



Home Office

# Protect Duty Consultation

Making the public safer at publicly accessible locations

## Contents

Contents	2
About this consultation	3
Ministerial foreword	5
Introduction	7
An introduction to protective security for owners and operators of publicly accessible locations	9
Section 1: Who (or where) should legislation apply to?	12
Section 2: What should the requirements be?	17
Section 3: How should compliance work?	26
Section 4: How should government best support and work with partners?	29
Responding to this consultation	34
Glossary	36
Table 1: Glossary of terms used in the Protect Duty Consultation.	36
Annex 1 - Exemptions and exclusions	38
Annex 2 – Best practice examples of security considerations and mitigations at different organisations	39
Annex 3 - What types of cost and benefits are expected?	48
Annex 4 – List of consultation questions	50

## About this consultation

<p><b>To</b></p>	<p>This consultation is open to the public, and is targeted at venues, organisations, businesses, local and public authorities, and/or individuals who own or operate at publicly accessible locations or others that a ‘Protect Duty’ would potentially affect.</p> <p>A publicly accessible location is defined as any place to which the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission. Publicly accessible locations include a wide variety of everyday locations such as: sports stadiums; festivals and music venues; hotels; pubs; clubs; bars and casinos; high streets; retail stores; shopping centres and markets; schools and universities; medical centres and hospitals; places of worship; Government offices; job centres; transport hubs; parks; beaches; public squares and other open spaces. <b>This list is by no means exhaustive, but it does demonstrate the diverse nature of publicly accessible locations.</b></p> <p>We welcome responses from anyone with an interest in or experience of the areas being consulted on within this consultation.</p> <p>The consultation relates to the United Kingdom of Great Britain and Northern Ireland only.</p>
<p><b>Duration:</b></p>	<p>From 26 February 2021 to 2 July 2021</p>
<p><b>Enquiries (including requests for the paper in an alternative format) to:</b></p>	<p>Email: <a href="mailto:ProtectDuty@homeoffice.gov.uk">ProtectDuty@homeoffice.gov.uk</a></p> <p>Or</p> <p>Protect Duty Consultation Protect and Prepare 5th Floor NE, Peel Building, Office for Security and Counter Terrorism Home Office 2 Marsham Street, London, SW1P 4DF</p>
<p><b>How to respond:</b></p>	<p>There are four thematic sections in this consultation.</p> <p>Respondents can answer as many or as few questions as they wish. You do not have to comment on every section or respond to every question on each section but can focus on where you have relevant views and evidence to share. If you wish to respond to all questions, you do not have to complete the whole form at once.</p>

	<p>Please send your response by 2 July 2021</p> <p>Please respond to the questions in this consultation online at:  <a href="http://www.homeofficesurveys.homeoffice.gov.uk/s/1D4SQ3/">www.homeofficesurveys.homeoffice.gov.uk/s/1D4SQ3/</a></p> <p>Alternatively, you can send in electronic copies to:  <a href="mailto:ProtectDuty@homeoffice.gov.uk">ProtectDuty@homeoffice.gov.uk</a>; or,</p> <p>Alternatively, you may send paper copies to:  Protect Duty Consultation  Protect and Prepare  5th Floor NE, Peel Building,  Office for Security and Counter Terrorism  Home Office  2 Marsham Street,  London, SW1P 4DF</p>
<b>Additional ways to respond:</b>	<p>If you wish to submit other evidence, or a long-form response, please do so by sending it to the email address or postal address above.</p>
<b>Response paper:</b>	<p>A response to this consultation and a Regulatory Impact Assessment will be published online at:  <a href="http://www.gov.uk/government/consultations/protect-duty">www.gov.uk/government/consultations/protect-duty</a></p>

## Ministerial foreword

The first duty of the Government is to protect the public. The terrorist threat we currently face is multifaceted, diverse and continually evolving. The police, security services, and other partners do all they can to combat this threat: since March 2017 UK police and security services have foiled 27 plots, including eight motivated by Right Wing ideologies. However, despite their best endeavours, it will never be possible to stop every attack. The attacks we have seen in the UK, particularly since 2017, have caused deaths and casualties amongst people going about their everyday business, often in open, public places; and have changed the lives of many people.

The Government is committed to improving the safety and security of public venues, as outlined in its 2019 manifesto. This consultation considers how we can work together to develop proportionate security measures to improve public security. It also considers how those responsible for publicly accessible locations are ready and prepared to take appropriate action, were a terrorist attack to happen.

Importantly, we also hope that these proposals respect and acknowledge the important work of all those who have campaigned for legislation. In particular, I want to thank Figen Murray, whose son Martyn was killed in the Manchester Arena attack, for the significant contribution she has made through her tireless campaign to introduce 'Martyn's Law'. We look forward to working with them throughout the consultation period to help gather their views and encourage others to contribute too.

There is much good work already being done by many organisations, and I welcome these ongoing efforts. However, in the absence of a legislative requirement, there is no certainty that considerations of security are undertaken by those operating the wide variety of sites and places open to the public, or, where they are undertaken, what outcomes are achieved. This consultation considers how we could improve this position, through reasonable and not overly burdensome security measures.

The Government is extremely conscious of the severe impacts that COVID-19 has had, and continues to have, on many businesses and organisations. The thresholds for venues and organisations potentially in scope have been carefully chosen at this time to recognise this.

It is envisaged that for many organisations and venues, the requirements of a Protect Duty would entail minimal new costs. Many have already undertaken or are pursuing ongoing significant work to consider security measures, systems and processes, including through recent consideration of COVID-19 health measures and ensuring appropriate security requirements as part of these.

The proposed Protect Duty is only one part of the Government's approach to improving protective security and preparedness at publicly accessible locations. We continue to seek to engage and provide advice and guidance to all who operate at or have an interest in public security. We also continue to expand and enhance these resources, and, where possible, tailor them to the needs of different user groups. I would encourage all readers of this consultation to consider the simple advice and to access the further reference sources provided at pages 9-11, in the section entitled 'An introduction to protective security for

owners and operators of publicly accessible locations'. We remain committed to working with you to protect the public and save lives.

**RT HON JAMES BROKESHIRE MP  
SECURITY MINISTER**

## Introduction

This consultation considers how we might use legislation to enhance the protection of publicly accessible locations across the UK from terrorist attacks and ensure organisational preparedness.

With some exceptions (e.g. on transport security and for certain sports grounds), there is no legislative requirement to consider or implement security measures at publicly accessible locations. However, there are many reasonable and appropriate measures which can be - and often already are - undertaken by organisations who operate at such locations. These include:

- Having security plans and procedures to react and respond to different threats which are understood by all staff and regularly exercised;
- Having simple and freely available training and awareness courses in place as part of new staff and refresher training programmes; and
- Employing simple security measures (such as door locks, roller shutters) for crime prevention and anti-social behaviour, which may also be used in response to other security threats.

For many stakeholders potentially in scope, these are requirements they have already undertaken, or requiring low or nil new costs to take forward. We know that there is a willingness to do more from many businesses and others with public facing operations, and that many organisations operating at publicly accessible locations would welcome a mandatory requirement to consider and mitigate against threats to security.

We understand that there is often a low awareness of existing information and tools available, but when organisations have engaged, there is evidence that they go on to implement changes. The next section, 'An introduction to protective security for owners and operators of publicly accessible locations' provides some simple security advice and further reference sources that all can follow.

We are mindful of the impact a legislative change could have for some organisations. However, this must be carefully balanced against the need to ensure effective consideration of public security, and the implementation of reasonable security measures, in order to improve public security.

We recognise that effective security requires a partnership approach, with Government, police, the security services, the wider public sector, businesses, and the public all having a role to play. If a legislative Protect Duty were to be introduced, we recognise the need to enhance Government support for all organisations within its scope.

This consultation seeks views from all parties that a 'Protect Duty' would potentially affect - in particular, organisations who own locations or operate at publicly accessible locations. We seek views from across the United Kingdom, since national security is a reserved matter, however we recognise that developing an effective process and support to implement such legislation would draw on delivery mechanisms and responsibilities within the Devolved Administrations.

The responses to the consultation questions and additional research and analysis will be used to develop a Regulatory Impact Assessment which will be published in due course.

The proposals and discussion issues are broken down into the following sections:

**Section 1: Who (or where) should legislation apply to?**

**Section 2: What should the requirements be?**

**Section 3: How should compliance work?**

**Section 4: How should Government best support and work with partners?**

## An introduction to protective security for owners and operators of publicly accessible locations

Recent years have seen an increase in terrorist attacks in publicly accessible locations, i.e. locations that people visit, congregate in, or transit through. A defining feature of such attacks is the targeting of people, whether randomly, or as representatives of specific groups (e.g. relating to race, religious beliefs, etc).

Any publicly accessible location is a potential target, and it is therefore essential that the owners and operators of all such locations understand the risks they face and consider appropriate mitigations.

This section is intended to introduce protective security for owners and operators of publicly accessible locations – whether businesses, or other organisations operating in permanent premises or the organisers of temporary events, or those with wider interests in public security such as public authorities.

It is worth noting that improvements made to security from a counter-terrorism (CT) perspective are likely to have wider benefits, potentially reducing other crime and antisocial behaviour. Similarly, existing or new security measures implemented for other purposes can have a counter-terrorism benefit.

An important tenet of protective security is that it should, wherever possible, utilise simple, affordable interventions that protect and reassure the public and deter would-be attackers, with no (or minimal) adverse impact on the site's operation or people's experience. Whilst an extensive pallet of countermeasures is available, many of the more complex and costly ones – particularly specialist physical security products – will be more relevant to larger sites likely to host higher visitor footfalls and/or crowds.

It is important to consider **security as a system**, a combination of physical and/or behavioural interventions deployed in a complementary manner to mitigate key risks. Getting the “people” aspects right (e.g. developing and sustaining a security culture, encouraging vigilance, and providing appropriate and effective training) is at least as important as selecting (and correctly installing) physical security measures (such as security doors, blast-resistant glazing, fences, bollards, CCTV, electronic access control and intruder detection systems). Further advice and guidance is available on [the NaCTSO website](#) or from your local [Counter Terrorism Security Advisor \(CTSA\)](#). Where you believe, based on your risk assessment, that you may need such measures, you may also wish to seek independent expert advice (<https://www.cpni.gov.uk/cpni-working-security-professionals>). Even where appropriate measures are selected that appear to match a site's needs, ensuring they are installed and operated to provide effective capability (and properly complement other security measures) is crucial.

Key initial steps are **understanding threat and risk**:

- Understanding the terrorist threat – noting that terrorist groups, their motivations and target preferences and attack methodologies can differ and tend to change over time.
  - A useful level of awareness can be achieved by following open source media reporting of recent attacks and their methodologies, understanding

and monitoring the National Threat Level (<https://www.gov.uk/terrorism-national-emergency>), and browsing relevant government websites (e.g. <https://www.cpni.gov.uk/terrorism>).

- Understanding the specific risks the threat poses for your site and / or organisation - how and why your site / organisation might be affected, either by being targeted directly; or through indirect impacts, due to its location in a particular area or because of its proximity to neighbouring sites, businesses, or organisations that may be targeted.
  - You should undertake a risk assessment to identify and record terrorism risks and appropriate mitigations. This should be aligned with your organisation's / site's wider assessment of risks and their management.

In order to maximise their likelihood of success, terrorists are likely to undertake research and planning activity in preparation for an attack; this can include visiting potential target locations ("**hostile reconnaissance**"), as well as conducting research online.

Consider what you and your colleagues (whether employees, contractors or volunteers) can do to make it harder for a would-be terrorist to carry out a successful attack, for example by:

- Being alert to suspicious behaviours and activity in and around your site, such as people loitering or displaying an unusual level of interest in asking questions, or filming or photographing. Note that you and your staff are well placed to know what is "normal" in your environment, and hence what may be suspicious. Where it feels safe to do so, consider engaging the person in a welcoming and helpful manner; if you have any concerns, consider reporting them to the police. Similarly, you and your colleagues should be alert to abandoned bags and other left items, and report any you deem suspicious to the police.
- Being security-minded in your communications, particularly online. Wherever possible, include positive general messages demonstrating your commitment to ensuring the security and safety of visitors and staff. Avoid providing specific information that could help a terrorist plan an attack, for example floor plans containing more detail than is necessary to assist customers with planning their visit, or details of where and when security patrols do (and don't) take place.
- Encouraging and enabling a security culture in the workplace, for example ensuring that any concerns can easily be reported and will be acted upon and ensuring that managers lead by example and avoid giving mixed messages.

Consider how you and your staff would respond to an incident occurring outside or near to your building or site, or inside it. Remember that every second counts.

- How quickly would you become aware of what was going on?
- How would you respond?
- Would you and your staff be able to act quickly enough to move yourselves and visitors to safety?
- What can you do to prepare for such an eventuality?

**ACT Awareness e-Learning** (Action Counters Terrorism), has been developed by Counter Terrorism Policing to provide nationally recognised corporate CT guidance to help

people better understand, and mitigate against, current terrorist methodology. It is available to all organisations, their staff and the general public (<https://www.gov.uk/government/news/act-awareness-elearning>).

For many organisations, security arrangements will be enhanced by developing relationships with neighbouring businesses and organisations, for example working together to make the local environment harder for would-be terrorists to operate in, including enabling the rapid exchange of information on suspicious activity and potential incidents. It is also advisable to engage with your local CTSA and neighbourhood policing team.

Take care to ensure that any security measures / plans don't conflict with health and safety requirements and fire regulations.

Remember to **review and refresh** (where appropriate) your risk assessment, your plans and mitigations, including your staff's awareness of the threat and how to respond. Routine reviews should be undertaken regularly, with reviews also carried out if there are changes to the threat – either in terms of national threat level (indicating the likelihood of an attack) or as a result of incidents that demonstrate a shift in attack methodology.

### **Further information**

- Counter Terrorism Policing and its National Counter Terrorism Security Office (<https://www.gov.uk/government/organisations/national-counter-terrorism-security-office>)
- Centre for the Protection of National Infrastructure ([www.cpni.gov.uk](http://www.cpni.gov.uk))

## Section 1: Who (or where) should legislation apply to?

The proposed Protect Duty could apply in three main areas (but may also apply to other locations, parties and processes by exception):

1. Public venues (e.g. entertainment and sports venues, tourist attractions, shopping centres)
2. Large organisations (e.g. retail, or entertainment chains)
3. Public spaces (e.g. public parks, beaches, thoroughfares, bridges, town / city squares and pedestrianised areas)

Our proposals focus on legislative considerations of security being undertaken at certain publicly accessible locations (any place to which the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission), but not private venues, such as places of employment, or other locations where there is not public access.

We acknowledge that security considerations, whilst still important, must be proportionate to the threat of terrorist attack. We are also mindful of the huge impact that COVID-19 has had, and continues to have, on many organisations.

However, we want to emphasise that appropriate and proportionate considerations of security are important at all locations – including those out of scope of the proposed Duty – and we recommend that all organisations should consider the Government advice outlined at pages 9-11.

### 1. Proposal: The Duty should apply to owners and/or operators of publicly accessible venues with a capacity of 100 persons or more

We consider that the capacity of a venue is a clear and simple basis to define venues that should fall within scope of a potential Duty. Capacity is a criterion already commonly used in fire safety risk assessments. We consider that it is reasonable for publicly accessible venues able to hold gatherings of 100 persons or more to carry out an assessment of threats and implement appropriate mitigating measures at their premises. This threshold has been set, mindful of the impact that COVID-19 has had, and continues to have, on many organisations, particularly public-facing businesses. At a future date, and when appropriate to do so, we may seek to consult again on a lower threshold.

Responses will be carefully considered in determining if a capacity threshold is an appropriate criterion, and, if so, at what level it is set.

Using capacity as a criterion captures many public venues; permanent buildings or temporary event locations (such as outdoor festivals) where there is a defined boundary.

A Protect Duty requirement would apply to the parties responsible for the venue, which would usually be the owners or operators, who have control and ownership of systems and processes. Where there is a shared organisational responsibility for a venue within scope, the parties would be required to work together to ensure the Duty requirements were met.

## **2. Proposal: The Duty should apply to large organisations (employing 250 staff or more) that operate at publicly accessible locations**

In addition to public venues, there are many large organisations (employing 250 staff or more) which operate at publicly accessible locations, with staff who are responsible for taking forward a range of legislative and other requirements to be implemented across the organisation, through its systems and processes. There will usually be standardised training and ongoing continuous professional development for these specialist roles, as well as wider staff training and awareness programmes. Organisational structures will usually be in place to enable delivery of policy, operational processes, planning, and business and legislative requirements, usually commissioned on a top down basis, from a company headquarters or otherwise.

This could also include organisations with a number of outlets, below a 100 persons or more venue capacity, across a wide geographical (often national or UK wide) footprint, where there is significant and/or regular public footfall and public engagement, on a routine and often daily basis e.g. high street retailers, supermarkets, betting shops, newsagents, chemists, and petrol stations.

We consider that it is reasonable that a Protect Duty should apply to large organisations employing 250 people or more, operating at publicly accessible locations.

## **3. Proposal: A Protect Duty should be used to improve security considerations and outcomes at public spaces**

The diverse nature of threats and targeting means we cannot predict where or when an attack will take place. Many of the attacks that have been seen recently, in the UK and elsewhere, have occurred at public spaces. These are open public locations which usually have no clear boundaries or well-defined entrance / exit points (e.g. city centre squares, bridges or busy thoroughfares, parks, and beaches).

These locations are often vulnerable to low sophistication methodologies such as knife attacks or the use of a vehicle as a weapon. However, it is usually innocent members of the public who are the target, rather than the location itself. Whilst these types of attacks are difficult to combat, the Government wants to consider how it can do more to work with the parties responsible for such locations to consider and achieve appropriate security measures. This is an issue which was raised in both the Westminster and London Bridge Inquests, and the Manchester Inquiry.

We want to consider further the questions of how responsibilities for public spaces could be established, what would be reasonable and appropriate to expect those responsible for public spaces to do to improve security at such locations, and the potential role played by legislation in these issues. We recognise that these are complex issues to resolve, and we are keen to hear the views of the range of organisations having ownership or responsibility for such locations. We would like them to consider whether, and if so how, legislation could be helpful to provide greater clarity and certainty of the responsibilities and requirements of parties owning and/or operating at these types of locations, and what security considerations and mitigations could be undertaken by them to achieve greater public

protection. In particular, we would like to seek the views of landowners, local and public authorities, and others who might coordinate or lead work to help improve protective security and preparedness at public spaces.

#### 4. Other aspects of a Protect Duty

We also want to consider whether other locations, parties or processes should be included within the scope of a Protect Duty to ensure better public protection and organisational preparedness.

This includes considering the potential for the Duty to require:

- Partnership working with parties already complying with security legislation, for example to ensure effective co-ordination between transport sectors (where security legislation is already in force) and operators responsible for publicly accessible locations adjacent to transport hubs;
- Existing security guidance (e.g. for bus and coach operators) to be given legislative effect for certain locations or sectors; and
- Companies and other organisations responsible for holding, selling or hiring products that could be used by terrorists as a weapon in an attack at a publicly accessible location to adhere to security guidance.

#### Exemptions and exclusions

Some legislation, (currently limited in the scope of its application), already requires certain stakeholders and/or locations to consider terrorist threats and to take forward appropriate security measures to mitigate these (e.g. transport security regulations). Where this is the case, we propose that these stakeholders and locations would be exempt from a Protect Duty, as the effect already being achieved by these regulations is equivalent to the proposed Protect Duty requirements.

Annex 1 sets out examples of locations/stakeholders that we propose should be exempt from the Duty.

#### Questions

To what extent do you agree or disagree with the following statement:

1. Venues and organisations owning, operating or responsible for publicly accessible locations should take appropriate and proportionate measures to protect the public from attacks in these locations  
Strongly Disagree (SD) – Disagree (D) – Neither Agree nor Disagree (NAND) – Agree (A) – Strongly Agree (SA) [scale]

To what extent do you agree or disagree with the following statement:

2. Venues and organisations owning, operating or responsible for publicly accessible locations should prepare their staff to respond appropriately in the event of a terrorist attack to best protect themselves and any members of the public present

Strongly Disagree (SD) – Disagree (D) – Neither Agree nor Disagree (NAND) – Agree (A) – Strongly Agree (SA) [scale]

3. We propose that a targeted Protect Duty applies only to certain public venues. What criteria would best determine which venues a Duty should apply to ?
- Capacity (as currently used in Fire Safety Regulations)
  - Annual revenue
  - Staffing levels
  - Other: \_\_\_\_\_(Free text, 100 words max)

**[Where 3 is a]**

4. We have proposed a venue capacity of 100 persons or more as a threshold. What capacity level do you think would be appropriate to determine venues in scope of the Duty?  
\_\_\_\_\_ (Free text, 100 words max)

**[Where 3 is b-d]**

5. What threshold would you propose for inclusion in the scope of the Protect Duty for this criterion?  
\_\_\_\_\_ (Free text, 100 words max)
6. We propose that a requirement to consider security and implement appropriate mitigations at a venue should fall to the owner and/or operator of the venue. Do you consider this appropriate?  
Y/N

**[If 6 = N]**

7. If no, why not:  
\_\_\_\_\_ (Free text, 100 words max)
8. We propose that where there is a shared organisational responsibility for a venue, or multiple organisations operating at a venue within scope, the parties would have to work together to meet the requirements. Do you consider this is appropriate?  
Y/N

**[If 8 = N]**

9. If no, why not:  
\_\_\_\_\_ (Free text, 100 words max)
10. We propose that a Protect Duty would also apply to certain organisations operating at publicly accessible locations. If an organisation's size were a criterion for its inclusion in the scope of the Duty, what would be an appropriate threshold? [select all that apply]
- All organisations
  - Micro (1-9 employees)
  - Small (10-49 employees)
  - Medium (50-249 employees)
  - Large (250+ employees)
  - Other \_\_\_\_\_(Free text, 100 words max)

**[Linked to Question 10]**

11. What is your reasoning for this answer?  
\_\_\_\_\_ (Free text, 100 words max)

12. We have proposed a Protect Duty would apply to organisations with 250 or more employees. Is it clear as to whether your organisation falls within this criteria?  
Y/N

**[If 12 = N]**

13. If no, why not?  
\_\_\_\_\_ (Free text, 100 words max)

14. Are you clear about whether your organisation falls within the scope of the definition of a 'publicly accessible location' (a place to which the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission)?  
Y/N

**[If 14 is N]**

15. If no, why not?  
\_\_\_\_\_ (Free text, 100 words max)

16. Referring to Annex 1, do you consider that there should be other exemptions from a Protect Duty?  
Y/N

**[if 16 is Y]**

17. If so what or who and why?  
\_\_\_\_\_ (Free text, 200 words max)

18. Are there any other issues regarding who legislation should apply to that you would like to offer views on?  
\_\_\_\_\_ (Free text, 200 words max)

## Section 2: What should the requirements be?

This section is about **what** parties within the scope of a Protect Duty (see Section 1) should be required to do. Again, we would emphasise that we would encourage all organisations to consider the safety and security of their staff and the public who use their facilities.

In considering what should be required by a Protect Duty, we recognise that:

- The nature of venues and organisations varies greatly, for example in respect of the type of business or undertaking, organisational size, and staffing profile.
- Different venues and organisations have different security skills and resources at their disposal - from those with dedicated security staff, budgets, training and procedures, to those with little or none.
- Risk assessments and mitigation measures should be proportionate to the specific circumstances of the venue/organisation and its environment, as well as the nature of the terrorist threat at any given point in time.
- In the difficult financial climate that many venues and organisations find themselves in, in particular due to the impacts of COVID-19, low and nil cost security solutions are desirable and, in many cases, will be a proportionate response to the risk.

The aim of a Duty would be to ensure the consideration of threat, leading to considering and taking forward appropriate and proportionate mitigation measures. It is envisaged that for many organisations and venues, these requirements would be simple changes to existing systems and processes, entailing nil or low new costs. For many, these will reflect work which has already been undertaken, including recent considerations of COVID-19 health measures and ensuring appropriate security requirements through these.

### Venues and large organisations

For public venues and large organisations with the scope of a Protect Duty, we consider that the owners/operators should be required to:

- Use available information and guidance provided by the Government (including the police) to consider terrorist threats to the public and staff at locations they own or operate;
- Assess the potential impact of these risks across their functions and estate, and through their systems and processes; and
- Consider and take forward 'reasonably practicable' protective security and organisational preparedness measures (for example staff training and planning for how to react in the event of an attack).

The term 'reasonably practicable' is already a well-established and understood concept for organisations through health and safety legislation and fire safety regulations, which requires owners/operators to weigh a risk against the effort, time and money needed to mitigate it.

However, we recognise that applying this concept in a security context will be new for many venues and organisations within the proposed scope of the Duty, who will potentially have little experience of considering and mitigating terrorist threats.

The Government wants to ensure that requirements undertaken to comply with the proposed Duty, are reasonable and appropriate for organisations within scope - and proportionate to the nature of the threat. Supporting Government guidance would provide details of the range of appropriate measures for organisations within scope.

For most organisations in scope of a Protect Duty, we propose that compliance would be demonstrated by providing assurance that the threat and risk impacts had been considered, and appropriate mitigations had been considered and taken forward (implemented or plans in place for their progression). For organisations at the lower end of criteria thresholds, this would entail simple low – or no - cost preparedness measures such as ensuring that:

- Staff are trained and aware of the nature of threats, likely attack methodologies and how to respond;
- Staff are trained to identify the signs of hostile reconnaissance and take appropriate action; and
- There are plans in place for an organisation's response to different attack types, which are regularly trained and exercised.

Where proportionate security measures would entail more significant mitigation requirements, a reasonable time would be allowed to plan and progress measures within business planning processes and cycles. For example, more complex mitigations such as implementing measures for appropriate access control or reducing the risk of vehicle as a weapon attack will entail financial costs to plan, design and implement, and to train staff in their use. These are issues on which supporting guidance would provide further details.

To help those who may be within scope of the proposed Duty to understand what 'reasonably practicable' and 'appropriate' security measures will mean for them - including in terms of cost and resource implications - we have developed a number of indicative good practice examples for different types and sizes of organisations to demonstrate compliance (Annex 2). We will use the responses to this consultation and evidence gathered directly from stakeholders to develop and publish a Regulatory Impact Assessment.

Government would ensure that a range of resources are available to support organisations to comply with the Duty, including providing guidance on understanding threat methodologies, how to carry out risk assessments, and information and advice on the range of security measures available to mitigate risks identified. What is required to support organisations to discharge the Protect Duty is considered further at Section 4.

## Public spaces

This section considers the potential for specific requirements under a Protect Duty to improve security at open public spaces. Section 1 raised the issue of parties with an interest in the mitigation of attacks at public spaces, including landowners, local and some public authorities, and other organisations who are responsible for or who operate at such locations. There are already a range of ongoing efforts to provide security advice and guidance to these parties. This includes awareness raising and training courses, such as the Action Counters Terrorism (ACT) and See Check and Notify (SCaN) modules

delivered by Counter Terrorism Policing, which aim to improve organisational and individual awareness, planning and processes for what to do in the event of an attack.

We would like to understand what mechanisms are already being used to consider and mitigate terrorism threats, whether more could be achieved through them, and the potential for utilising them, or by establishing new requirements to discharge a Protect Duty at public spaces.

Many local, and other public authorities (such as Highways Agencies) are already fulfilling a range of functions within their jurisdictions to consider aspects of crime prevention, public safety, and security. These mechanisms<sup>1</sup> include:

- CONTEST and Protect Boards;
- Community Safety Partnerships;
- Licensing for sports grounds safety;
- Planning processes;
- Local Resilience Forums;
- Safety Advisory Groups (for events);
- Business Improvement Districts (which can be set up by Local Authorities, businesses or individuals to benefit local businesses);
- Licensing Committees (for the sale and supply of alcohol, the provision of late-night entertainment and refreshment); and
- Health and Safety, fire safety and building control processes.

We are aware of the limitations of these mechanisms in the context of the proposed Duty: most are not designed to achieve security outcomes; and some are not a legislative requirement, which means that they are able to mitigate threats to varying degrees, and it is hard to have assurance of the level of public protection which is achieved. This is not a criticism of authorities, merely a reflection of the current lack of a dedicated legislative security requirement.

In these and other areas, local and public authorities already play a vital role in convening interested parties from across their areas, to discuss issues of shared concern, and to work together to help resolve and mitigate risks, including criminal acts. From previous discussions with local authorities, we are aware that different authorities are using different mechanisms in different ways to consider security risks and implement appropriate mitigating measures. We would like to seek views on whether existing mechanisms (for example those listed above) could be used, or adapted, to bring about more effective security outcomes.

In addition, security outcomes could potentially be improved by organisations responsible for, or operating at public spaces, working with partners (e.g. police) to ensure there is a better understanding of:

- Threat;
- Attack methodologies;
- Processes by which organisations can assess and manage risk; and

---

<sup>1</sup> These mechanisms vary across the UK, and in many cases there are different comparable mechanisms in the Devolved Administrations of Northern Ireland, Scotland and Wales.

- Simple security measures and processes, such as those identified on pages 9-11, “an introduction to protective security for owners and operators of publicly accessible locations.”

We would like to consider cost effective means by which such efforts could become more commonplace and co-ordinated, such as through local business groups and other existing mechanisms (e.g. Business Improvement Districts).

Security outcomes could also be more fundamentally improved through a requirement for local/authorities and other relevant local partners to consider security risks and implement appropriate mitigations for public spaces. Requirements could include:

- Developing local, strategic plans to mitigate the risks and impacts of terrorism;
- Implementing proportionate measures through relevant systems, processes and functions to improve public safety and security;
- Establishing clear roles and responsibilities for local partners; and
- Working with key partners (e.g. police) to consider how a security plan would operate in priority local areas.

It is recognised that achieving effective security outcomes at public spaces will usually be achieved through partnership working by multiple organisations who own or operate at such locations. Achieving protective security and preparedness outcomes will usually not be the responsibility of one organisation. There would also need to be coherence between public space requirements and those for venues and organisations within Protect Duty thresholds. These are difficult issues which will require further consideration through the consultation process.

As for the proposed requirements for venues and organisations, Government would need to support local partners in considerations of mitigations for public spaces, for example by providing guidance to enable them to better understand threat methodologies, assess risks, and understand the range of security measures available to mitigate these. Given the complexity of public spaces, there may be a need to consider how bespoke support and expertise could be provided. What is required to support organisations to discharge the Protect Duty is considered further at Section 4.

## Other aspects of a Protect Duty

Where security legislation already exists, we could potentially seek to achieve more effective security outcomes through a requirement for partnership working. For example, under the Sports Grounds Safety Authority guidance, ‘Guide to Safety at Sports Grounds (Green Guide) and Safety Management’, partners are required to work together to consider spectator safety, including for terrorist threats, for the journey to sports grounds (referred to as ‘Zone Ex’ or the ‘Last Mile’), for example from public car parks, local train stations, bus stops and so on.

Similar partnership approaches could be adopted where other legislative requirements already apply (e.g. locations subject to transport security regulation); or where other venues and/or organisations within the scope of a Protect Duty are responsible for events

or activities that could impact on areas outside the boundaries of their own site (for example where large numbers of people are expected to attend an event).

Guidance (potentially legislative) could be used to establish how partners would be required to work together to achieve security outcomes, for example, to help manage queues in the public spaces outside a venue where multiple partners have an interest, or to develop communication mechanisms and ways of working between organisations in response to incidents.

We are aware of examples of organisations already working together on a voluntary basis to improve the security of the shared public spaces in which they operate, for example through joint vigilance and patrolling initiatives, information sharing, or communication networks. We are keen to explore how existing mechanisms, networks and good practice could be spread to realise improved security outcomes, and whether a Protect Duty could be used to support improved co-ordination and delivery of security outcomes amongst organisations operating across shared public spaces and localities.

There are other, specific sectors which could be brought within the scope of the Protect Duty to drive additional security improvements. For example, in the transport sector:

- Bus and coach operators could be required to comply with existing Department for Transport (DfT) best practice security guidance in order to discharge the Protect Duty; and
- Commercial ports and UK flagged ships, which already receive DfT guidance, could be asked to comply with this guidance in order to discharge the Protect Duty.

A Protect Duty could also be applied to companies and other organisations responsible for holding, selling or hiring products that could be used as weapons by terrorists in an attack at a publicly accessible location, such as – vehicles, knives and explosives. Government already legislates or publishes security guidance for some sectors that aims to mitigate the use of certain products and objects as weapons in terrorist attacks. Selling, buying and carrying knives is regulated, as is the purchase of explosives and explosive precursors. DfT's Rental Vehicle Security Scheme includes a ten-point code of practice, and DfT's Goods Vehicle Security Guidance sets out simple steps the operators and drivers of commercial vehicles can take to improve security. A Protect Duty could potentially require these companies and organisations to adhere to security guidance of this kind.

## Questions

19. Does your organisation currently undertake a risk assessment for terrorism?  
Y/N

### [Linked to Question 19]

20. Is this process undertaken by an in-house or an externally appointed individual?  
In house/External

[Where 19 = Y]

21. When you do undertake a terrorism risk assessment, how many working days a year do you estimate your organisation typically spend on this task? (Where this is undertaken by multiple staff, please include total days spent by all staff)?  
\_\_\_\_\_ (Free text, 100 words max)

22. How frequently does your organisation typically review this risk assessment?
- Multiple times per year
  - Around once per year
  - Around once every 2 years
  - Around once every 3 or more years
  - Other (please specify)

23. What mitigations against terrorism risks does your organisation currently undertake (select all that apply)?
- Well defined organisational security protocols and procedures, including for response to terrorist attack
  - Measures are in place to spot and disrupt hostile reconnaissance
  - Work to ensure security behaviours are adopted by the workforce
  - Personnel security policies and procedures consider security risks
  - Site/location vulnerabilities (to terrorist threats) and appropriate physical mitigations are considered
  - Evacuation, invacuation, lockdown procedures are in place and are understood and exercised by staff
  - Staff training is undertaken to raise awareness of the threat and what to do
  - Business continuity procedures or app (e.g. Action Counters Terrorism app) include information on how to respond to attacks
  - Liaison with police or other resource (e.g. security consultant) on threats and appropriate security measures
  - Involved in local security initiatives
  - Other \_\_\_\_\_ (Free text, 100 words max)

24. How much money does your organisation typically spend on new or revised security measures or processes that would mitigate against terrorist risks in one financial year?  
\_\_\_\_\_ (Free text, 100 words max)

25. What are the existing activities and mechanisms which you consider result in the best protective security and organisational preparedness outcomes at public spaces (select all that apply)?
- Communications campaigns e.g. Action Counters Terrorism and See It, Say It, Sorted
  - Staff awareness raising and training courses
  - Advice and guidance products and tools
  - Local authority mechanisms and processes (as outlined at page 19)
  - Other \_\_\_\_\_ (Free text, 100 words max)

26. What are the existing local authority functions which currently result in the best protective security and organisational preparedness outcomes at public spaces (select all that apply)?
- CONTEST and Protect Boards
  - Community Safety Partnerships
  - Licensing for sports grounds safety
  - Planning processes
  - Local Resilience Forums
  - Safety Advisory Groups (for events)
  - Business Improvement Districts (which can be set up by Local Authorities, businesses or individuals to benefit local businesses)
  - Licensing Committees (for the sale and supply of alcohol, the provision of late-night entertainment and refreshment)
  - Health and Safety, fire safety and building control processes.
  - Other \_\_\_\_\_(Free text, 100 words max)
27. What are the existing local authority functions which have the potential to result in the best protective security and organisational preparedness outcomes at public spaces (select all that apply)?
- CONTEST and Protect Boards
  - Community Safety Partnerships
  - Licensing for sports grounds safety
  - Planning processes
  - Local Resilience Forums
  - Safety Advisory Groups (for events)
  - Business Improvement Districts (which can be set up by Local Authorities, businesses or individuals to benefit local businesses)
  - Licensing Committees (for the sale and supply of alcohol, the provision of late-night entertainment and refreshment)
  - Health and Safety, fire safety and building control processes.
  - Other \_\_\_\_\_(Free text, 100 words max)

**[Linked to Question 27]**

28. For your preferred option/s what would be required to improve or support this/these to realise more effective security outcomes?  
\_\_\_\_\_(Free text, 100 words max)

29. How could organisations who work at public spaces be encouraged or required to engage with partner organisations (e.g. police) to ensure there is a better understanding of terrorist threat, the management of risk and mitigating measures?  
\_\_\_\_\_(Free text, 100 words max)

30. What are your views on a potential legislative requirement for local authorities (and relevant public authorities such as Highways Agencies) and other relevant local partners to develop a strategic plan to combat terrorism, to ensure public security, through partnership working?  
\_\_\_\_\_(Free text, 100 words max)

**[Linked to Question 30]**

31. What in your view would be the key components of such a legislative provision and associated guidance?

\_\_\_\_\_ (Free text, 100 words max)

**[Linked to Question 30]**

32. What organisation/s could play a leading role in bringing together and convening such partnerships?

\_\_\_\_\_ (Free text, 100 words max)

**[Linked to Question 30]**

33. What requirements to improve protective security and preparedness could be realistically achieved by such partnerships?

\_\_\_\_\_ (Free text, 100 words max)

34. Do you have any additional proposals to put forward which could improve security at public spaces?

\_\_\_\_\_ (Free text, 100 words max)

35. Where there is an existing legislative requirement for security (e.g. at certain sports grounds and transport sites, or in future those organisations and venues subject to a Protect Duty), is it reasonable to require relevant organisations (for example those surrounding the site) to work in partnership to achieve security outcomes?

\_\_\_\_\_ (Free text, 100 words max)

36. Where there is currently Government security guidance (e.g. bus and coach operators and commercial ports and UK flagged ships) would it be appropriate for this guidance to be become legislative guidance under the Protect Duty to achieve greater certainty on security considerations and outcomes?

\_\_\_\_\_ (Free text, 100 words max)

37. Where Government has published security guidance (e.g. bus and coach operators and commercial ports and UK flagged ships) or put in place voluntary schemes for products that could be used as weapons, would it be reasonable for businesses and other operators responsible to be mandated to follow that guidance under a Protect Duty?

\_\_\_\_\_ (Free text, 100 words max)

To what extent do you agree with the following statement:

38. Compliance with a Protect Duty would require greater effort (e.g. time, staff resource) than compliance for comparable legal and other obligations (e.g. fire safety, health and safety, Licensing Act 2003 guidance, licensing for sports grounds, Safety Advisory Groups)?

Strongly Disagree (SD) – Disagree (D) – Neither Agree nor Disagree (NAND) – Agree (A) – Strongly Agree (SA) [scale]

39. How do you think these new requirements/mitigations will affect:

- a. Number of customers/visitors visiting venues in scope of the duty? (not at all, increase, decrease)
- b. The public's perception of the terrorist threat? (not at all, increase, decrease)

c. Vigilance of the workforce/use of good security behaviours by staff? (not at all, increase, decrease)

40. Annex 3 sets out the anticipated costs and benefits of intervention in the form of a Protect Duty. Please provide any comments you have on this Annex.

\_\_\_\_\_(Free text, 100 words max)

41. Are there any other issues regarding **what** parties within the scope of a Protect Duty should be required to do that you would like to offer views on?

\_\_\_\_\_(Free text, 200 words max)

## Section 3: How should compliance work?

We are committed to using the proposed Protect Duty to help a wide range of businesses and other organisations improve their preparedness for, and protection from, terrorist attack. However, in line with the [‘Better Regulation Framework’](#), we also want to ensure that the Duty does not create unnecessary costs or burdens on staff resource or time. For many organisations falling under the Duty, we anticipate that financial costs incurred will be minimal, and proportionate compliance can be achieved by undertaking simple measures such as regular risk assessment and preparedness activities, for example regular staff training. An impact note has been provided at Annex 3 to indicate expected types of cost and benefits. Further to this, a Regulatory Impact Assessment will be developed and published, informed by the responses to these consultation questions and additional research and analysis.

A key objective of the proposed Protect Duty is to drive forward an improved culture of security, where owners/operators can undertake informed security considerations, and implement reasonable and proportionate security measures, which together will result in much broader improved security outcomes. A Duty would form part of wider, extensive Government efforts to improve protective security and preparedness through other voluntary mechanisms and awareness raising initiatives.

In this section, we consider further how those within scope of a Protect Duty, could demonstrate compliance in the most efficient way. We also consider the basis on which Government would oversee and seek assurance on the delivery of a Protect Duty.

### Venues and large organisations

For public venues, and large organisations, section 2 proposed that responsible owners/operators should be required to:

- Consider terrorist threats to the public and staff at locations they own or operate;
- Assess those risks across their functions and estate; and
- Consider and take forward ‘reasonably practicable’ protective security and organisational preparedness measures.

We propose that risk assessments required by the Duty should demonstrate:

- The range of threats that have been considered;
- The steps that have been subsequently taken to mitigate these threats;
- The steps that have been taken to prepare for and/or respond in the event of an attack; and
- Where steps have not been taken, the reasons why.

These risk assessments will need to be recorded and retained by venues and organisations in scope, as part of evidence to demonstrate part of the process of compliance with the Duty if required to do so. They will need to be reviewed by their owner, at least once a year, and as and when circumstances change, for example following changes to the:

- External risk context - for example a significant terrorist attack in the UK, a change in the Government national terrorism threat level assessment, or a change to the likelihood of threat methodologies); and

- Internal risk context - for example following an expansion of an organisation's premises and/or staff numbers, or a change in the business model, such as a restaurant starting to serve customers outside.

For most organisations, carrying out and implementing appropriate mitigating measures would be straightforward, quick and incur minimal cost. Detailed guidance would be made available to explain the nature of threats and terrorist methodologies, advice on how to assess the potential impacts of an attack at a specific site or public space, and the range of mitigating measures which may be appropriate and proportionate for the range of organisations within scope.

Such measures cannot stop every malicious attack, but should go a long way to reducing the impact on staff and members of the public, without resulting in unreasonable burdens in terms of cost or staff resource. Larger organisations and venues carrying greater or more complex risks, may be required to ensure additional or more sophisticated mitigating measures are put in place, but this would be proportionate to the risk.

Developing an evidence base to support these risk assessments will also assist an inspection regime. Appropriate supporting evidence might include: a brief summary of risks and actions considered and subsequently taken; completion certificates from appropriate staff training courses; evidence of physical security measures implemented, such as door locks, roller shutters and gates; or evidence of attack response plans and their testing with staff.

## Others subject to a Duty

In Section 2 we also considered other locations and parties that could potentially be covered by a Duty, particularly for improving security at public spaces and requirements for partnership working. Compliance requirements for these parties will be dependent on the outcome of discussions to determine what would constitute appropriate legislative requirements in these areas. We will continue to develop thinking and options on this issue further to engagement with relevant stakeholders as part of the consultation process.

## Inspection and enforcement

We consider that an inspection regime would be required to provide the necessary assurance that those within scope of a Protect Duty are meeting its requirements.

We are keen to develop a light touch inspection regime, and will consider whether, and how far compliance could be assessed remotely and or through appropriate third-party agencies. We envisage that an inspection regime would use evidence-based risk assessments and other proportionate means to determine how and where inspections take place. This would take in to account the specific nature of the threat, as well as information regarding levels of compliance and concern.

Inspections would offer an opportunity to provide specific support and advice to venues and organisations to help them improve their protection and preparedness, before any further action was considered. Wherever possible, we would want to encourage compliance with the Duty through incentives and a range of available support.

Further work is taking place to identify the most appropriate and cost-effective delivery authority and mechanisms for carrying out inspections. Consideration is also ongoing as to what powers should be given to inspectors to enable them to effectively assess compliance where necessary.

As detailed above, a key objective of the Duty is to encourage the development of an improved security culture, but to ensure that improvements are made, the Duty must be robust enough to hold those within its scope to account if required. We therefore propose that a proportionate enforcement model is developed where there are issues of non-compliance.

We envisage the development of an enforcement model which gives inspectors the capacity to provide advice and guidance on risk assessment and appropriate mitigations for organisations within scope of the duty; where these were considered insufficient, inspectors could request necessary improvements were made. If these were not taken forward, further steps could include notices of deficiency and enforcement action.

Given the severe impacts that could occur as a result of a breach of the proposed Duty, we propose that a new offence is created for non-compliant organisations who persistently fail to take reasonable steps to reduce the potential impact of attacks. We propose that an enforcement regime is developed, with penalties primarily based on civil sanctions (such as fines) for organisations in breach of the Duty. We consider this is an appropriate framework for a regime that is seeking to encourage more effective organisational security cultures, than a system of criminal sanctions which could result in persons responsible for security at venues and organisations being imprisoned.

Further work will take place to develop detailed options for an enforcement model, relevant offences, and an associated penalties framework.

## Questions

42. How can an inspection regime best be used to support improvements to security culture and practices?

\_\_\_\_\_ (Free text, 100 words max)

43. What are your views on the use of civil penalties (fines) for organisations who persistently fail to take reasonable steps to reduce the potential impact of attacks associated with ensuring compliance with a Protect Duty?

\_\_\_\_\_ (Free text, 100 words max)

44. Do you have any other comments regarding how a compliance regime (inspection and enforcement) could operate?

\_\_\_\_\_ (Free text, 200 words max)

## Section 4: How should government best support and work with partners?

Government currently undertakes significant efforts to ensure parties responsible for publicly accessible locations can be appropriately advised on:

- Understanding the terrorist threat and attack methodologies;
- What constitutes appropriate and proportionate protective security and preparedness measures;
- Understanding the importance of vigilance, the reporting of suspicious behaviour or activity, and what constitutes appropriate action to be taken following a terrorist attack; and
- How to plan and prepare for possible terrorist attacks, for example through staff training and awareness raising and the testing and exercising of emergency procedures.

There are a variety of mechanisms to provide this advice and guidance. These include:

- Engagement by Counter Terrorism Security Advisers ('CTSAs') who provide bespoke advice to site owners and operators, local authorities and others;
- Targeted awareness-raising sessions and training courses delivered by NaCTSO, CTSAs and Counter Terrorism Awareness Advisers to managers, front of house and other staff at publicly accessible locations;
- Engagement with representatives of leading sectors (e.g. sports grounds, shopping centres, entertainment centres), member associations and organisations who own or are responsible or operate at publicly accessible locations;
- Advice provided to local authorities, planners, developers and architects by CTSAs, the Centre for the Protection of National Infrastructure (CPNI), and by the Ministry of Housing, Communities and Local Government through the National Planning Policy Framework and associated Guidance, designed to ensure that proportionate security measures are considered for appropriate new builds and refurbishments;
- Online advice and guidance regularly reviewed and updated, for responsible parties from Counter Terrorism Policing and CPNI; and
- Targeted communications to stakeholders and the public from Counter Terrorism Policing.

We have also been developing new mechanisms to increase the range of our engagement and to develop tools and products tailored to the needs of users, including:

- A new, freely available digital service where security content, advice and training can be accessed through one platform (due to launch in 2021);
- Sectoral and regional engagement days (Action Counters Terrorism Corporate) initiated by Counter Terrorism Policing to provide advice and guidance to sectoral and regional groupings of responsible stakeholders;
- New and revised training and awareness products for managers, front of house and other staff at publicly accessible locations;
- An e-learning awareness training programme (covering spotting the signs of suspicious behaviour and what to do if an attack should take place) freely available to all;
- An Action Counters Terrorism (ACT) app (launched in March 2020) providing easy access to a range of stakeholder advice and guidance, tools and products;

- A range of regularly revised and new advice and guidance provided by Counter Terrorism Policing and CPNI; and
- More extensive communications regarding threat, methodologies and mitigating measures by Counter Terrorism Policing to businesses and the public.

However, we are conscious that take up is voluntary, and research has shown that those responsible for publicly accessible locations are not always aware of these tools. As such, if a Protect Duty is developed, efforts to support organisations within scope of the Duty will need to be enhanced. Dedicated advice and guidance could include:

- Easy to understand information regarding threat and attack methodologies;
- Advice on understanding risk assessment and managing risks;
- Outlining the considerations and tools which allow for mitigating threats through systems and processes; and
- Detailed guidance on protective security and preparedness mitigations.

Supporting guidance will need to reflect clear and simple advice for a wide range of users (in terms of organisation size, type / business, and security expertise).

In some cases, as was noted in section 2 regarding a potential legislative requirement for public spaces, Government will need to work with partners to consider bespoke support for taking forward aspects of a Protect Duty, to ensure that effective security outcomes are realised.

In addition, there is a role for wider partners in supporting the Duty. Member and representative associations (e.g. for business sectors, and local areas) will be important in raising awareness of new requirements, to support understanding and delivery efforts, as well as considering new delivery and communications channels.

There would also be a need to engage with the security industry and other organisations with a role in delivering and supporting security solutions (services and products) that help owners and operators to comply with the Duty. It will be important to ensure that the market can provide sufficient high-quality advice, products and services to all those within scope. To do this, the Government may consider the introduction or support for new and existing initiatives which can help promote and maintain appropriate standards such as accredited training, approved contractor schemes, or regulation.

We also want to consider how and where a Duty could be used to incentivise, rather than enforce, compliance. Incentives are already used to encourage security behaviours and activities. For example, PoolRe, the Government-backed terrorism reinsurer, encourages businesses to consider the risks from terrorism and to implement protective security and preparedness measures. In return, organisations can qualify for a discount on their insurance premium, usually set at 5%. To encourage widespread compliance with a Protect Duty, we are keen to ensure that a broad range of incentives are considered and developed, both within the insurance industry and beyond. This could include the development and use of product certifications or standards where relevant to aspects of the Duty.

In all these efforts, we are also mindful to ensure that the Duty does not inadvertently create any unintended consequences or costs.

## Questions

45. Do you currently access Government advice (primarily from Counter Terrorism Policing and the Centre for the Protection of National Infrastructure) regarding threat, protective security and preparedness?

Y/N

### [If 45 = Y]

46. What, if anything, do you find most valuable in current advice and guidance?  
\_\_\_\_\_ (Free text, 100 words max)

### [If 45 = N]

47. Why do you not currently access this advice and guidance?

- a. I did not know it existed
- b. I do not think I need to address the threat
- c. I do not have the time to access this
- d. It is too confusing to find what I want
- e. Other \_\_\_\_\_ (Free text, 100 words max)

48. What would you find most useful to help you to comply with a Protect Duty (select all that apply)?

- a. A single, digital service where you could access relevant material, advice and training in one place
- b. Easy to digest information regarding threat and attack methodologies
- c. A risk assessment template
- d. Information on undertaking a risk assessment for terrorism threats
- e. Advice relating to protective security mitigations
- f. Advice relating to personnel and people security
- g. Advice relating to how an organisation can prepare for terrorism attack
- h. Advice on what constitutes reasonably practicable and appropriate mitigations appropriate for my circumstances
- i. Development of product certifications or standards for aspects of the approach
- j. Staff training and awareness courses
- k. E-learning products
- l. An App
- m. A sector meeting where I can talk about the Duty with experts and other similar organisations
- n. A local meeting where I can talk about the Duty with experts and other similar organisations
- o. Other: \_\_\_\_\_ (Free text, 100 words max)

49. Counter-Terrorism Policing are working with Government and the Private Sector to design a digital service to provide access to relevant counter-terrorism material, advice and training in one place for organisations operating in publicly accessible locations. Do you anticipate that you would access counter terrorism information through this service if it were available to you?

Y/N

### [If 49= N]

50. Why not?

\_\_\_\_\_(Free text, 100 words max)

**[If 49 = Y]**

51. What would you most likely use this kind of service for (tick all that apply)?

- a. To get general updates on how the terrorism risk is changing
- b. To support business planning activities
- c. To understand what risk management activities you need to do
- d. To access CT training
- e. To connect with other organisations to discuss counter terrorism
- f. To understand what to do after an incident
- g. Reporting of suspected terrorist activity/concerns

52. Do you have any further comments or suggestions for how you might like to access counter-terrorism information and work with local partners on counter-terrorism issues in the future?

\_\_\_\_\_(Free text, 100 words max)

53. What role should local business partnerships (such as Business Improvement Districts, Local Enterprise partnerships, etc.) have in supporting organisations and venues to deliver improved security?

\_\_\_\_\_(Free text, 100 words max)

54. Working with others, what could the Government best do to incentivise improved security practices?

\_\_\_\_\_(Free text, 100 words max)

55. To support the provision of high-quality advice and guidance from private sector security professionals providing counter terrorism security advice, Government should consider (tick all that apply)

- a. Government supported standards for Counter Terrorism (CT) risk assessments and advice
- b. Qualifications / Accredited training for individual professionals
- c. Government supported 'approved contractors scheme'
- d. Regulation of CT consultants
- e. None
- f. Other \_\_\_\_\_ (Free text, 100 words max)
- g. I don't know

56. What advice and support would be required for organisations and venues within the scope of Protect Duty?

\_\_\_\_\_(Free text, 100 words max)

57. Given the complexity of public spaces, and the potential need for partnership working to achieve effective ways of working leading to improvements in protective security and preparedness, what additional bespoke support and expertise could be provided?

\_\_\_\_\_(Free text, 100 words max)

58. Do you have any other proposals on what Government could do to support partners in the delivery of a Protect Duty?  
\_\_\_\_\_ (Free text, 200 words max)

## Responding to this consultation

### Responding online

Please respond online to this consultation using our online form at [www.homeofficesurveys.homeoffice.gov.uk/s/1D4SQ3/](http://www.homeofficesurveys.homeoffice.gov.uk/s/1D4SQ3/)

### Representative groups

Representative groups are asked to give a summary of the people and organisations they represent when they respond.

### Alternative ways to respond and additional copies

To help us analyse the responses please use the online system wherever possible. If, for exceptional reasons, you are unable to use the online system, for example because you use specialist accessibility software that is not compatible, you may download a word document version of the form and email it, or post it to:

Protect and Prepare  
Office for Security and Counter Terrorism  
5th Floor NE, Peel Building,  
Home Office  
2 Marsham Street,  
London, SW1P 4DF

Further paper copies of this consultation can be obtained from this address and it is also available online at [www.gov.uk/government/consultations/](http://www.gov.uk/government/consultations/)

Alternative format versions of this publication can be requested from [ProtectDuty@homeoffice.gov.uk](mailto:ProtectDuty@homeoffice.gov.uk)

### Comments and complaints

If you have any complaints or comments about the consultation process you should contact the Home Office using the above email or postal address.

### Publication of responses and Impact Assessment

A paper summarising the responses to this consultation will be published. The response paper will be available online at [www.gov.uk/government/consultations/protect-duty](http://www.gov.uk/government/consultations/protect-duty) . This will be accompanied by an Impact Assessment of the proposals drawing from the responses to this consultation and additional research and analysis work.

### Confidentiality

Information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are

primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 2018 (DPA) and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential.

If we receive a request for disclosure of the information, we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Home Office.

The Home Office will process your personal data in accordance with the DPA and in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties.

## Glossary

**Table 1: Glossary of terms used in the Protect Duty Consultation.**

Attack methodologies	Different methods of attack used by terrorists. These have recently included attacks in the UK and Europe involving the use of Person Borne Improvised Explosive Devices (IEDs), postal IEDs, Vehicle As a Weapon, bladed weapons and firearms.
Action Counters Terrorism (ACT)	A national awareness scheme to protect buildings, business areas and their surrounding neighbourhoods from the threat of terrorism.
ACT Awareness e-Learning	A nationally recognised corporate CT guidance product, developed by Counter Terrorism Policing, to help people better understand, and mitigate against, current terrorist methodology. It is available to all organisations, their staff and the general public ( <a href="https://www.gov.uk/government/news/act-awareness-elearning">https://www.gov.uk/government/news/act-awareness-elearning</a> )
Centre for the Protection of National Infrastructure (CPNI)	The Government authority for protective security advice to the UK national infrastructure. It protects national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats.
Counter Terrorism Security Advisors (CTSAs)	Individuals who work within local police forces as officers and staff. Their primary role is to provide help, advice and guidance on all aspects of counter-terrorism protective security to industry sectors and others.
Hostile reconnaissance	The information-gathering phase conducted by those individuals or groups with malicious intent.
Large organisations	Organisations with 250 or more employees
National Counter Terrorism Security Office (NaCTSO)	A police unit that supports the 'Protect and Prepare' strands of the Government's counter-terrorism strategy.
Public Venues	In the Protect Duty context these are permanent buildings (e.g. entertainment and sports venues) or temporary event locations (such as outdoor festivals) where there is a defined boundary and open access to the public
Public spaces	These are open public locations which usually have no clear boundaries or well-defined entrances / exit points

	(e.g. city centre squares, bridges or busy thoroughfares, parks, and beaches).
Publicly Accessible Location	Any place to which the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission. Publicly accessible locations include a wide variety of everyday locations such as: sports stadiums; festivals and music venues; hotels; pubs; clubs; bars and casinos; high streets; retail stores; shopping centres and markets; schools and universities; medical centres and hospitals; places of worship; Government offices; job centres; transport hubs; parks; beaches; public squares and other open spaces. This list is not exhaustive.
Reasonably practicable (mitigations)	Requires owners/operators to weigh a risk against the effort, time and money needed to mitigate it.
See, Check and Notify (SCaN)	Training which aims to help businesses and organisations maximise safety and security using their existing resources. It empowers staff to correctly identify suspicious activity and know what to do when they encounter it. It helps ensure that individuals or groups seeking to cause your organisation harm are unable to get the information they need to plan their actions.

## Annex 1 - Exemptions and exclusions

The following sectors already have legislative requirements in place to consider terrorist threats and take forward appropriate mitigating measures. Since these outcomes are very similar to those envisaged under a potential Protect Duty, we propose that they are considered exempt from any new legislative requirements.

### Rail

- Domestic heavy rail (Network Rail, train and freight operating companies and depot operators). Not heritage rail operators.
- Domestic light rail (currently only London Underground, Docklands Light Railway and Glasgow Subway are regulated, but a review (Trams) is underway, which aims to bring all light rail operators into scope of DfT's rail security regulation by Summer 2021).
- International rail (Channel Tunnel operators).
- Transportation of dangerous goods by road and rail.

### Aviation

- Landside publicly accessible areas at the UK's 50 airports already follow guidance captured under the National Aviation Security Programme (NASP).
- Airfields which do not fall under the NASP are being reviewed separately to potentially be brought into the programme.

We do not envisage the following sector to be within the scope of a Duty:

### Maritime

- Chemical Oil Gas (COG) and Container Ro-Ro (CRR) and Other Bulk Cargo (OBC) ports - as these are not publicly accessible locations.

## Annex 2 – Best practice examples of security considerations and mitigations at different organisations

Venue/Organisation Description	Reasonably Practicable Mitigating Measures
<p><b>1. Small business</b></p> <ul style="list-style-type: none"> <li>• For example a retail outlet</li> <li>• Single rented premises (town centre location).</li> <li>• 10-15 staff.</li> <li>• Up to 100 customers at a time.</li> </ul>	<p><b>Risk Assessment:</b></p> <ul style="list-style-type: none"> <li>• Undertake a recorded risk assessment based upon information about terrorist attacks available through freely accessible government websites (CPNI and NaCTSO).</li> <li>• Consideration of a limited number of risks – e.g. marauding weapon attack, and an improvised explosive device.</li> </ul> <p><b>Active Security:</b></p> <ul style="list-style-type: none"> <li>• The staff should know how to spot and report suspicious activity and may have received some level of hostile behaviour awareness (e.g. as provided by the free Action Counters Terrorism (ACT) e-learning and which can be developed for customer facing staff through the See Check and Notify courses).</li> <li>• The business could coordinate its active security measures with other businesses in the area, possibly coordinated by the local Business Improvement District or Community Safety Partnership.</li> </ul> <p><b>Physical Security:</b></p> <ul style="list-style-type: none"> <li>• There would be no expectation that the business would invest in specific physical security measures.</li> <li>• However, it would be expected that existing security measures (such as roller shutters or locks on doors) would be included in plans on how to respond to an attack.</li> </ul> <p><b>Response:</b></p> <ul style="list-style-type: none"> <li>• The business would be expected to have a plan for each of the attack types identified as a risk. These would be known to staff, in a similar manner to a fire plan.</li> </ul>

	<ul style="list-style-type: none"> <li>• Staff would be expected to have been given training in appropriate response to risks identified in the risk assessment and to know who has the authority to activate specific elements of a plan (for example a lock down procedure).</li> <li>• The training required for this is available free through the ACT e-learning product and the guidance on appropriate measures is available online from NaCTSO.</li> <li>• The business should work with the local Community Safety Partnership and Local Resilience Forum to ensure their plans are consistent.</li> </ul> <p><b>Intervention:</b></p> <ul style="list-style-type: none"> <li>• A small business like this would not be expected to have any measures in place to support police interventions.</li> </ul> <p><b>Recovery:</b></p> <ul style="list-style-type: none"> <li>• A single site like this would not be expected to have a business continuity plan.</li> </ul>
<p><b>2. Local large event</b></p> <ul style="list-style-type: none"> <li>• No employees, 20-40 volunteers,</li> <li>• Between 250-500 people attending.</li> <li>• Some police engagement through Neighbourhood Policing Teams. Not subject to Safety Advisory Group assessments.</li> </ul>	<p><b>Risk Assessment:</b></p> <ul style="list-style-type: none"> <li>• A recorded risk assessment based upon information available through freely accessible government websites (CPNI and NaCTSO).</li> <li>• The information used to build this risk assessment could be supported by information from the Neighbourhood Policing Team.</li> <li>• The risk assessment would cover the most applicable risks – e.g. marauding knife attack, improvised explosive device, marauding gun attack and vehicle as a weapon.</li> </ul> <p><b>Active Security:</b></p> <p>Lower levels of active security can be implemented including:</p> <ul style="list-style-type: none"> <li>• Making volunteer staff visible and professional looking to establish a deterrent posture (this is not expecting local volunteers to take on a security role, but reflects the effect that vigilant, professional and visible staff have on those with a hostile mindset)</li> <li>• Providing some form of awareness training for the volunteers (for example the ACT e-learning course, which is provided free by NaCTSO and incorporates a base level of hostile behaviour detection and reporting)</li> </ul>

	<p><b>Physical Security:</b></p> <ul style="list-style-type: none"> <li>• Dependent on the appropriate mitigation measures identified in the risk assessment.</li> <li>• It may be appropriate to consider (and record decisions on) traffic management measures (e.g. local road closures) or temporary vehicle mitigation measures.</li> <li>• In an open space, it would be unlikely that other physical security measures would be effective or proportionate.</li> </ul> <p><b>Response:</b> Event organisers would be expected to:</p> <ul style="list-style-type: none"> <li>• Have a plan for each of the attack types identified as a risk (known to all volunteers in the same way that plans for lost children, first aid or fire would be shared).</li> <li>• Provide aide memoires for volunteer staff to support the response to potential incidents, examples are available through the Neighbourhood Policing Team from Counter Terrorism Policing allowing these to be provided at print cost only.</li> <li>• Engage with available awareness training (e.g. ACT e-learning) to build their capability for both the active security and response elements at low to no cost.</li> </ul> <p><b>Intervention:</b></p> <ul style="list-style-type: none"> <li>• A one-off event like this would not be expected to have any measures in place to support police interventions.</li> </ul> <p><b>Recovery:</b></p> <ul style="list-style-type: none"> <li>• A one-off event like this would not be expected to have a business continuity plan.</li> </ul>
<p><b>3. Medium sized business location, part of a national chain</b></p> <ul style="list-style-type: none"> <li>• For example, a cinema or supermarket.</li> <li>• Possibly several hundred employees (nationally)</li> </ul>	<p><b>Risk Assessment:</b></p> <ul style="list-style-type: none"> <li>• Risk assessment drawn from the national chain's security team (may attend the ACT Corporate: National events or other sector engagement forums) Expected to have a corporate policy for carrying out risk assessments; may have issued direction on what is required from staff.</li> </ul>

- Hundreds of visitors (at each location at any one time) and hundreds of thousands of attendees (at all locations nationally in a year).
- Ongoing police liaison through crime prevention partnerships or the Community Safety Partnership.

- Although the risk assessment may not score some threats as highly (due to low likelihood), it would be expected to include assessments for most attack types and justifications for not implementing mitigations where not appropriate.
- The risk assessment should include a pre-written plan for mitigating actions that will be taken for increases to the National Threat Level.

**Active Security:**

- Building on the corporate posture, which should include security minded communications messages, the site should include a range of active security measures that match the identified risks.
- This is likely to include visible security staff, trained hostile behaviour detection staff (which is available at the lowest level through ACT e-learning and ACT Awareness, but can build through SCaN Customer Facing) and closed-circuit television.
- These measures should be integrated with neighbouring businesses and linked into the plans developed by the local Community Safety Partnership or other appropriate local forum.

**Physical Security:**

- With the increased risk awareness and the resources available, a range of suitable physical security measures would be expected.
- These may complement existing crime reduction and loss mitigation measures. They are likely to include mechanisms such as access control to secured areas, physical protection in areas that vehicles can access and the ability to secure the site during a lock down.

**Response:**

- Based on the risk assessment, the business would be expected to have a plan for each of the attack types identified as a risk.
- Where there are risks that the business feels it would be disproportionate to practically hold a plan for, this must be justified in the risk assessment.
- These plans need to be known by staff and key roles identified.

	<ul style="list-style-type: none"> <li>• All staff should receive some form of awareness training that allows them to respond appropriately at a personal level.</li> <li>• Key staff should be trained and exercised in their roles and the decisions they may be expected to make.</li> <li>• It should be clear who the key decision makers are to enable actions such as evacuation or invacuation.</li> </ul> <p><b>Intervention:</b></p> <ul style="list-style-type: none"> <li>• A business at this scale should consider how they can support a police intervention.</li> <li>• This should include identifying police rendezvous sites in plans and may include considering how they pass situational awareness to responding officers.</li> <li>• At this level the business may consider placing back office signage to support an intervention and could support the local force’s firearms officers in the development of a tactical information pack.</li> </ul> <p><b>Recovery:</b></p> <ul style="list-style-type: none"> <li>• There should be a corporate business continuity plan, with managerial connection to the Local Resilience Forum.</li> </ul>
<p><b>4. Large site with multiple individual businesses renting units</b></p> <ul style="list-style-type: none"> <li>• For example, an out of town outlet centre.</li> <li>• Small number of employees providing infrastructure and security, large number of employees of individual businesses.</li> <li>• Thousands of visitors daily.</li> </ul>	<p><b>Risk Assessment:</b></p> <ul style="list-style-type: none"> <li>• The risk assessment would cover all the current threat spectrum, although security measures may not be necessary for the least plausible risks.</li> <li>• This risk assessment needs to be recorded and available for all the businesses that occupy units within the site.</li> <li>• A large site would likely be working with their local authority to allow them to base their risk assessment on the Counter Terrorism Local Profile, which is shared with each local authority.</li> </ul> <p><b>Active Security:</b></p>

- The business should provide for the integration of loss prevention and public safety personnel into their security posture (considering the level of training required by their staff) to ensure that they can deliver the desired effect.
- The site owner should set the standards required for active security within the units, working with the local Community Safety Partnership to ensure this is consistent.
- At the very least, the site should be considering a visible guarding deterrent, some form of hostile behaviour detection and should be employing security minded communications techniques.

**Physical Security:**

- With the increased risk awareness and the resources available, suitable physical security measures would be expected.
- The site should have physical security that controls access to secure locations independently.
- This protection should be at a suitable standard, using a mix of hostile vehicle mitigation, traffic control measures, deterrence and the ability to secure the site during a lock down.
- The decisions around this need to be recorded in the risk assessment.

**Response:**

- Through a risk-based approach, the site would be expected to have a plan for each of the attack types identified as a risk.
- Where there are risks that the business feels it would be disproportionate to practically hold a plan for, this must be justified in the risk assessment.
- Site owner should provide clear direction on the responses required by their staff. Within this direction, there should be a requirement that all staff employed have some form of awareness training.
- The site should provide clear plans for all potential events, should train their staff appropriately and may conduct exercises with the Local Resilience Forum.

	<ul style="list-style-type: none"> <li>Enhanced first aid kits should be considered and training on first aid could be provided to staff to allow them to deal with the aftermath of an incident. There should be consideration of crisis communications.</li> </ul> <p><b>Intervention:</b></p> <ul style="list-style-type: none"> <li>The site should have a plan how they can support a police intervention.</li> <li>This plan must include identified police rendezvous sites, should include clear direction on how they will pass situational awareness to responding officers.</li> <li>There should be back office signage to support an intervention and the site owners should work with the local force's firearms officers in the development of a tactical information pack.</li> </ul> <p><b>Recovery:</b></p> <ul style="list-style-type: none"> <li>The business should have a comprehensive business continuity plan, including how support will be offered to the businesses operating from the units.</li> </ul>
<p><b>5. Large venue</b></p> <ul style="list-style-type: none"> <li>For example, a theme park.</li> <li>Many employees.</li> <li>Thousands of visitors daily.</li> </ul>	<p><b>Risk Assessment:</b></p> <ul style="list-style-type: none"> <li>They would be supported by their local authority and would have access to the Counter Terrorism Business Information Exchange sub-sectors and may attend the ACT Corporate: National events.</li> <li>They will be regularly briefed by a dedicated CTSA and are likely to have information released to them from any counter terrorism investigation that identifies that they are being targeted.</li> <li>From this, there is no reason for them not to make appropriate risk assessments based on all the available information.</li> <li>The risk assessment would cover all the current threat spectrum, although security measures may not be necessary for the least serious risks, it would be expected to include assessments for most attack types and justification for not implementing specific mitigations or CTSA recommendations.</li> </ul>

- This risk assessment should include a pre-written plan for mitigation actions and be understood by all key staff throughout the site, for example if the terrorist threat level moved to critical.

**Active Security:**

- The nature of this type of location makes it possible to layer active measures.
- As a public facing business that actively engages with their customers, the site could use deterrence messaging in their communications.
- At the access points, a search and screening process could be implemented, for example using a modern, proportionate high footfall screening approach.
- If there is an active control room with live CCTV feed, the opportunity for hostile behaviour detection can be spread more widely than in other sites.
- All the active measures require staff to deliver, which will require the development of a security culture and the implementation of measures (e.g. by employment screening) to minimise the insider threat.

**Physical Security:**

- The site should have physical measures and associated policies and processes in place to control access to the site by vehicles and pedestrians.
- Where there are key assets, measures should be taken to minimise their vulnerability, typically through adding appropriate additional layers of security.
- There should be measures to reduce the risk of vehicle as a weapon attack both within and on the approach to the site. This protection should include an appropriate mix of hostile vehicle mitigation, traffic control measures and deterrence.

**Response:**

- Detailed plans with clear direction to all staff should be available, with clear delegation of responsibilities. Consideration should be given to how this extends to contractors and other partners working on the site (e.g. private contract security providers, catering concession personnel).

- Training in generic awareness and specific roles should be undertaken for all staff and exercising should be used to prepare for any incident.
- These plans could include dedicated first aid support and should have enhanced first aid kits at key locations and a plan around casualty handling.
- The site should have a detailed communications plan to be used in the event of a crisis.

**Intervention:**

- The site should have a plan as to how they can support a police intervention.
- This plan must include identified police rendezvous sites, should include clear direction on how they will pass situational awareness to responding officers.
- There should be back office signage to support an intervention and the site owners should work with the local force's firearms officers in the development of a tactical information pack.

**Recovery:**

- The business should have a comprehensive business continuity plan, that is flexible depending on the scale or duration of the events, including restoration of critical services/function, the support to staff and proactive engagement with the Local Resilience Forum, Policing and the community.

## Annex 3 - What types of cost and benefits are expected?

Should the evidence gained from the consultation support further intervention or change, then detailed proposals will be set out in full at a later date, supported as required by a Regulatory Impact Assessment and analysis of the expected effects. At this stage costs and benefits will be identified and assessed for the primary options, drawing on the information gained through the consultation.

The expectation is that the current situation will be used as the baseline or counterfactual. The Home Office will seek to measure the marginal change in costs and/or benefits arising from any change to the current recommendations. Direct, indirect and wider effects will be considered. The assessment will also examine risks, any unintended consequences and any potential impacts on specific groups. Both quantitative and qualitative evidence will be used.

The following costs and benefits of further intervention may be seen:

<b>Stakeholder group</b>	<b>Potential benefits</b>
Organisations owning / operating Publicly Accessible Locations (Including Businesses, publicly owned and third sector)	Reduced risk to organisations from disruption (direct and indirect) caused by terrorist incidents
	Reduced impact of terrorist incidents on organisations (e.g. reduced property damage costs)
	Improved reassurance/feeling of safety among employees/volunteers from increased considerations of security from terrorist threats and mitigating measures
	Potential for increased revenue for security providers
	Potential for reduced insurance premium for businesses that implement mitigating measures
	Wider benefits of a perceived reduction in risk (e.g. increased visitors/revenue)
	Dependent on the nature of the duty, greater cohesion between emergency services, local authorities and businesses
Society	Improved vigilance, security measures, systems and processes, have the potential to disrupt, deter or detect terrorist incidents
	Reduced impact of terrorist incidents (e.g. loss of life, injury, psychological impact)
	Wider benefits of actual and perceived reduction in risk (e.g. increased visitors/revenue)
	Improved reassurance/feeling of safety to members of the public
	Spill over effects of security measures being beneficial in deterring or reducing other high harms or forms of crime

<b>Stakeholder group</b>	<b>Potential costs</b>
Organisations owning / operating	Familiarisation time with changes to the Protect Duty's requirements
	Cost of undertaking risk assessments
	Cost of developing and updating action plans

Publicly Accessible Locations (Including Businesses, publicly owned and third sector)	Cost of introducing measures to mitigate risks identified (e.g. training costs, range of mitigating measures, staff costs)
	Potential costs of an inspection/regulatory or self-reporting regime
	Cost of sanctions/penalties if non-compliant
	Staff costs to keep internal guidance, staff processes and procedures up to date
	Potential displacement of threat towards smaller organisations which are out of scope of the duty.
	Firms in scope of this duty will have a higher marginal cost versus those operating online only (for example in store retail vs online)
	Greater awareness of risks of terrorism could lead to some individual employees overestimating the likelihood of an attack, which could have potential psychological effects
Public Sector	Enforcement costs
Society	Potential displacement of terrorist threat from in scope areas to out of scope areas

## Annex 4 – List of consultation questions

### Section 1: Who (or where) should legislation apply to?

To what extent do you agree or disagree with the following statement:

1. Venues and organisations owning, operating or responsible for publicly accessible locations should take appropriate and proportionate measures to protect the public from attacks in these locations  
Strongly Disagree (SD) – Disagree (D) – Neither Agree nor Disagree (NAND) – Agree (A) – Strongly Agree (SA) [scale]

To what extent do you agree or disagree with the following statement:

2. Venues and organisations owning, operating or responsible for publicly accessible locations should prepare their staff to respond appropriately in the event of a terrorist attack to best protect themselves and any members of the public present  
Strongly Disagree (SD) – Disagree (D) – Neither Agree nor Disagree (NAND) – Agree (A) – Strongly Agree (SA) [scale]
3. We propose that a targeted Protect Duty applies only to certain public venues. What criteria would best determine which venues a Duty should apply to ?
  - a. Capacity (as currently used in Fire Safety Regulations)
  - b. Annual revenue
  - c. Staffing levels
  - d. Other: \_\_\_\_\_(Free text, 100 words max)

#### [Where 3 is a]

4. We have proposed a venue capacity of 100 persons or more as a threshold. What capacity level do you think would be appropriate to determine venues in scope of the Duty?  
\_\_\_\_\_ (Free text, 100 words max)

#### [Where 3 is b-d]

5. What threshold would you propose for inclusion in the scope of the Protect Duty for this criterion?  
\_\_\_\_\_ (Free text, 100 words max)
6. We propose that a requirement to consider security and implement appropriate mitigations at a venue should fall to the owner and/or operator of the venue. Do you consider this appropriate?  
Y/N

#### [If 6 = N]

7. If no, why not:  
\_\_\_\_\_ (Free text, 100 words max)
8. We propose that where there is a shared organisational responsibility for a venue, or multiple organisations operating at a venue within scope, the parties would have to work together to meet the requirements. Do you consider this is appropriate?

Y/N

**[If 8 = N]**

9. If no, why not:

\_\_\_\_\_ (Free text, 100 words max)

10. We propose that a Protect Duty would also apply to certain organisations operating at publicly accessible locations. If an organisation's size were a criterion for its inclusion in the scope of the Duty, what would be an appropriate threshold?

- a. All organisations
- b. Micro (1-9 employees) and above
- c. Small (10-49 employees) and above
- d. Medium (50-249 employees) and above
- e. Large (250+ employees)
- f. Other \_\_\_\_\_ (Free text, 100 words max)

**[Linked to Question 10]**

11. What is your reasoning for this answer?

\_\_\_\_\_ (Free text, 100 words max)

12. We have proposed a Protect Duty would apply to organisations with 250 or more employees. Is it clear as to whether your organisation falls within this criteria?

Y/N

**[If 12 = N]**

13. If no, why not?

\_\_\_\_\_ (Free text, 100 words max)

14. Are you clear about whether your organisation falls within the scope of the definition of a 'publicly accessible location' (a place to which the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission)?

Y/N

**[If 14 is N]**

15. If no, why not?

\_\_\_\_\_ (Free text, 100 words max)

16. Referring to Annex 1, do you consider that there should be other exemptions from a Protect Duty?

Y/N

**[if 16 is Y]**

17. If so what or who and why?

\_\_\_\_\_ (Free text, 200 words max)

18. Are there any other issues regarding who legislation should apply to that you would like to offer views on?

\_\_\_\_\_ (Free text, 200 words max)

## Section 2: What should the requirements be?

19. Does your organisation currently undertake a risk assessment for terrorism?  
Y/N

### [Linked to Question 19]

20. Is this process undertaken by an in-house or an externally appointed individual?  
In house/External

### [Where 19 = Y]

21. When you do undertake a terrorism risk assessment, how many working days a year do you estimate your organisation typically spend on this task? (Where this is undertaken by multiple staff, please include total days spent by all staff)?  
\_\_\_\_\_ (Free text, 100 words max)

22. How frequently does your organisation typically review this risk assessment?

- Multiple times per year
- Around once per year
- Around once every 2 years
- Around once every 3 or more years
- Other (please specify)

23. What mitigations against terrorism risks does your organisation currently undertake (select all that apply)?

- Well defined organisational security protocols and procedures, including for response to terrorist attack
- Measures are in place to spot and disrupt hostile reconnaissance
- Work to ensure security behaviours are adopted by the workforce
- Personnel security policies and procedures consider security risks
- Site/location vulnerabilities (to terrorist threats) and appropriate physical mitigations are considered
- Evacuation, invacuation, lockdown procedures are in place and are understood and exercised by staff
- Staff training is undertaken to raise awareness of the threat and what to do
- Business continuity procedures or app (e.g. ACT app) include information on how to respond to attacks
- Liaison with police or other resource (e.g. security consultant) on threats and appropriate security measures
- Involved in local security initiatives
- Other \_\_\_\_\_ (Free text, 100 words max)

24. How much money does your organisation typically spend on new or revised security measures that would mitigate against terrorist risks in one financial year?  
\_\_\_\_\_ (Free text, 100 words max)

25. What are the existing activities and mechanisms which you consider result in the best protective security and organisational preparedness outcomes at public spaces (select all that apply)?

- a. Communications campaigns e.g. Action Counters Terrorism and See It, Say It, Sorted
- b. Staff awareness raising and training courses
- c. Advice and guidance products and tools
- d. Local authority mechanisms and processes (as outlined at page 19)
- e. Other \_\_\_\_\_ (Free text, 100 words max)

26. What are the existing local authority functions which currently result in the best protective security and organisational preparedness outcomes at public spaces (select all that apply)?

- a. CONTEST and Protect Boards
- b. Community Safety Partnerships
- c. Licensing for sports grounds safety
- d. Planning processes
- e. Local Resilience Forums
- f. Safety Advisory Groups (for events)
- g. Business Improvement Districts (which can be set up by Local Authorities, businesses or individuals to benefit local businesses)
- h. Licensing Committees (for the sale and supply of alcohol, the provision of late-night entertainment and refreshment)
- i. Health and Safety, fire safety and building control processes.
- j. Other \_\_\_\_\_ (Free text, 100 words max)

27. What are the existing local authority functions which have the potential to result in the best protective security and organisational preparedness outcomes at public spaces (select all that apply)?

- a. CONTEST and Protect Boards
- b. Community Safety Partnerships
- c. Licensing for sports grounds safety
- d. Planning processes
- e. Local Resilience Forums
- f. Safety Advisory Groups (for events)
- g. Business Improvement Districts (which can be set up by Local Authorities, businesses or individuals to benefit local businesses)
- h. Licensing Committees (for the sale and supply of alcohol, the provision of late-night entertainment and refreshment)
- i. Health and Safety, fire safety and building control processes.
- j. Other \_\_\_\_\_ (Free text, 100 words max)

**[Linked to Question 27]**

28. For your preferred option/s what would be required to improve or support this/these to realise more effective security outcomes?

\_\_\_\_\_ (Free text, 100 words max)

29. How could organisations who work at public spaces be encouraged or required to engage with partner organisations (e.g. police) to ensure there is a better understanding of terrorist threat, the management of risk and mitigating measures?  
\_\_\_\_\_ (Free text, 100 words max)

30. What are your views on a potential legislative requirement for local authorities (and relevant public authorities such as Highways Agencies) and other relevant local partners to develop a strategic plan to combat terrorism, to ensure public security, through partnership working?  
\_\_\_\_\_ (Free text, 100 words max)

**[Linked to Question 30]**

31. What in your view would be the key components of such a legislative provision and associated guidance?  
\_\_\_\_\_ (Free text, 100 words max)

**[Linked to Question 30]**

32. What organisation/s could play a leading role in bringing together and convening such partnerships?  
\_\_\_\_\_ (Free text, 100 words max)

**[Linked to Question 30]**

33. What requirements to improve protective security and preparedness could be realistically achieved by such partnerships?  
\_\_\_\_\_ (Free text, 100 words max)

34. Do you have any additional proposals to put forward which could improve security at public spaces?  
\_\_\_\_\_ (Free text, 100 words max)

35. Where there is an existing legislative requirement for security (e.g. at certain sports grounds and transport sites, or in future those organisations and venues subject to a Protect Duty), is it reasonable to require relevant organisations (for example those surrounding the site) to work in partnership to achieve security outcomes?  
\_\_\_\_\_ (Free text, 100 words max)

36. Where there is currently Government security guidance (e.g. bus and coach operators and commercial ports and UK flagged ships) would it be appropriate for this guidance to become legislative guidance under the Protect Duty to achieve greater certainty on security considerations and outcomes?  
\_\_\_\_\_ (Free text, 100 words max)

37. Where Government has published security guidance (e.g. bus and coach operators and commercial ports and UK flagged ships) or put in place voluntary schemes for products that could be used as weapons, would it be reasonable for businesses and other operators responsible to be mandated to follow that guidance under a Protect Duty?  
\_\_\_\_\_ (Free text, 100 words max)

To what extent do you agree with the following statement:

38. Compliance with a Protect Duty would require greater effort (e.g. time, staff resource) than compliance for comparable legal and other obligations (e.g. fire safety, health and safety, Licensing Act 2003 guidance, licensing for sports grounds, Safety Advisory Groups)?

Strongly Disagree (SD) – Disagree (D) – Neither Agree nor Disagree (NAND) – Agree (A) – Strongly Agree (SA) [scale]

39. How do you think these new requirements/mitigations will affect:

- a. Number of customers/visitors visiting venues in scope of the duty? (not at all, increase, decrease)
- b. The public's perception of the terrorist threat? (not at all, increase, decrease)
- c. Vigilance of the workforce/use of good security behaviours by staff? (not at all, increase, decrease)

40. Annex 3 sets out the anticipated costs and benefits of intervention in the form of a Protect Duty. Please provide any comments you have on this Annex.

\_\_\_\_\_ (Free text, 100 words max)

41. Are there any other issues regarding **what** parties within the scope of a Protect Duty should be required to do that you would like to offer views on?

\_\_\_\_\_ (Free text, 200 words max)

### Section 3: How should compliance work?

42. How can an inspection regime best be used to support improvements to security culture and practices?

\_\_\_\_\_ (Free text, 100 words max)

43. What are your views on the use of civil penalties (fines) for organisations who persistently fail to take reasonable steps to reduce the potential impact of attacks associated with ensuring compliance with a Protect Duty?

\_\_\_\_\_ (Free text, 100 words max)

44. Do you have any other comments regarding how a compliance regime (inspection and enforcement) could operate?

\_\_\_\_\_ (Free text, 200 words max)

### Section 4: How should Government best support and work with partners?

45. Do you currently access Government advice (primarily from Counter Terrorism Policing and the Centre for the Protection of National Infrastructure) regarding threat, protective security and preparedness?

Y/N

[If 45 = Y]

46. What, if anything, do you find most valuable in current advice and guidance?  
\_\_\_\_\_ (Free text, 100 words max)

**[If 45 = N]**

47. Why do you not currently access this advice and guidance?

- a. I did not know it existed
- b. I do not think I need to address the threat
- c. I do not have the time to access this
- d. It is too confusing to find what I want
- e. Other \_\_\_\_\_ (Free text, 100 words max)

48. What would you find most useful to help you to comply with a Protect Duty (select all that apply)?

- a. A single, digital service where you could access relevant material, advice and training in one place
- b. Easy to digest information regarding threat and attack methodologies
- c. A risk assessment template
- d. Information on undertaking a risk assessment for terrorism threats
- e. Advice relating to protective security mitigations
- f. Advice relating to personnel and people security
- g. Advice relating to how an organisation can prepare for terrorism attack
- h. Advice on what constitutes reasonably practicable and appropriate mitigations appropriate for my circumstances
- i. Development of product certifications or standards for aspects of the approach
- j. Staff training and awareness courses
- k. E-learning products
- l. An App
- m. A sector meeting where I can talk about the Duty with experts and other similar organisations
- n. A local meeting where I can talk about the Duty with experts and other similar organisations
- o. Other: \_\_\_\_\_ (Free text, 100 words max)

49. Counter-Terrorism Policing are working with Government and the Private Sector to design a digital service to provide access to relevant counter-terrorism material, advice and training in one place for organisations operating in publicly accessible locations. Do you anticipate that you would access counter terrorism information through this service if it were available to you?

Y/N

**[If 49= N]**

50. Why not?

\_\_\_\_\_ (Free text, 100 words max)

**[If 49 = Y]**

51. What would you most likely use this kind of service for (tick all that apply)?

- a. To get general updates on how the terrorism risk is changing
- b. To support business planning activities

- c. To understand what risk management activities you need to do
  - d. To access CT training
  - e. To connect with other organisations to discuss counter terrorism
  - f. To understand what to do after an incident
  - g. Reporting of suspected terrorist activity/concerns
52. Do you have any further comments or suggestions for how you might like to access counter-terrorism information and work with local partners on counter-terrorism issues in the future?  
 \_\_\_\_\_(Free text, 100 words max)
53. What role should local business partnerships (such as Business Improvement Districts, Local Enterprise partnerships, etc.) have in supporting organisations and venues to deliver improved security?  
 \_\_\_\_\_ (Free text, 100 words max)
54. Working with others, what could the Government best do to incentivise improved security practices?  
 \_\_\_\_\_ (Free text, 100 words max)
55. To support the provision of high-quality advice and guidance from private sector security professionals providing counter terrorism security advice, Government should consider (tick all that apply)
- a. Government supported standards for Counter Terrorism (CT) risk assessments and advice
  - b. Qualifications / Accredited training for individual professionals
  - c. Government supported 'approved contractors scheme'
  - d. Regulation of CT consultants
  - e. None
  - f. Other \_\_\_\_\_ (Free text, 100 words max)
  - g. I don't know
56. What advice and support do you think would be required for organisations and venues within the scope of a Protect Duty?  
 \_\_\_\_\_ (Free text, 100 words max)
57. Given the complexity of public spaces, and the potential need for partnership working to achieve effective ways of working leading to improvements in protective security and preparedness, what additional bespoke support and expertise could be provided?  
 \_\_\_\_\_ (Free text, 100 words max)
58. Do you have any other proposals on what Government could do to support partners in the delivery of a Protect Duty?  
 \_\_\_\_\_ (Free text, 200 words max)





© Crown copyright 2021

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit [nationalarchives.gov.uk/doc/open-government-licence/version/3](https://nationalarchives.gov.uk/doc/open-government-licence/version/3) or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: [psi@nationalarchives.gov.uk](mailto:psi@nationalarchives.gov.uk).

Where we have identified any third-party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at [www.gov.uk/government/publications](https://www.gov.uk/government/publications)

Any enquiries regarding this publication should be sent to us at [public.enquiries@homeoffice.gov.uk](mailto:public.enquiries@homeoffice.gov.uk).