting point, it is not prescriptive. It is ultimately up to staff to use their judgement to decide whether an unattended item is suspicious or not.

C.7 Staff should seek immediate advice from their supervisor if they are unsure about whether an item is suspicious or not. If your supervisor deems the item suspicious, they should contact the police. At this stage, people should be moved away from the immediate vicinity.

C.8 If the police officer cannot clear the item as safe, then the situation will be elevated, through the deployment of specialised resources who are trained to deal with suspect packages.

C.9 Note: If the item is believed from the outset to pose an immediate threat to life, police advice will be to move people at least 100m away and to stay behind hard cover (brick or concrete).A larger area may have to be evacuated if the item is particularly large or associated with a vehicle.

Annex D - Quick reference security checklist

ITEM	REMARKS	ACTION REQUIRED
INTRODUCTION (Section 1)		
1.1 Do you have copies of the Passenger Rail Security DVD available?		
1.2 Do you use wider sources of security advice? E.g. Crime reduction / prevention officers, CTSAs.		
ORGANISATIONAL SECURITY CULTURE (Section 2)		
2.1 Does your organisation encourage staff to respect common values and standards towards security?		
2.2 Does your organisation have ongoing effective personnel security measures in place?		
2.3 Are staff undertaking security related duties/tasks appropriately briefed/trained?		
2.4 Does your organisation have contingency plans to deal with major incidents? Are these tested and practised?		
HANDLING THREATS AND INCIDENTS (Section 3)		
3.1 Do you have a process in place for handling, reporting and recording bomb threats, and are you/your staff familiar with it?		
3.2 Do you have a formal process of assessment for establishing whether an item is unattended or suspicious? (e.g. the 'HOT' protocol)		

3.3 Are your staff aware of the BTP "Marauding Active Shooter" guidance?		
SECURITY OF LIGHT RAIL CARRIAGES AND VEHICLES (Section 4)		
4.1 Is the vehicle checked at end of route/turnaround?		
4.2 Do you have a process for evaluating and dealing with suspicious items/behaviour?		
4.3 Are the doors/windows secured when the vehicle is left out of service?		
4.4 Are passengers being prevented from boarding when vehicle not in service or driver not present?		
4.6 Is there a process in place for dealing with luggage that appears suspicious or is handled suspiciously?		
4.7 Are there on-board passenger security announcements/information displayed?		
4.8 Have you considered guidance in the surveillance camera code of practice where any CCTV has been fitted on board?		
4.9 Is the retention period for CCTV data proportionate to the stated purpose of the system?		
4.10 Are there processes, procedures and training of system users that enable the CCTV to deliver images and information that is of evidential value to the police and the criminal justice system?		
4.11Is there as much transparency as possible over the use of CCTV?		
4.12 What arrangements are in place for the regular review of the CCTV system?		
SECURITY AT LIGHT RAIL STATIONS, TERMINI AND INTERCHANGES (Section 5)		
Areas of concealment		
5.1 Are all possible small concealed/hidden from view areas removed or reduced?		

5.2 Are they checked frequently?		
5.3 Are security features designed into station/termini/stops?		
Access control		
5.4 Are all doors to non-public areas locked or subject to access control?		
5.5 Are keys/access codes kept in a secure place?		
5.6 Are access codes changed regularly?		
5.7 Is the movement of vehicles (other than your rolling stock) controlled?		
5.8 Is there a process in place for dealing with illegally parked or suspicious vehicles?		
5.9 Are visitors/contractors required to report to the station manager or other responsible person to sign in and provided with an ID pass?		
5.10 Are visitors given a security briefing?		
5.11 Are there procedures in place for reporting suspicious behaviour?		
Patrolling public areas		
5.12 Is there a plan in place for regular patrols of public areas?		
5.13 Are patrols/search regimes changed regularly so that they cannot be monitored/learnt by those undertaking hostile reconnaissance?		
5.14 Is there a record of patrols?		
5.15 Are seals on locked doors checked?		
5.16 Is there a process in place for evaluating and dealing with suspicious items?		
Waste Management		
5.17 Are litter bins of an IED resistant or clear plastic sack design?		

5.18 Are litter bins emptied frequently?		
5.19 Is CCTV monitoring of litter bins necessary?		
5.20 Are large bulk waste containers stored in secure non-public areas?		
5.21 If not stored away from public areas, are large bulk waste containers kept locked, emptied regularly and CCTV monitored?		
Bicycles		
5.22 Are bicycle racks/lockers positioned away from crowded areas? Is CCTV monitoring necessary?		
5.23 Are keys to lockers controlled and can staff access spare keys?		
Equipment boxes		
5.24 Are equipment boxes kept shut and secured?		
Public toilet facilities		
5.25 Are public toilets included in searches?		
Post boxes		
5.26 Are post boxes kept closed when not being emptied?		
Tenants and Cleaners		
5.27 Do you have regular security meetings with tenants and cleaners?		
5.28 Are your tenants/cleaners security briefed?		
Passenger Security Awareness measures		
5.29 Are there passenger security announcements, or information displayed?		
CCTV		

5.30 Is CCTV fitted and monitored where necessary, and have you considered guidance in the surveillance camera code of practice where any CCTV has been fitted on board?		
5.31 Is the retention period for CCTV data proportionate to the stated purpose of the system?		
5.32 Are all sensitive areas covered by CCTV cameras?		
5.33 Is there a robust maintenance system in place with arrangements for the regular review of the CCTV system?		
5.34 Is there as much transparency as possible over the use of CCTV?		
5.35 What arrangements are in place for the regular review of the CCTV system?		
Left luggage		
5.36 Are bags searched/screened before being stored?		
5.37 Do you have a process in place for reporting suspicious persons/bags?		
Car Parks		
5.38 Are public car parks monitored and is there a procedure for dealing with suspicious vehicles?		
SECURITY OF DEPOTS AND MAINTENANCE FACILITIES (Section 6)		
6.1 Is the site perimeter secured with fencing/walls to keep intruders out?		
6.2 Are access control measures in place at all site entrances to prevent unauthorised access?		
6.3 Are CCTV cameras in place and monitoring/recording sensitive areas of the site?		
6.4 Are vehicles on site secured when not in use/undergoing maintenance work?		

6.5 Are vehicles searched before leaving the depot to enter service and again on returning, and is there a search recording system in place?		

Annex E - General online resources

CPNI: Protecting against terrorism: 3rd edition (2010)

http://www.cpni.gov.uk/documents/publications/2010/2010002-protecting_against_terrorism_3rd_edition.pdf

CPNI: Guidance on personnel security

http://www.cpni.gov.uk/advice/Personnel-security1

CPNI: Further guidance on CCTV

http://www.cpni.gov.uk/advice/Physical-security/CCTV/

CPNI: Integrated Security: A Public Realm Design Guide for Hostile Vehicle Mitigation

http://www.cpni.gov.uk/documents/publications/2011/2011001-integrated_security_v1.0.pdf?epslanguage=en-gb

Department for Transport, British Transport Police & Centre for the Protection of National Infrastructure (2012) Security in Design of Stations (SIDOS)

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/4345/sidos-guide.pdf

Home Office, Centre for the Protection of National Infrastructure & National Counter Terrorism Security Office (2012) Protecting Crowded Places: Design and Technical Issues

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97992/design-tech-issues.pdf

MI5: Terrorist Threat Level to the United Kingdom

https://www.mi5.gov.uk/home/the-threats/terrorism/threat-levels.html

National Counter Terrorism Security Office (NaCTSO) Guidance on crowded places, with links to several publications

http://www.nactso.gov.uk/crowded-places

Secured by Design (with link to the Safer Tram Award)

http://securedbydesign.com/professionals/guides.aspx

Annex F - Closed Circuit Television (CCTV) specific publications

The Home Office Centre for Applied Science and Technology publish a number of documents covering CCTV.

We would recommend that all of them are followed.

These are the most relevant:

Cohen, Gattuso & MacLennan-Brown (2009) CCTV Operational Requirements Manual, version 5, (publication number 28-09)

Cohen & MacLennan-Brown (2007) Digital Imaging Procedure, version 2.1, (publication number 58-07)

Walker (2005) UK Police Requirements for Digital CCTV Systems, (publication number 09-05)

Home Office Centre for Applied Science and Technology publications can also be accessed at:

http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/cctv-imaging-technology/CCTV-and-imaging-publications.html

The Home Office have also published a Surveillance Camera Code of Practice, (June 2013):

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

Annex G - Vehicle search routine for entry to depots

G.1 For those vehicles selected for search this should consist of a selection of at least one of the following five areas of the vehicle:

Area 1 - front door pockets, sun visors and glove box;

Area 2 - rear of front seats (map pockets), under seats and foot wells;

Area 3 - boot/luggage/cargo area;

Area 4 - wheel arches; and

Area 5 - under the bonnet.

G.2 These areas should be checked visually to a standard sufficient to reasonably ensure that no prohibited articles are contained in the area or areas searched.

G.3 A record should be kept of the vehicles searched and those areas searched. It should also record details of any prohibited articles found.

Annex H - Glossary of terms

Active Shooter Scenario/Marauding Active Shooter
An attack using firearms, involving either a group or a lone shooter. (While the emphasis is on firearms it should not be assumed that attackers will not have access to knives and/or IEDs).

Bicycle/Cycle Locker
An enclosed structure provided for the storage of bicycles (whether singly or in bulk).

Bicycle/Cycle Rack
Device for the storage of bicycles that is of open construction and any bicycle placed in the rack is clearly visible.

Bomb Threat
A communication, anonymous or otherwise, which threatens people or property. This could involve an explosive hazard, or chemical, biological or radiological substances.

BTP
British Transport Police

Bulk Rubbish Container
A large, rigid container (including wheelie bins and skips) for storing and disposing of bagged and bulky waste items.

CCTV
Closed Circuit Television

CDM
The Construction (Design & Management) Regulations 2007

CPNI
The Centre for the Protection of National Infrastructure is the Government authority that provides security advice to businesses and organisations across the national infrastructure.

CTSA
Police Counter Terrorism Security Advisor. CTSAs offer provide advice and guidance on all aspects of counter terrorism protective security to operators, with BTP CTSAs able to offer you advice specifically tailored to the railway environment.

Device
This relates to threat items of improvised or military origin. It covers explosive (high-explosive and incendiary), chemical, biological and radiological, threats.

DfT
Department for Transport

DOCO
Police Designing Out Crime Officer

Hoax
A benign item, material or received threat placed maliciously in such a way as to cause concern on the part of the finder / recipient. The term 'hoax' covers a range of scenarios, from overtly benign items placed in such a way as to attract staff / police interest (e.g., an empty cardboard box), to elaborate mechanisms designed to represent viable hazardous devices or materials.

HOT protocol
Procedure devised by BTP and promoted by NaCTSO to assist in determining whether an unattended item is lost property or something more suspicious

HVM
Hostile Vehicle Mitigation

IED
Improvised Explosive Device

Left Luggage
Any item deposited by a member of the public at a storage facility provided at a station (whether or not it is provided by the owner or operator).

Lost property
Items misplaced during travel

MAS
Marauding Active Shooter

NaCTSO
Police National Counter Terrorism Security Office

Non-public area
Area of a station to which the public do not generally have access or to which they do not normally have access in the absence of supervision by a member of staff. Only members of staff or those contracted to provide services to light rail vehicles/trams, stations, buildings or machinery would ordinarily be expected to need access to those areas.

Operator
In relation to a light rail station, this means the person having the management of that station. This may be for a fixed period as part of a contractual service agreement.

Owner
In relation to a light rail station, means any person:
(a) Who is the owner of, or who has any right over or interest in, the station; and
(b) Whose consent is needed to use the station by any other person

PBIED
Person-borne Improvised Explosive Device

Security Awareness Message
Message that makes the travelling public and those in the vicinity aware of and vigilant towards potential security threats affecting vehicles or stations.

Security Incident
Any incident of a security nature where:

a. the police are called and:

   (i) a full or partial evacuation of a station/vehicle is required before the incident is resolved; or

   (ii) the initial police responders are unable to resolve the incident and call on further specialist assistance, such as Explosive Ordnance Disposal Officers, to resolve the incident; or

   (iii) the incident is resolved, but remains the subject of further police investigation; or

b. police confirm the incident as an attempted or actual attack; or

c. any security related incident which attracts media interest, even if it would not be one requiring notification in line with 1 to 3 above; and

d. any discovery of firearms, ammunition, or other weapons; and

e. any incidents of unauthorised access, or attempted unauthorised access, to non-public areas; and

f. bomb threats; and

g. any discovery of explosive devices, component parts of explosive devices, or articles having the appearance of such.

Security Staff
In relation to any station means a member of staff who is engaged to provide security services to that station.

SOP
Standard Operating Procedure

Station
Means any light rail/tram station, terminus or interchange.

Suspicious Item
An item assessed as exhibiting unusual characteristics (particularly in terms of appearance or placement) and for which ownership or other legitimate purpose cannot be established readily.

Suspicious Behaviour
Any behaviour that would be perceived by a reasonably prudent individual as of a kind that ought to be investigated by a person with security responsibilities.

Threat Level
The level of threat the UK faces from terrorism at any given time.

Training Plan
A written document developed and maintained by an operator which describes the type of security training that should be undertaken to ensure staff are aware of their security responsibilities and how to respond appropriately.

Unattended Item
An item for which an owner cannot be identified readily but is, in other respects, typical of the environment within which it is located. Unattended items do not usually require a police response. However, police officers may be called when either: (a) the HOT protocol has not been applied, (b) the protocol has been applied incorrectly or (c) other doubts remain but where the item is not believed to pose an immediate threat to life.

VBIED
Vehicle-borne Improvised Explosive Device

White Powders
A 'white powder incident' is a phrase applied to the discovery of a substance (solid or liquid) where the finder suspects the presence of a chemical or biological hazard. Not all such hazards are white, or powders, and can usually be discounted quickly if subject to a rational evaluation.