UK ROADS LIAISON GROUP

Guidance for Local Highway Authorities: a security-minded approach to [Counter Terrorist] Security

1. Introduction and Background

This guidance aims to provide support and advice for highway authorities to develop a [counter-terrorist (CT)] security strategy[1], and has been developed in response to the London attacks on Westminster and London bridges. This is not new guidance but endeavours to provide signposting to existing resources, enabling highway authorities to develop their own security systems and culture. These systems help to support staff and supply chains to deliver security by adopting and embedding a security-minded approach. When new infrastructure is put in place, or existing infrastructure is upgraded or renewed, security issues should be considered from project inception; this document provides links to useful guidance on the approach that should be adopted.

By adopting such an approach, highway authorities will be contributing to the mitigation of the risk from terrorist attack and will be able to demonstrate that they have done so. Most of this guidance is publicly available from the relevant authorities including the Centre for the Protection of National Infrastructure (CPNI) website, who are the UK's National Technical Authority for physical and people security. Your local territorial police force also has specially trained Counter Terrorist Security Advisors (CTSA) who can provide more bespoke advice. Advice can also be obtained from private-sector consultants who should be members of the Register of Security Engineers & Specialists (RSES)[2] or Chartered Security Professionals (CSyP)[3]. It is essential that the consultants have specialist knowledge in the areas that you need.

The local highway network is among the most valuable infrastructure for which local authorities are responsible. Highway assets include not just the facilities, systems, and networks in and around highways, but also the processes and even the essential workers that operate, facilitate, and maintain them, including the data and information about them and how they are used. These assets have also become, over time, more interconnected and dependent on information and communication technologies. Intrusions and deliberate disruptions in one part of infrastructure can lead to unexpected failures in others, and therefore understanding and handling interdependencies are key issues. The loss or compromise of any one of these aspects of infrastructure could detrimentally impact on the availability, integrity, or delivery of essential highways services. Where such compromise takes place, it can leave parts of the highway network, and the areas adjoining it, open to adverse events such as vandalism or terrorism.

The increase in the availability of information technologies, and the diminishing costs associated with them and the storage of data, is facilitating the ease with which highway assets can both interact with other assets and provide essential data streams of their own. This can support the efficient management of traffic flow and mobility, as well as increasing the safety of the road user. Adopting CPNI Open and Shared Data: Adopting a Security-Minded Approach[4] and PAS 1192-5 will help to avoid your data being exploited by those with hostile or malicious intent. Further advice on Cyber Security can be obtained from the National Cyber Security Centre (NCSC)[5], the UK National Technical authority for cyber security.

Furthermore, many of the UK's important assets are in heavily populated urban environments, where some streets have high volumes of pedestrian traffic. Crowded spaces can become

[1] https://www.cpni.gov.uk/developing-security-strategy
[2] https://www.rses.org.uk/
[3] https://www.charteredsecurityprofessional.org/
[4] https://www.cpni.gov.uk/open-data
[5] https://www.ncsc.gov.uk/

attractive as potential sites of terrorist attack including from vehicles used as weapons and other low sophistication attacks against people on the roadside as witnessed at Westminster Bridge and at London Bridge.

It is important to follow a holistic approach to overall security (both the **physical** environment[6] and the **digitally engineered/connected** one). Such an approach will both consider different threat types on their own and acknowledge and respond to the interdependence of physical measures with electronic and procedural security measures to ensure that overall security is enhanced.

This guidance document provides information to encourage local highway authorities to adopt a security-minded approach in relation to their assets, including their information, to deter and disrupt hostile, malicious, fraudulent, and criminal behaviours and activities. It should be read in conjunction with best practice principles included within the Transport Asset Management Guidance[7] **document**.

2. Culture & Governance

Culture is about encouraging behaviours or installing internal mechanisms/procedures to embed a security-minded approach within your organisation; there are two broad steps for this:

1) Governance - an important step to achieving a security culture is to have a senior level official responsible for security; and,

2) Providing training and support to staff to help deliver a security-minded culture.

Governance is important for security: this means the need to '*identify who is accountable for security at the highest board/executive level*' – either a designated point of contact or a virtual security 'team' of people throughout the organisation. A board level executive should be appointed as Senior Risk Owner for Security, who has corporate responsibility for security and ensuring that there is a clear security governance process within the organisation in order to ensure that risks are owned, managed and reviewed regularly.

Visible senior leadership will promote positive security behaviours and help ensure security processes and procedures are adopted throughout the business. This will establish a security culture throughout the business. Further guidance can be found on CPNI's website[8]. The CPNI Passport to Good Security for Senior Executives[9] sets out the key themes for top down best practice and provides relevant prompts for the actions you need to take as part of your strategy. It will help authorities to identify, assess, and mitigate the threats to their organisation[10].

Highway authorities should also **develop an appropriate security strategy[11]**.This strategy should be embedded in the organisation; CPNI's 5E's approach[12] is a recommended approach to delivery. Ensuring that all front-line staff are trained in being vigilant and understanding how to respond to unusual activity or items is essential for good security. Highway authorities should

[6] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/820082/170614_crowded-places-guidance_v1b.pdf
[7] http://www.ukroadsliaisongroup.org/en/UKRLG-and-boards/uk-roads-liaison-group/transport-asset-management-guidance.cfm
[8] https://www.cpni.gov.uk/leadership-security
[9] https://www.cpni.gov.uk/managing-my-asset/leadership-in-security/board-security-passport
[10] https://www.cpni.gov.uk/security-considerations-assessment
[11] https://www.cpni.gov.uk/developing-security-strategy
[12] https://www.cpni.gov.uk/system/files/documents/98/dc/Embedding-Security-Behaviours-Using-5Es.pdf

undertake training of their staff and those in their supply chain[13], for example, encouraging their parking enforcement officers, street cleaning, and refuse collection staff to remain vigilant[14] and immediately report, any suspicious looking activity, behaviour, or objects.

This training could involve putting all staff through the ACT Awareness e-Learning[15] developed by National Counter Terrorism Office (NaCTSO) and security experts which is now freely available. In addition to staff knowing what to look out for it is essential that issues are reported to the appropriate authorities and management must positively thank staff when issues are reported. Authorities may wish to develop their own triage process before items are reported to the police either locally or through National Counter Terrorism Policing mechanisms such as the ACT app. This app provides access to the latest messaging, advice and protective security documents created by Counter Terrorism Police. 999 should always be used in an emergency.

The value and effectiveness of security measures can be significantly enhanced by publicising their existence. This can be a deterrent to those seeking to cause harm, whilst simultaneously reassuring the public. For example, by publicising the installation or renewal of Hostile Vehicle Mitigation and other measures such as CCTV as part of enhancement to an area or urban realm, it would signal to those seeking to cause harm that those measures exist and may deter them from continuing with their plans.

While it is valuable to publicise that security measures are in place, a security-minded approach should be taken to all public information and communications. You should avoid publishing specific technical details (especially online) that could be useful for those carrying out research as part of an attack-planning process.

Training in how to adopt a security-minded communications approach can be arranged by your local Counter Terrorism Security Advisor (CTSA) as part of the See, Check and Notify (SCaN) training programme[16]. The free training is suitable for your communications professionals, subject matter experts and policy teams, and provides simple and easy to apply guidance to maximise safety and security and deny those with malicious intent the information they need to plan effectively.

3. Major schemes/maintenance renewals

Security-mindedness should inform both the design and maintenance of major highway works, e.g. integrating security for the public realm by considering security at project inception[17] or protecting more critical infrastructure (telecoms/gas/electricity) rather than leaving it accessible or vulnerable during the maintenance process. This is particularly important in crowded places and spaces; these can be regularly crowded places (e.g. a railway station[18] or shopping district) – where hostile vehicle mitigation (HVM) measures should be considered as appropriate during any refurbishment or new build project.

There are also temporary crowded places, where measures can be employed for a time limited period, or where socketed systems could be considered if the site is repeatedly temporarily protected. Further advice on security measures can always be obtained from your local CTSA. It

[13] https://act.campaign.gov.uk/
[14] https://www.cpni.gov.uk/employee-vigilance
[15] https://www.gov.uk/government/news/act-awareness-elearning
[16] https://www.gov.uk/government/news/security-training-package-empowers-staff-to-see-check-and-notify-scan
[17] https://www.cpni.gov.uk/system/files/documents/40/20/Integrated%20Security%20Guide.pdf
[18] https://www.gov.uk/government/publications/land-adjacent-to-railway-bus-and-coach-stations-security-reducing-vulnerabilities

is, of course, worth noting that not all security enhancements require major civil engineering, such as HVM and using CPNI's Operational Requirements[19] process, will help highway authorities identify and proportionally mitigate the risks.

Advice is also available on how to blend in physical features to prevent against vehicles being used as weapons (hostile vehicle mitigation (HVM))[20]. In considering appropriate physical security measures, the potential for negative impacts on the aesthetics of the public realm should be considered, for example using specially designed planters and artwork rather than a row of bollards. Other measures are available that provide protection while blending in with the surrounding architecture and streetscape, which will help retain a sense of place without compromising security.

Local authorities, along with their consultants and contractors, should consider the advice available as part of the design process[21]. Where work is being undertaken using building information modelling or other digital engineering processes, or concepts such as 'smart cities' and interconnectivity of assets are being considered, a security-minded approach should be taken in relation to the generation, processing, sharing and storage of information[22].

4. Developing an integrated security network

Highway authorities should consider their whole network in terms of security risks and seek security advice in doing this. Highway authorities can seek advice from their local police force counter-terrorism security advisors to ensure an awareness of the potential risks they face. A local authority should consider undertaking a Security Considerations Assessment (SCA)[23] to assess how well security is understood and embedded across its organisation as well as how it is considered in the work it undertakes across the assets it manages. As we have seen with vehicle as a weapon attacks in 2017, threats can shift (where the vehicle occupants caused further disruption whilst on foot). Highway authorities should give due regard to shifting attack methodologies[24] when considering their security posture and network.

Highway authorities should look for opportunities to work with partners to have a common approach to addressing security, for example by attending security meetings at major railway stations. There is useful guidance[25] that highway authorities would also benefit from on reducing security vulnerabilities at rail, bus, and coach stations[26].

It is more important than ever that your organisation is aware of the heightened risks and adequately prepared for any potential attack. With lockdown restriction easing, businesses everywhere will be getting ready to get back to work or increase their activity. As the threat has sadly not gone away, and socially distanced queues may lead to vulnerabilities in new places, it is important that highway authorities put security high on their agenda.

---

[19] https://www.cpni.gov.uk/system/files/documents/2c/cc/Operational_Requirements.pdf
[20] https://www.cpni.gov.uk/hostile-vehicle-mitigation
[21] https://www.gov.uk/government/publications/vehicle-security-barriers-within-the-streetscape
[22] https://www.cpni.gov.uk/digital-built-assets-and-environments
[23] https://www.cpni.gov.uk/security-considerations-assessment
[24] https://www.cpni.gov.uk/marauding-terrorist-attacks-0
[25] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875547/bus-and-coach-security-recommended-best-practice.pdf
[26] https://www.gov.uk/government/publications/land-adjacent-to-railway-bus-and-coach-stations-security-reducing-vulnerabilities