Government Response to the Intelligence and Security Committee of Parliament Report ‘The 2017 Attacks: What needs to change?’

Presented to Parliament
by the Prime Minister
by Command of Her Majesty

January 2019

CP 22

Government Response to the Intelligence and Security Committee of Parliament Report ‘The 2017 Attacks: What needs to change?’

Presented to Parliament
by the Prime Minister
by Command of Her Majesty

January 2019

CP 22

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at Cabinet Office, 70 Whitehall, London, SW1A 2AS

ISBN 978-1-5286-0966-1

CCS 0119361008 01/19

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office

INTELLIGENCE AND SECURITY COMMITTEE REPORT 'THE 2017 ATTACKS: WHAT NEEDS TO CHANGE?' GOVERNMENT RESPONSE

The Government is grateful to the Intelligence and Security Committee (ISC) for its continued independent oversight. On 22 November 2018, the ISC published its report 'The 2017 Attacks: What needs to change?', covering the terrorist attacks in Westminster, Manchester, London Bridge, Finsbury Park and Parsons Green which occurred in 2017. The Prime Minister acknowledged and thanked the ISC for the report in a Written Ministerial Statement on the same day. The report is thorough and comprehensive. This document provides further detail on the Government's response to each of the ISC's recommendations and conclusions contained in that report.

Our thoughts remain with the victims and all those affected by the attacks in 2017.
As the Prime Minister stated in her written ministerial statement to accompany the publication of the report, it is right that we look at what happened so that we have the best chance of preventing further attacks.

Significant progress has already been made, but further work is needed and we remain committed to continuing to address these issues. We can and will improve in these areas and we and the Committee recognise that a cross Government response is required to tackle the threat from terrorism. As well as CT Policing (CTP) and the UK Intelligence Community (UKIC), a range of Government departments are working on the response to the terrorist threat.

As well as the ISC's report, MI5 and CTP conducted their own independent reviews of the handling of intelligence relating to the Westminster, Manchester, London Bridge and Finsbury Park attacks to identify enhancements to their operational practices. These reviews were independently assessed by Lord Anderson of Ipswich. We welcome the Committee's recognition of the thoroughness of these reviews and the demonstration of commitment shown to continual improvement by MI5 and CTP. A review of the Parson's Green attack has also led to improvements in the implementation of the Channel programme.

Since the completion of the internal MI5 and Police reviews there have been significant efforts to implement their findings. This has happened alongside Government's wider efforts to tackle the threat from terrorism, including publishing a strengthened version of the UK's comprehensive counter-terrorism strategy, CONTEST, which reflects the findings of a fundamental review of all aspects of counter-terrorism, and builds on the lessons learned from 2017's attacks.

In addition, MI5 and Counter Terrorism Policing (CTP) initiated the Operational Improvement Review (OIR) in the wake of the 2017 Terror Attacks. This was also independently reviewed by Lord Anderson, who described it as "one of the most detailed examinations ever conducted of the UK's counter-terrorism machine and its operation". The OIR recommendations include commitments to significant change which are being overseen by teams in CTP, MI5 and HMG. MI5 have already started reporting their progress on these recommendations to the ISC as part of their Quarterly Reports.

As a result of these efforts since the attacks, significant improvements have already been made which relate to the ISC's recommendations. Areas where such progress has been made includes liaison with Communication Service Providers about online extremist material and regulation of precursor chemicals. The improvement work in these and other areas will continue in the months and years ahead. Lord Anderson will also provide a stocktake to the Home Secretary on the delivery of the OIR recommendations shortly.

The ISC have noted in their report that some of the recommendations from this report are similar to those made in previous reports, particularly their reports following the murder of Fusilier Lee Rigby and the 7/7 attacks. Much of this relates to the complex challenges inherent to counter-terrorism work, that the Government, CTP and UK Intelligence Community (UKIC) have been working hard to address over a number of years. We have committed to providing the Committee with a means of tracking the delivery of recommendations from the ISC's previous inquiries and we will work with them to provide the specific updates that have been requested in relation to this report.

<u>Responses to individual recommendations</u>

The ISC's recommendations and conclusions are set out below in **bold**, followed immediately by the Government reply.

A. This Committee was the first to identify – in its Report into the murder of Fusilier Lee Rigby – the problem of Communications Service Providers (CSPs) failing to remove extremist material from their platforms. In 2014, we urged Government to engage with the CSPs to get them to take action. Progress has been slow but we welcome the steps now being made by CSPs to automate the removal of extremist material.

The Government welcome the Committee's interest in this important area. Our aim is to make the online space a hostile environment for terrorists to operate, and to prevent

the dissemination of terrorist content online. CTP established a dedicated unit in 2010 to help to do this, the Counter Terrorism Internet Referral Unit (CTIRU).

Following the Westminster attack in March 2017, the former Home Secretary Amber Rudd convened a roundtable with major industry players, including Facebook, Twitter, Google, and Microsoft to see what more could be done to tackle terrorist content online. This led to the major companies setting up the Global Internet Forum to Counter Terrorism (GIFCT). As a result, these companies have expanded the use of automated technology to detect and remove terrorist content. For example, Twitter announced in April that, between July and December 2017, 274,460 accounts were suspended for violations related to promotion of terrorism, and of those suspensions 93% consisted of accounts flagged by internal, proprietary spam-fighting tools, while 74% of those accounts were suspended before their first tweet. Google announced that 81.4% of 7.8 million videos removed in Q3 2018 were flagged using automated technology, of which 74.5% had no views at the time of takedown. Facebook announced in November 2018 that it had taken action on 9.4 million pieces of Daesh and al-Qaeda content in Q2 of 2018, 99% of which was found proactively by Facebook.

These efforts are making it much harder for terrorists to disseminate propaganda. We continue to press the CSPs to focus more on automation, and to share their expertise and technology with smaller, less well-resourced companies.

B. Systems that the CSPs do put in place must ensure that law enforcement agencies are notified of any material that may have a national security threat element. Failure to do so will prevent early detection of potential threats.

The Government agrees that CSPs should ensure law enforcement agencies are notified of material that may have a national security element where relevant. This is a shared challenge and CSPs must step up to their responsibilities to ensure that their platforms are not being abused by terrorists and other serious criminals. We welcome the references to this in the draft EU Regulation on terrorist content online.

C. In return, Government should ensure that it takes a co-ordinated approach to the CSPs: rather than confronting them with competing messages, single points of contact will ensure consistency and simplify the relationship for the CSP.

The Government welcomes this assessment. We have worked to coordinate our approach to the CSPs. Relevant departments and agencies have their own single points of contact for liaison with CSPs, while CTP is the UK's single point of contact for referring terrorist content for removal to the CSPs.

At Ministerial level, the Home Secretary holds regular discussions with leaders of the relevant companies: he attended the GIFCT's Summit in San Francisco in June and met Sheryl Sandberg (COO, Facebook) and Kent Walker (General Counsel, Google and current chair of the GIFCT) to discuss progress in November. Now, as we develop the Online Harms White Paper, the Home Office holds coordinated meetings with the CSPs jointly with DCMS to consider the whole range of online harms. We hope to build on this with better prioritisation of Government's asks in the future.

D. We particularly note the impact that recent action from advertisers such as Unilever has had in encouraging the CSPs to take action. Where reputational levers have failed to produce action, financial levers could provide the solution. We commend these companies and would encourage other major companies to follow their lead.

E. Government should now seek to lobby the business community to take action, following the Unilever example. This is a matter on which we expect a full report from the Government on what action has been taken with the business community within the next six months.

Joint response to D and E

As part of the Government's work to prevent the dissemination of terrorist content online, the Home Office has been engaging with wider industry stakeholders, in addition to the major social media companies. We recognise in particular the important role advertisers can play in this area. The Home Office and CTP CTIRU have been engaging with the advertising industry to make them more aware of the kinds of illegal terrorist content that is appearing on social media platforms and highlight that their advertisements may unknowingly be appearing next to this unacceptable content. This was thrown into sharp relief in March 2017, when a number of major global brands and high profile advertisers withdrew advertising from YouTube after they were found to be appearing next to videos promoting extremist views. Working with advertising trade bodies such as Incorporated Society of British Advertisers (ISBA), we are calling on social media companies to identify and remove terrorist content quickly and to encourage a more responsible advertising marketplace. The Home Secretary held a roundtable in December with representatives from the advertising industry to address this issue, alongside other illegal content online. We commit to share a report on this area of work with the ISC within the next six months.

F. The ISC recommended in its 2014 Report into the murder of Fusilier Lee Rigby that more should be done to prosecute those accessing extremist material online. We are disappointed to note that the last four years have seen no progress on this issue. The Government must ensure that the Counter-Terrorism and

Border Security Bill, when passed, tackles those who view extremist material online, as well as those who disseminate it.

The Government is seeking to update the law through the Counter-Terrorism and Border Security Bill, so that it is an offence to view or access terrorist material online. The proposed changes will strengthen the existing offence under section 58 of the Terrorism Act 2000 so that it will apply to material that is viewed or otherwise accessed online. This Bill has neared completion of its parliamentary passage and is expected to gain Royal Assent shortly.

G. We support the intention expressed in the Internal Reviews to improve the Approved Visitor Scheme in relation to Category A prisoners – although clearly this is dependent on the detail of any measures to be implemented. We expect this detail to be provided by the Government within the next 12 months.

The Government notes and accepts this recommendation. As the committee notes, work is ongoing to strengthen controls around communications and visits for Category A prisoners. The Government will report back to the Committee within 12 months on the outcome of that work.

H. The monitoring of visitors to extremist prisoners below Category A is haphazard. This is concerning: it allows known extremist prisoners to potentially maintain links with those vulnerable to extremism. The Government should consider expanding the Approved Visitor Scheme to include all extremist prisoners.

The Government accepts this recommendation and is undertaking work to address this issue alongside recommendation G. Her Majesty's Prison and Probation Service (HMPPS) is working with partners to explore the potential to expand the Approved Visitor Scheme to include all extremist prisoners that present a risk to the community. The Government will report back to the Committee within 12 months on the outcome of that work.

I. It would be wholly inappropriate for prisoners who convert to Islam to be subject to routine monitoring. Nonetheless, prison officers must be trained to identify instances where someone has converted following association with extremists, to assess whether that conversion is therefore part of a positive journey or a negative one for an individual, and to be able to take action in the latter case.

The Government accepts this conclusion. Training prison staff to recognise and deal with the signs of extremism is an important part of our approach to countering terrorism and extremism in prison and over 19,000 prison staff have been trained since

2016. Additional counter-terrorism training for HMPPS Muslim Chaplains is underway to better equip them to challenge and address extremist behaviour and attitudes in prison, which includes identifying concerns around conversions. Those prisoners who do demonstrate concerning behaviours or vulnerabilities are referred for specialist case management.

Finally, the Government recognises the importance of faith and the positive impact that it can have on the lives of offenders. We also recognise the need for a clear distinction to be made between 'conversion' and 'radicalisation' – the vast majority of offenders who convert to Islam do so for positive reasons.

J. While the Committee recognises the sound intention behind segregating extremist prisoners, we are concerned that the new Separation Centres may also provide a networking opportunity for extremists. We urge Government to keep this risk under review, and take what steps it can to minimise it. We expect to see the results of this review in 12 months' time.

The Government notes the Committee's concern. Separation Centres were introduced 18 months ago as an important safeguarding capability. The small number of prisoners in Separation Centres have been removed from the mainstream population because their behaviour presents challenges and risks to fellow prisoners that cannot otherwise be managed. Reviews at 6 and 12 months found no evidence to suggest that prisoners in Separation Centres are actively attempting to develop new networks. However, the Government recognises the potential risks associated with the centres, and will continue to closely monitor and periodically review them to determine their impact on the terrorist and extremist risk in prisons. We will provide the Committee with a report within 12 months' time.

K. We are encouraged by witnesses' evidence that those organisations involved in managing, and gathering intelligence on, extremist prisoners are working well together. Nonetheless, we remain concerned that the number of organisations and teams working in this area makes it a crowded space. The Government should keep this matter under review and we expect a report on whether it is still working well in the next 12 months.

The Government notes the Committee's concern. The creation of the Home Office and HMPPS Joint Extremism Unit (JEXU) in 2017 has provided the single co-ordination point for the delivery of counter terrorism in this sector and has enabled closer working between all of the relevant agencies. The Government agrees that this is currently working well.

It is essential that this close collaboration continues, to ensure we are effectively tackling current and emerging threats. The Government will keep this under review and provide a report on this issue to the Committee within the next 12 months.

L. Whilst there may be some merit in increasing *, the Committee is conscious of the limitations of this capability. We query whether resources may be better served in seeking alternative solutions.**

The Government notes the ISC's concern regarding the limitations of this capability and have recognised this issue. Alternative solutions are being explored.

M. Given the propensity for vehicles to be used as weapons, monitoring vehicle hire must be a significant element of counter-terrorism work. The Committee is encouraged that the Department for Transport and the Home Office are working on a new system to improve the information provided by vehicle hire companies. However, we are concerned that the * of the proposed scheme significantly reduces the likelihood of its success.**

The Government notes this conclusion. On 6 December 2018 the Department for Transport launched the Rental Vehicle Security Scheme. Companies joining the scheme commit to implementing a ten point code which promotes security awareness and checks, vigilance and co-operation with law enforcement. This includes designating a company security contact and training staff in reporting suspicious behaviour.

All vehicle hire companies are encouraged to join the scheme. The scheme has been developed in collaboration with vehicle hire sector leads and industry associations and is supported by the Centre for the Protection of National Infrastructure. The Government will keep the take up and impact of the scheme under review, including the case for putting security measures on a mandatory footing.

N. The previous system for regulating and reporting purchases of the ingredients used to make explosives such as TATP (triacetone triperoxide) and PETN (pentaerythritol tetranitrate) was out of date in dealing with the threat at the time. The Manchester Arena bombing showed this to devastating effect. We therefore welcome the updates to the current system of regulating and reporting explosives precursor purchases.

The Government notes this conclusion and is committed to continuing to develop the system of regulating and reporting explosives precursor purchases.

O. The Committee notes that the proposed changes to the system will result in a considerable increase in the volume of data generated. We are concerned that there must be sufficient resources to deal with this increase in data. The Home

Office must ensure that proper support is in place *: we expect to see an analysis of what is required within the next six months.**

The Government notes this recommendation. Work is already taking place to ensure that appropriate resource is allocated to this important task and that we are able to monitor the impact of our work.

P. We are pleased to hear that progress is being made to develop relationships between retailers and the counter-terrorism network: again, this is overdue.

The Government has been developing relationships between retailers and the counter-terrorism network over a number of years and continues to prioritise this vital work. We welcome the recognition of its importance.

Q. Whilst there are changes that can – and should – be made to the current arrangements around the regulation of chemicals used in explosives, it is not possible to prevent all purchases: at a certain point the benefits that can be gained from successive tightening of the system will become marginal.

The Government notes this conclusion.

R.***

S.***

T.***

These recommendations were redacted from the public report. A closed response will be submitted to the Committee separately.

U. The Committee has raised concerns about the need for improved joint working between MI5 and CTP for over ten years. Improvements have been made but we note that this is an area that requires continuous improvement.

V. Further issues that MI5 and the police might consider are: how to ensure comprehensive dissemination of information from MI5 to CTP; cultural change to support the new structures in place to facilitate closer working; and a renewed impetus to resolve the problems caused by incompatible IT systems.

Joint answer to recommendations U and V

The Government welcomes the acknowledgement that progress has been made in joint MI5 and CTP working over the last ten years.

CTP and MI5 have an outstanding track record of working together to counter the threat from violent extremists who believe they can advance their aims through acts of

terrorism. MI5 and CTP know that they are most effective when they work together, and with partners in HMG, combining their distinctive expertise and strengths.

The current threat from terrorism is intense – operating at a scale and pace not seen before, and evolving rapidly. MI5 and CTP have built a joint operational model that has proven its effectiveness against threats of many sorts.

Since 2011, the joint Intelligence Handling Model (IHM) has provided a framework by which, together, they have identified and developed reporting about new threats and risks and ensured that finite resources are directed against the most credible leads and investigations. This model has been adapted and improved in 2018, implementing changes proposed in the OIR and further changes have been made to the way in which MI5 and CTP jointly manage priority investigations. Increasing co-location of CTP and MI5 teams serves to further strengthen this collaboration.

The implementation of recommendations under the OIR is driving further improvements for both organisations. MI5 and CTP are making progress in all of the areas identified as part of Recommendation V. Through the CT Step Up programme, MI5 and CTP, along with GCHQ and SIS, are committed to sharing knowledge within the UK CT community to have a single, shared understanding of subjects of interest (SOI), capabilities and objectives, making it easier to share, access and enrich each organisation's information. MI5 and CTP, along with the wider intelligence community, work closely to agree shared priorities and objectives, and to continue to build collaborative ways of working, governance and IT infrastructure to achieve this.

W. The Committee welcomes the number of initiatives focused on improving the flow of information between MI5 and CTP; however, it is important that this results in real, practical change. The Committee expects a report on how this is working and what tangible benefits have been seen in six months' time.

The Government acknowledges this conclusion and will provide an update to the Committee in six months.

X. The Committee considers that the Government failed to tackle the leaking of information about the Manchester Arena attack sufficiently robustly. Leaking our information – and potentially causing distress to the victims and families in so doing – will not be tolerated. The US administration recognised the seriousness of the situation and we welcome the thorough investigation they undertook.

The Government engaged repeatedly at senior levels with the US Government on this issue, and they have (as the ISC note) recognised the seriousness of the matter. We welcome the conclusion of the US Government investigation.

Y. The Emerging and Residual Threats system, CLEMATIS and DAFFODIL all clearly represent major steps forward in MI5's management of Closed Subjects of Interest (SOIs). We support improving these operations yet further, including progressing the Science Advisory Council's recommendation that CLEMATIS should be run *. We also support MI5's current work to categorise its entire pool of Closed SOIs into risk bands and to treat the higher-risk individuals accordingly, although we were surprised to learn that they had not already been subject to such categorisation.**

MI5 and CTP have always faced – and will continue to face - the challenge of balancing the deployment of resource to current investigations and monitoring the residual risk posed by individuals who have been previously subject to investigation. This is one of the enduring challenges for counter terrorism. It is also important to note that the vast majority of those responsible for the 27 Islamist plots disrupted since 2013 were SOIs under active investigation.

Since the 7/7 terrorist attacks, each new iteration of the solution is an improvement on the last. This is a complex and challenging problem for which there is no perfect or simple solution. The increasing volume of this lower level risk requires increasingly active management. The intelligence community and CTP have committed to deliver against this through better acquisition, analysis and sharing of data and improvements in the CLEMATIS and DAFFODIL tools.

There are a number of challenges to running the CLEMATIS and DAFFODIL processes. While investments are being made to improve the process, these will take time to develop and implement, as will securing adequate resources to manage this work alongside existing operational pressure.

Z. From the date of his phone number first appearing on the periphery of an investigation, it took MI5 over six years to identify Khalid MASOOD. This is despite email addresses and phone numbers, which we now know to have belonged to him, being in contact with known extremists on numerous occasions, and his being mentioned in reporting. Whilst we recognise that 'joining the dots' between thereto-unconnected pieces of information and identifiers is a highly complex task, we nonetheless urge MI5 to consider what more can be done to connect those seen on the peripheries of investigations.

MI5 and CTP have increased their focus on 'discovery', to identify those who are engaging in activity of national security concern, which may include those who appear on the peripheries of existing investigations. As part of the CT Step Up programme, MI5 and CTP are aiming to proactively discover and identify new SOI and identify shifts and abnormalities in behaviour which may indicate a changing threat.

MASOOD first came to MI5's attention when his telephone number appeared in the contacts list of another subject of interest. MASOOD appeared to have no direct connection with the plot that individual was involved in. MASOOD then appeared on the periphery of investigations. These factors do not necessarily meet the threshold for further action.

Recent changes to the Intelligence Handling Model provide advice as to how to manage risk where individuals have links to existing SOI. MI5 and CTP will continue to assess all incoming intelligence on a case by case basis in line with this model.

AA. We are encouraged that the CLEMATIS process correctly identified SALMAN Abedi as being of concern. However, there is clearly a problem in terms of timescales: in this case, the activity which had triggered the concern *. Had he been flagged and considered for referral sooner, then SALMAN might have been subject to investigation under DAFFODIL before he committed an attack.**

The Government notes the ISC's conclusion. We consider that it is inherently difficult to speculate on what would have happened if this process had moved more quickly. Thorough reviews conducted by MI5 and CTP did not identify any points where a different course of action would have been likely to lead to a different outcome.

Nonetheless, changes have been implemented to this system to improve timescales, specifically including increasing the amount of resource dedicated to this area, which may improve our ability to identify re-engagement of Closed SOIs. However, this will remain a challenge, as individuals will continue to look for ways to obfuscate their behaviour from the authorities.

BB. Overall, it is clear that MI5 are now taking serious steps to improve their management of Closed SOIs, and we welcome this. It is disappointing, however, that previous recommendations of this Committee have clearly not been taken on board until now.

Closed SOIs pose a challenge for MI5 and CTP. Within the numbers of Closed SOIs, there are individuals who have been the subject of malicious reporting, those whose activity has not been corroborated and those who have ceased engaging in activity, or have been disrupted. Given the wide range of SOIs, MI5 and CTP cannot and should not apply a "one size fits all" approach to Closed SOIs, and actions taken should be proportionate to the intelligence received and the threat that the individual is assessed to pose. Serious steps to address the challenge of Closed SOIs had already been taken prior to the 2017 attacks, notably through the existence of the CLEMATIS process. Further changes have already been implemented as a result of the OIR

recommendations, and a new team was stood up with sole responsibility for Closed SOIs.

MI5 and CTP must balance the deployment of their resources against Closed SOIs with the impact this has on their ability to investigate and disrupt live SOIs. The ISC has previously recognised the risk within the pool of Closed SOIs, however the Government does not accept that these recommendations were not taken on board. This is something that MI5 and CTP have been acutely aware of, as is illustrated through their commitments as part of the OIR, but their primary focus is rightly on those SOIs whom intelligence suggests pose the greatest threat.

CC. SALMAN Abedi should have been subject to travel monitoring and/or travel restrictions. *, MI5 should have put alternative measures in place to alert them to SALMAN Abedi's movements.**

DD. The Committee notes MI5's assessment that had SALMAN Abedi been placed under travel restrictions, there still may not have been sufficient time to identify or act on his attack planning. It would, nevertheless, have provided more of an opportunity.

Joint response to CC and DD

Though choices made at the time were rational, MI5 recognises that, with the benefit of hindsight, it would have been the better course of action to subject SALMAN to travel monitoring. It is inherently difficult to speculate if this could have helped to identify SALMAN's activity. It is also unlikely that, given the intelligence picture at the time, MI5 would have been able to secure restrictions on SALMAN's travel.

However, thorough reviews conducted by MI5 and CTP, independently assured by Lord Anderson, did not identify any points where a different course of action would have been likely to lead to a different outcome.

EE. The Committee supports the policy change being implemented by MI5 and CTP in respect of the use of travel monitoring for Closed SOIs. We note, however, the impact that these changes will have on day-to-day resourcing: both organisations will need to assess these during the implementation phase.

Both MI5 and CTP are aware of the potential resourcing ramifications in relation to the policy changes they have implemented.

While it would not be appropriate to comment on specifics of these policies, where necessary and proportionate MI5 and CTP are looking to identify signs of re-engagement within the Closed SOI pool, which may include travel.

FF. Regardless of operational demands, an eight-week delay between the receipt of a trace request from a partner agency and onward dissemination is far too long. Delays of this nature could have a very significant impact on an operation, not just here in the UK but in other countries too.

The Government notes this conclusion. SIS have updated guidance in consultation with MI5 regarding the appropriate and timely dissemination of information or requests from foreign liaisons, providing a clear set of handling guidelines concerning responsibilities towards data and issuing tactical reporting. SIS has also taken steps to ensure officers deployed overseas have been trained in these processes and are upskilling overseas officers with language capability. SIS is also looking to increase the ability for partners to communicate with UKIC directly.

GG. The Committee acknowledges the difficulties of working with partners with different organisational structures and ways of working. We welcome the progress made during the UK's Presidency of the Counter Terrorism Group on national security collaboration: the UK's exit from the EU must not impact on the information-sharing relationships and powers currently available to the UK intelligence community.

The UK Intelligence Community (UKIC) and CTP remain committed to cooperating with European partners to counter National Security threats. This commitment to intelligence sharing and operational cooperation is unconditional and will not decrease after the UK leaves the EU. The Political Declaration, agreed between the UK and EU, sets out the framework for future security cooperation and specifically protects the ability of the UK and EU to continue '*intelligence exchange on a timely and voluntary basis*' (paragraph 105).

It has always been the UK's position that National Security is a matter for Member States, not the European Union. This is enshrined in Article 4(2) of the Treaty for the European Union which states that National Security is a matter for Member States exclusively. The Political Declaration also seeks to protect this principle at paragraph 136, '*The future relationship should provide for appropriate exceptions regarding security; national security is the sole responsibility of the Member States of the Union and the United Kingdom respectively*.'

Core collaboration between the UK and European partners on matters of mutual National Security occurs outside EU mechanisms, both through long standing bilateral relationships, many dating back decades and multilaterally through mechanisms such as the Counter Terrorism Group (CTG) of 30 European Intelligence and Security Services.

HH. The Committee is reassured to see the Agencies have taken on board our previous recommendation that the Behavioural Science Unit be better integrated into the investigative process. We expect to be kept updated on progress, with a full report on this matter in 12 months' time.

The Government welcomes this conclusion and will report to the Committee in 12 months' time.

II. SALMAN Abedi should have been considered for a Prevent referral after his closure as an SOI in July 2014. It is concerning that there is no evidence of a discussion between CTP and MI5 as to a potential referral.

JJ. The Committee is surprised that at no point were any members of the Abedi family referred to the Prevent programme – *. It is highly disappointing that Prevent was, once again, not applied to SOIs who later went on to instigate an attack – an issue this Committee has previously criticised.**

Joint response to II and JJ

SALMAN Abedi was only briefly investigated in 2014, when he was was identified as a candidate for an individual acting suspiciously; this was later discounted. MI5 and CTP are continuing to improve the way in which Prevent is considered at the conclusion of an investigation. However, it is purely speculative whether such a referral would have had any effect, or even whether SALMAN would have engaged with a Prevent referral.

MI5 have reinforced their closure processes, which includes directing investigators to give greater consideration to proportionate closing actions, including PREVENT referral where appropriate. Guidance for Joint Operational Team meetings also encourages MI5 and CTP to consider and discuss Prevent engagement at the start and throughout an investigation.

Separately, as part of the refreshed CONTEST strategy, MI5, CTP and Home Office are piloting new operational approaches, including the experimental Multi-Agency Centre (MAC) pilots which aim to test different models to better understand risk around individuals who have been subject to active national security investigations.

The multi-agency centre pilots will use information sharing to improve understanding of individuals and how we might support them. Information sharing will be proportionate and appropriate to understand the risk people pose and opportunities to intervene and will be based on existing legislation and processes. Any intervention taken forward will be with the aim of managing the risk of an individual re-engaging in violent extremism or terrorism.

KK. The Committee considers the Home Office's failure to provide evidence relating to Ahmed HASSAN's case such that the Committee could consider it as part of this Inquiry as unacceptable. There are a number of fundamental failings in the handling of HASSAN's case: the Committee hopes that the Home Affairs Select Committee will instigate a thorough review of the Prevent programme in relation to this case.

The Government accepts that there were deeply regrettable errors made in the handling of Ahmed HASSAN's case, and that our response to the Committee did not meet its expectations. The lessons from the case were identified, and recommendations made to address them, by an independent review into the case, which was jointly commissioned by Surrey County Council and CT Police HQ. All parties have acted swiftly to implement, where appropriate, the recommendations made.

Sir Philip Rutnam's letter to the Chairs of the Home Affairs Select Committee (HASC) and the ISC of 18th June, which was also made public, set out a summary of the review, the recommendations, and the action taken to address them. In addition, many of the lessons coming out of this case relate to the need for improved information sharing between local and national agencies, which is a strong theme which has emerged from all of last year's attacks, and which is being addressed through a number of projects and initiatives coming out of the Operational Improvement Review, such as Multi-Agency Centres.

Other on-going work to improve the delivery of the Channel process (a voluntary initiative that provides a multi-agency approach to support vulnerable people being drawn into terrorism) includes increased training for those involved in Channel, and a pilot project to shift responsibility for much of the information gathering and assessment work from the police to local authorities, which will also improve consistency of delivery by allowing panel chairs to draw on regional hubs of expertise. Given all the work which has so far taken place to understand and learn from the mistakes made in this case – including an independent review – the Government does not agree that a further review into this case by the HASC would achieve more than has already been achieved. Furthermore, the Government has now agreed (as part of the Counter-Terrorism and Border Security Bill) a formal independent review of Prevent. While the exact shape of this review is yet to be agreed, consideration of known successes and areas for improvement is likely to form part of it.

LL. Although we are encouraged by OSCT's reports of positive engagement on counter-terrorism issues by the owners of public places, we remain concerned that there appears to be no way of mandating owners of public places to install necessary protective security measures where they do not do so voluntarily. This

issue becomes yet more difficult where sites have multiple owners. The Government should consider clarifying the legal responsibilities of both site owners and relevant public authorities in this regard.

The Government notes this conclusion. There is extensive advice and guidance on threat methodologies and their mitigation to those responsible for crowded places. We continue to consider how we can make this more user friendly, and engage more effectively with the range of responsible parties, to achieve effective and consistent security outcomes.

This advice reaffirms existing responsibilities, however a decision to mandate protective security and preparedness measures needs to be carefully weighed against the proportionality of establishing such a requirement in light of the threat and the impact such a decision would have on all affected parties.

The Government keeps this matter under regular review to ensure that our strategies deliver effective protection of the public through appropriate and proportionate security measures. As the most recent publication of CONTEST notes, this includes potential legislative measures.

MM. We understand that well-known places are particularly attractive targets for terrorists, and that making them harder targets therefore makes sense. Nonetheless, we recommend that Government remains cognisant of the displacement risk, and in each case carefully considers whether or not to install barriers: it is neither practical nor desirable to install such measures at every potentially crowded place in the UK.

The Government notes this conclusion. The Government provides expert advice to responsible parties to assist in the development of both appropriate and proportionate protection measures. Parties responsible for security at crowded places locations are encouraged to work on mitigations with those responsible for locations which are their immediate neighbours, where it is feasible and appropriate to do so. This is particularly pertinent when considering measures to combat vehicle borne threats, where working on a wider scheme will often be more cost effective and efficient than undertaking a number of smaller schemes.

We accept and agree that it would not be appropriate for hostile vehicle mitigation measures to be developed at all crowded places. Expert resource helps responsible parties to make decisions on where such mitigations would be appropriate on a permanent or temporary basis.

NN. Even with the most comprehensive training available, it is not clear that Manchester Arena staff could have been expected to identify SALMAN Abedi's behaviour on either of his two visits to the attack site as suspicious. Nonetheless, we support Government's efforts to ensure that those working at major venues are trained to spot suspicious activity.

The Government welcomes this conclusion. A fundamental part of our strategic approach and delivery activity is the provision of a variety of advice and awareness raising activity regarding terrorist threats and their mitigation, and to deny, detect and deter those with malicious intent.

This includes: police operational decisions to deploy at high profile locations to identify and disrupt hostile reconnaissance and a wider range of criminal activity; a range of communications and awareness raising activity through the CTP Action Counters Terrorism initiatives for different audiences; and approaches for sites/organisations to use their existing resources to create a sustained, disruptive environment to deny, detect and deter hostile reconnaissance activity.

OO. The Committee welcomes the new initiative to share intelligence beyond the traditional boundaries in order to strengthen the ability to connect information. This will nevertheless place an additional burden on frontline services already under pressure. We encourage the Government to ensure that this change is sufficiently resourced.

The Government accepts this recommendation. Pilot funding includes support for participating local authorities and covers the cost of any locally delivered interventions. The overall evaluation of the pilots will include an assessment of potential future funding requirements, should the pilots be successful.

The Government recognises the importance of local policing and its role in crime prevention and counter-terrorism. We are continuing to support general policing to ensure change is sufficiently resourced.

We are proposing total funding of up to £14 billion for 2019-20, an increase of up to £970m compared to 2018/19, including precept, pensions funding and national investment. Our commitment to support the police to deliver for the public is for the long term and we are prepared to invest appropriately at the next Spending Review.

In the Autumn budget the Chancellor announced an additional £160m for counter-terrorism policing for the coming financial year (2019-20), a year-on-year increase of £59m, to ensure that police across the country are well equipped to work closely with our communities and keep citizens safe. This takes counter-terrorism policing annual funding to over £800m.

PP. The Committee welcomes the Agencies' proposals to use data in a more innovative way. We are encouraged by MI5's commitment to work with industry and academia to help in the design and delivery of this and believe this partnership has the potential for significant skill and capability transfer. These changes are very much in the initial design stages, however, and we will wish to see how they develop.

The Government welcomes this conclusion and are developing plans to ensure this work progresses, including a strategy for acquiring, analysing and sharing data across intelligence and policing along with increasing cooperation with the private sector. The UKIC will provide the ISC with further detail on these proposed plans in due course.

QQ. The Committee notes the increased pressure that the changes in the Agencies' use of data will have on existing capabilities and fully supports the proposed sharing of analytical expertise across the organisations. It is encouraged by the Agencies' commitment to the establishment of a more defined Analyst career path and hopes that this will encourage greater retention of staff.

The Government welcomes this recognition. The UKIC will keep the ISC updated on the improved Analyst career path.

CCS0119361008

978-1-5286-0966-1