Witness Name: JONATHAN EMMETT

Exhibits: [JE/01-JE/125]
Dated: 31/07/2026

THE SOUTHPORT INQUIRY: PHASE 2

FIRST WITNESS STATEMENT OF JONATHAN EMMETT

INTRODUCTION **3**

(A) ROLES AND RESPONSIBILITIES - OVERVIEW **7**

HOME OFFICE 7
Homeland Security Group *7*
Public Safety Group (PSG) *10*
Digital and Innovation Group *11*
The Security Service *12*
CABINET OFFICE (CO) 15
Economic and Domestic Affairs Secretariat (EDS) *15*
National Security Secretariat (NSS) *16*
National Security Council (NSC) *16*
T1D - Cabinet Office Body *16*
T1D *16*
FORMER DEPARTMENT FOR SCIENCE, INNOVATION AND TECHNOLOGY (DSIT) 17
Security and Online Harms Directorate *17*
Government Office for Science (GO-Science) *17*
DEPARTMENT FOR DIGITAL, CULTURE, MEDIA AND SPORT (DCMS) 17
DEPARTMENT OF HEALTH AND SOCIAL CARE (DHSC) 17
MINISTRY OF JUSTICE (MoJ) 18
Youth Justice Policy Unit *18*
Counter-Terrorism Assessment and Rehabilitation Centre (CT-ARC) *18*
MINISTRY OF HOUSING, COMMUNITIES AND LOCAL GOVERNMENT (MHCLG) 18
DEPARTMENT FOR EDUCATION (DfE) 19
COUNTER TERRORISM POLICE HEADQUARTERS (CTPHQ) 19

(B) NIEV POLICY LEADERSHIP – OVERVIEW **19**

CONTEXT 19
COUNTER-TERRORISM DIRECTORATE LEADERSHIP 20
2025 ARRANGEMENTS 21
VFI Unit (March – October 2025) *21*
Violence Fixated Individuals Analytical Group (VFIAG) *22*
NSC *22*
ARRANGEMENTS ESTABLISHED IN 2026 22
NIEV Taskforce (cross government) and NIEV team (Home Office) *22*
Overview of NIEV Taskforce governance *23*
NIEV Team *24*

(C) EXISTING ARRANGEMENTS RELEVANT TO THE NIEV RISK 25

PREVENT 25
Overview 25
Guidance and training 27
Information sharing 31
COMMUNITY SAFETY PARTNERSHIPS (CSPS) 32
VIOLENCE REDUCTION UNITS (VRUS) 33
YOUNG FUTURES PANELS 34
MULTI-AGENCY SAFEGUARDING HUBS (MASH) 35
MAPPA 36
OTHER POTENTIALLY RELEVANT SERVICES 37

(D) NARRATIVE SUMMARY OF HMG INITIAL POLICY DEVELOPMENT WORK 38

JULY 2024 – JANUARY 2025 39
JANUARY 2025: POST SENTENCING POLICY PACKAGE 40
MARCH 2025: NATIONAL SECURITY COUNCIL ACTIONS 41
CROSS-GOVERNMENT WORK TO SUPPORT ACTIONS SET BY THE NSC AND THE VFIAG 47
NSC PROGRESS UPDATE 54
RESPONSE TO SOUTHPORT INQUIRY PHASE 1 RECOMMENDATIONS 55

(E) KEY THEMES AND CHALLENGES 55

DEFINITIONS, CHARACTERISTICS AND RISK FACTORS 55
Definition of the harm we are seeking to address 55
Working definition of Non-Ideological Extreme Violence (NIEV) 56
Risk factors and characteristics 58
SIZE OF THE COHORT 60
NEURODIVERSITY, MENTAL ILL HEALTH AND NIEV RISK 62
Relationship between neurodiversity, mental health and risk 62
Operational challenges 64
THE IMPACT OF EXTREME VIOLENT CONTENT ONLINE 65
EFFECTIVENESS OF INTERVENTIONS TO PREVENT NON-IDEOLOGICAL EXTREME VIOLENCE 65
LIMITATIONS OF POWERS TO REQUIRE ENGAGEMENT OR IMPOSE INTERVENTIONS 66
DATA AND INFORMATION SHARING 67
REGIONAL VARIATION 69
LAW ENFORCEMENT CHALLENGES 69

(F) THE ROLE OF THE INTERNET AND SOCIAL MEDIA 70

EXTREME VIOLENCE CONTENT (EVC) ONLINE 70
THE EFFECT OF ONLINE PLATFORMS AND COMMUNITIES 73
PATHWAYS FROM ONLINE ACTIVITY TO REAL-WORLD HARM 75
SHARING OF INFORMATION BY POLICE, PREVENT AND OTHER AGENCIES ABOUT ONLINE BEHAVIOUR 77
EXISTING WORK ON ONLINE HARMS IN RELATION TO TERRORISM 78
Reducing exposure to online content which is used to radicalise, recruit, or incite terrorism 79
Reducing permissive online spaces which allow for terrorist and extremist activity 82
Identifying individuals susceptible to radicalising narratives, in order for the appropriate support to be provided 83
Challenges in identifying concerning patterns of online behaviour 85
CURRENT WORK ON ONLINE HARMS IN RELATION TO NIEV 86
The National Security Bill 86
Takedown powers 89
The OSA and potential amendment or extension to its powers or duties 91
Social Media Ban 95
Device level interventions 97
LONGER-TERM OR WIDER WORK ON ONLINE HARMS OF POTENTIAL RELEVANCE TO NIEV RISK 98
Age verification for VPNs 98
Restricting certain aspects of online access for children in schools 99

Potential civil orders *100*

(G) MEASURES THAT HAVE BEEN IMPLEMENTED OR ARE BEING DEVELOPED **100**

HOMELAND SECURITY GROUP 101
Prevent Thresholds Review *101*
Addressing violence fascination risk in individuals who are suitable for Prevent support *103*
The Prevent system's role in managing violence fascination risk in individuals who are offered Prevent support, but do not consent *113*
Addressing the risk from NIEV risk individuals who are not suitable for Prevent support *114*
Oversight and assurance of Prevent's role in managing the risk from violence fixated individuals *116*
The Prevent system's role in supporting risk management in Pursue casework where violence fascination may be a concern *117*
Emphasis on multi-agency working *117*
PUBLIC SAFETY GROUP 118
Knife Crime *118*
Young Futures Prevention Partnerships *118*
WIDER GOVERNMENT 119

(H) LONGER TERM REFORM – CONSIDERATIONS AND CHALLENGES **120**

DESIGNING AN APPROACH – OVERVIEW OF HOME OFFICE POSITION 121
PROS AND CONS OF POTENTIAL CHANGES TO EXISTING ARRANGEMENTS OR DEVELOPMENT OF NEW MECHANISMS.... 124
A NATIONAL PREVENTION GATEWAY OR 'BIG FRONT DOOR' 131
WIDER WORK THAT WILL INFORM CONCLUSIONS 134
The harm we are seeking to prevent *134*
Equipping frontline services to identify NIEV risk *134*
Understand referral routes *135*
Ability to assess risk *136*
Ownership of risk *137*
Case management *138*
Interventions *139*
LEGISLATIVE OPTIONS 140
Expanding the remit of existing multi-agency structures *140*
Prioritisation due to public protection risk *141*
Consent and mandating engagement via civil orders *141*
General public protection duty *142*
Duty to Warn *143*
ONLINE INFORMATION ENVIRONMENT 143
A Strategic Approach *143*
Specific Areas of Concern *144*

CONCLUSION **149**

STATEMENT OF TRUTH **150**

INTRODUCTION

1. I am the Director of Counter-Terrorism at the Home Office, a post I have held since November 2025. Immediately prior to that I was the Director for CONTEST (the UK's Counter-Terrorism Strategy) and Homeland Security Strategy for a period of four years. I joined the Civil Service in 2000 and since 2002 I have held roles relating to counter-terrorism and national security in a variety of UK Government Departments, including in the Cabinet Office, Home Office and Foreign, Commonwealth and Development Office.

I lead the Counter-Terrorism Directorate which leads and coordinates delivery of CONTEST and is also responsible for delivering key elements of the Prevent and Pursue strands of that strategy. In addition to my counter-terrorism duties I am responsible for overseeing policy development on non-ideological extreme violence (NIEV) and Violence Fixated Individuals (VFIs).[1] I am a core member of the CONTEST Counter-Terrorism Strategy Board, I chair the Prevent and Pursue System Boards and I also chair the recently established NIEV Taskforce Strategic Delivery Board (see further paragraph 69 below).

2. The horrific attack in Southport raised and continues to raise serious issues for Government. A key issue, the failure of local public bodies to work together to identify or manage the risk posed by AR, has been the focus of much of the evidence the Inquiry heard in Phase 1. In Phase 2 the Home Secretary has asked the Inquiry to look more widely at, and to consider recommendations in respect of, other issues that form part of the context in which this terrible tragedy occurred:

    1) The limitations of existing multi-agency systems to manage non-ideological extreme violence.

    2) The role of the online environment in influencing, accelerating and facilitating extreme violence.

    3) The effectiveness of the current laws and systems for identifying, monitoring and disrupting the activities of VFIs online and reducing the harm caused by online spaces which promote extreme violence.

    4) The effectiveness of policies and regulation in relation to the sale and possession of offensive weapons and articles with a point or blade.[2]

3. As this statement will set out, following the attack, and in particular since AR's conviction, there has been a significant amount of work done by His Majesty's Government (HMG) to analyse the current position regarding identifying and managing the risk of non-ideological extreme violence and to identify related problems or gaps, steps that can and should be taken now and options for the future. That work is a cross government effort,

[1] Paragraph 7 below addresses terminology
[2] See: https://www.southport.public-inquiry.uk/southport-inquiry-terms-of-reference-phase-2/

coordinated primarily by the Home Office, but also by the Cabinet Office. The product of that work enables HMG to assist the Inquiry with what is known and unknown, where there appear to be gaps, the most significant obstacles and challenges, and options for reform that have been and are being considered. It is hoped the analysis and work that has already been done will provide the Inquiry with a framework to assist its investigations. A separate witness statement has been provided by Nicholas Hunt, Deputy Director of Firearms and Weapons Policy in the Public Safety Group of the Home Office, to address the issues raised in connection with Offensive Weapons.

4. I make this corporate witness statement on behalf of the Home Office to assist the Inquiry with the matters set out in the Inquiry's request for evidence dated 3 July 2026 and generally. I have prepared this statement with extensive support from my Home Office colleagues, the Government Legal Department and counsel. Given the scope of the evidence request and pace of the Inquiry I have not read every document exhibited to this witness statement, but have necessarily been reliant on my colleagues and the legal team to identify and place before me copies of key documents. Some of the matters addressed in this statement concern policy that is under development and I anticipate it may be necessary to provide an updating statement to the Inquiry at a later point this year.

5. There are two important issues to signal at the outset of this statement.

6. First, as I set out in more detail below, whilst the Inquiry conducts its work in Phase 2 government will continue to progress the policy work that has been underway since the attack. We must do this because these are urgent issues and they present a complex and evolving challenge, but it is intended that our work will not duplicate the Inquiry's work. It is also our intention that fundamental decisions for Ministers, which must necessarily take into account recommendations from this phase of the Inquiry, will not be taken until the Inquiry has reported.[3] By working alongside the Inquiry, sharing our progress and drawing on the Inquiry's far reaching programme of evidence and ultimately its conclusions and recommendations, we aim to deliver a response that will close the gap that the terrible attack in Southport has laid bare.

[3] If a discrete emergency matter were to arise which touched upon the Inquiry's Terms of Reference and required an immediate Ministerial decision, the Inquiry would be informed.

7. Second, part of the work that has already been done has been to consider carefully the extent of that gap, and how it should be defined. In the aftermath of the attack the formulation of the problem we were looking to address was the risk posed by 'Violence Fixated Individuals'. As our work has progressed, for reasons I will explain in more detail (paragraphs 153 to 156 below), we have identified the threat we need to address, that is not currently managed adequately by existing systems, as the use or threat of extreme violence by individuals who are not driven by a clear ideological purpose. Thus, the key terminology I use in this statement should be understood as follows:

    1) 'Non-ideological extreme violence' (NIEV) describes the threat the Government is working to address – namely the use or threat of extreme violence[4] by individuals who are not driven by a clear ideological purpose. The 'NIEV risk cohort' comprises individuals who may commit extreme violence which is intended to shock, intimidate or outrage an audience beyond the immediate victims, often generating fear in the wider public, where there is no clear ideological purpose. This violence is often – but not always – grievance-fuelled or accompanied by violence fascination.

    2) The term 'Violence Fixated Individual' (VFI) was defined in 2025 by T1D - Cabinet Office Body **T1D - Cabinet Office Body** to describe a type of individual who has both a *fascination*[5] with extreme violence and *intent* to inflict extreme violence, where ideology is not the primary driver. Although the term 'VFIs' has been, until very recently, used in policy development work, thinking has developed and evolved significantly since the **T1D*** definition. Counter Terrorism Policing (CTP) is not using VFI terminology as the term no longer accurately reflects the latest understanding of the threat. There is consensus across government and policing analytical and assessment bodies that 'violence fascination' is more appropriately understood as a behavioural indicator or risk factor, rather than a discrete offender cohort. Thus, where I refer to VFIs in this witness statement it will generally be in the context of previous policy work.

T1D* - Cabinet Office Body

[4] Paragraph 160 below sets out the meaning of extreme violence in the NIEV context.

[5] Whilst they have different meanings, the terms 'fascinated' and 'fixated' have been used somewhat interchangeably through this programme of work. Going forward, due to the specific meaning of "fixation" in different threat management contexts, the Home Office will use 'violence fascination'.

3) Fascination with violence can occur across ideological and non-ideological contexts. Individuals who present with violence fascination will include both individuals who are not driven by a clear ideological purpose *and* those whose risk falls to be managed under Prevent where there are reasonable grounds to believe they are vulnerable to being drawn into terrorism.[6]

8. These terminology changes do not in any way affect the substance of the Inquiry's work, which has of course been framed in accordance with the Terms of Reference as directed at the threat posed by VFIs. The Inquiry is working to consider and make recommendations about the same threat and the same gap.

(A) ROLES AND RESPONSIBILITIES - OVERVIEW

9. Whilst each department will be able to explain their work and role more fully, I provide an overview here of the roles and responsibilities of the key government departments, teams and bodies in connection with the work on VFIs and NIEV. Section B below provides more information about how, going forward, this work will be coordinated across government.

HOME OFFICE

10. As the lead department for national security and public safety, it has been agreed that the Home Office (HO) should hold coordination and policy development responsibility for addressing the risk posed by NIEV, although as set out below, delivery of mitigations for NIEV risk is a cross government effort.

Homeland Security Group

11. The Homeland Security Group (HSG) in the Home Office leads on supporting the Home Secretary in delivery of her national security responsibilities. It also provides oversight of Counter Terrorism Policing; enables Home Secretary oversight of MI5; and co-ordinates the response to terrorism-related crises.

---

[6] As set out in Cathryn Ellsmore's first witness statement, although the s.36 CTSA test is whether someone is "vulnerable" to being drawn into terrorism, CONTEST 2023 and the refreshed Prevent Duty Guidance reflect that the test CTCOs apply is whether there are reasonable grounds to suspect a person is susceptible to terrorism (see paragraphs 42 and 129 **[JE/001 - HOM000078]**). In this statement I use the statutory language.

Counter-Terrorism Directorate (sits within HSG)

12. As I set out in the introduction, the Counter-Terrorism Directorate leads and coordinates delivery of CONTEST and is also responsible for delivering key elements of the Prevent and Pursue strands of that strategy. It comprises: the CONTEST Unit, the Counter Radicalisation and Extremism Unit, the Prevent Delivery Unit, the CT Pursue Unit and the Joint (Prisons) Extremism Unit.

Prevent Delivery Unit (PDU)

13. PDU leads on the Prevent Programme, one of the four core strands of CONTEST. Prevent is designed to stop people from becoming terrorists or supporting terrorism through early intervention and multi-agency support. The unit oversees the policy and overall delivery of the statutory Prevent and Channel Duties, within the Counter-Terrorism and Security Act 2015. The Desistance and Disengagement Programme (DDP) strand of Prevent aims to rehabilitate those who have already engaged in terrorism or terrorism related activity using tailored interventions by practical and ideological intervention providers.

Non-Ideological Extreme Violence (NIEV) Team

14. The NIEV Team sits within the PDU. It was established in April 2026 to coordinate cross-government work on NIEV, and establish governance at senior and ministerial level. It provides the secretariat function for the new **NIEV Taskforce**. I address its role and the role of the NIEV Taskforce in Section B below.

The VFI Unit

15. The VFI Unit was a temporary (effective from March to October 2025) Home Office led cross-government team to coordinate government work and develop policy responses to the VFI risk in 2025. It sat initially within the Homeland Security Strategy Directorate before moving to the former Prevent Directorate. The limited timeframe of the VFI Unit was due to the fact the team was established at pace as part of early cross-government efforts to understand and address what was then termed 'VFI risk' and was largely staffed by secondees. Further details about the role and work this team carried out are covered in the narrative section below.

Counter Radicalisation and Extremism Unit (CREU)

16. CREU's Preventing Radicalisation Online (PRO) team works to prevent individuals from becoming radicalised online by reducing the availability and accessibility of radicalising content online, reducing permissive spaces for terrorist and extremist activity online and

identifying individuals susceptible to radicalising narratives, in order for the appropriate support to be provided. PRO does this by directly engaging with industry partners, UK law enforcement and agencies, international partners, the private sector, and civil society organisations to work collectively towards the goal of preventing radicalisation online.

Research, Information and Communications Unit (RICU)

17. The Research, Information and Communications Unit Knowledge Hub (RICU KH) sits within the CREU. It provides analysis on terrorist use of propaganda and exploitation of the internet to inform the UK's counter-terrorism system, through open-source monitoring. Its activity is underpinned and directed by sensitive information pertaining to terrorism threats and the identification of at-risk audiences. RICU KH has produced analysis on topics relating to NIEV. T1D

T1D

T1D

CONTEST Unit

18. The CONTEST Unit is based in the Home Office with responsibility for coordinating the departments and agencies across government involved in counter-terrorism policy and response, known as the counter terrorism system, to deliver CONTEST, the UK's counter-terrorism strategy.

Technology, Data and Innovation Directorate (TDID)

19. The Technology, Data and Innovation Directorate (TDID) sits within the Homeland Security Group and brings together the Home Office's core capabilities on technology, data and innovation to address national security threats in a more joined-up way. It takes a "technology-first" approach, focusing on how technologies create harms and opportunities, and works across the Home Office and with external partners to develop policy, capabilities and delivery that protect the public. Core units include the Emerging Technology Safety and Security Unit (ETSSU), Investigatory Powers Unit (IPU), Digital Communications Capabilities Unit (DCCU), National Communications Data Service (NCDS), Accelerated Capability Environment (ACE) and Science and Technology (S&T).

Emerging Technology Safety and Security Unit (ETSSU)

20. ETSSU was established in January 2025 and provides cross-cutting coordination for the Home Office on online harms policy and strategy, supports wider government engagement and leads strategic engagement with DCMS (formerly DSIT) and

technology companies. The teams sitting within ETSSU are the Online Harms Strategy, Coordination and Tech engagement team, the Emerging Tech AI and Cross-cutting Threats team (responsible for the new Extreme Violence Content measure, as outlined in the King's Speech on 13 May 2026, and and the NIEV Taskforce Online Environment Working Group – see paragraph 69 below) and the Online Safety Act team.

Public Safety Group (PSG)

21. The Public Safety Group (PSG) is responsible for leading the Home Office's work to keep the public safe and reduce crime. PSG set the strategic direction for public safety, ensuring the system is working effectively to deliver the outcomes that matter to the public. This means protecting the vulnerable, cutting crime, disrupting the highest harm criminals, and ensuring that the police are as trusted, efficient, and effective as they can be in serving the public.

Crime Directorate

Youth Futures Unit

22. The Young Futures Programme is about ensuring that Children and Young People (CYP) who are vulnerable to being drawn into crime are identified earlier and offered the right support in a more consistent and coordinated way. It is also about creating more opportunities for young people within their communities. The Programme consists of two component parts - Young Futures Prevention Partnerships led by the Home Office and Young Futures Hubs led by the Department for Culture, Media and Sport (DCMS, with cross-government support as appropriate). I provide further information about Young Futures Prevention Partnerships below (paragraphs 360 to 362).

Firearms and Weapons Policy Unit

23. The Firearms and Weapons Policy Unit is responsible for ensuring that legislation and controls on firearms, knives and other bladed articles and offensive weapons support public safety by minimising the risk to the public and reducing crime.

Violence against Women and Girls Directorate and Safer Streets Mission Directorate

Tackling Child Sexual Abuse Unit (TCSAU)

24. TCSAU is responsible for tackling all forms of child sexual abuse by preventing offending and re-offending, bringing more perpetrators to justice and ensuring victims and survivors receive support, justice and accountability. TCSAU drives both Home Office activity

relevant to tackling child sexual abuse and co-ordinates wider cross-government action. Over recent years we have seen the threat from child sexual abuse increase in severity and complexity. An example of the increasing complexity is Com groups, sadistic online communities primarily made up of minors who aim to cause severe harm and which often engage in online child sexual abuse in combination with other online harms relating to NIEV. Capabilities funded and supported by TCSAU in the National Crime Agency, and an undercover network of officers based in Regional Organised Crime Units can play a critical role in identifying offending and victimisation within Com Groups. In addition to areas of direct overlap with NIEV risk, the Home Office recognises that learning from TCSAU's work on online protection and online investigation reads across to online capabilities for detection and management of NIEV risk.

The Interpersonal Abuse Unit (IAU)

25. The Interpersonal Abuse Unit is responsible for the Home Office's policy and strategy on violence against women and girls (VAWG), including domestic abuse, sexual violence, stalking, forced marriage, female genital mutilation and 'honour'-based abuse, including where offences occur or are coordinated online or facilitated by the use of technology. The Unit leads Home Office activity in these areas and coordinates cross-government work to reduce harm, improve outcomes for victims and survivors, and strengthen the response across policing, the criminal justice system and wider public services. Technology is increasingly being used as a mechanism through which VAWG is perpetrated, intensified, concealed or extended, with content online also normalising harmful attitudes. This can overlap with other online harms including relating to NIEV. The Home Office is committed to expanding the use of undercover online officers for VAWG and here also recognises the potential for overlap with NIEV risk.

Digital and Innovation Group

26. The Digital and Innovation Group was created in January 2026 to bring together Home Office science, innovation, data and technology functions. The Home Office 2030 Digital Strategy sits in the Digital and Innovation Group.

Home Office Analysis and Insight (HOAI) Directorate

27. The HOAI directorate is comprised of economists, statisticians, operational and social researchers, intelligence analysts and others. It provides evidence based insights, data

science and official statistics to inform policy and operational decisions across the Home Office's policy areas.

Homeland Security Analysis and Insight (HSAI)

28. HSAI sits within the HOAI Directorate. HSAI undertakes research and analysis to support with evidence and insights the policy formulation and operational decision making across HSG policy areas. They have written analytical papers to support understanding on VFIs, and HSAI chairs the new cross system NIEV Taskforce Analytical Working Group (see paragraph 69 below).

Home Office Science

Home Office Chief Scientific Advisor

29. The Home Office's Chief Scientific Advisor (CSA) since 1 February 2026 is Professor Brooke Rogers. The core role of the Home Office CSA is to ensure that departmental decisions are informed by the best science and engineering advice. The Home Office CSA works with other departmental CSAs under the leadership of the Government Chief Scientific Adviser to support each other and to resolve cross departmental problems.

Home Office Science Advisory Council

30. The Home Office Science Advisory Council supports the Home Office's CSA and provides independent, expert advice on the use of science, technology, analysis, and research across Home Office priorities supporting evidence based decision making. This has included research related to VFIs and work on risk communication, risk perception, and approaches to responses.

The Security Service

Legal framework

31. The functions of the Security Service are governed by statute. Section 1 of the Security Service Act 1989 (SSA) provides that these are:

    1) To protect national security against threats from terrorism; espionage; sabotage; the activities of agents of foreign powers; and actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means;

2) To safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands; and

3) To act in support of the activities of the police forces and other law enforcement agencies in the prevention and detection of serious crime

32. The legal framework within which the Security Service operates not only circumscribes its functions but also ensures intelligence powers are only used where necessary and proportionate to ensure the minimum level of intrusion relative to the threat. The Security Service must also comply with Article 8 of the European Convention on Human Rights (ECHR).

33. The Security Service is subject to oversight by the Intelligence and Security Committee, the Investigatory Powers Commissioner and the Investigatory Powers Tribunal. The Director General is accountable to the Home Secretary, who is in turn accountable to Parliament for the activities of the Security Service. In carrying out its functions, the Security Service is guided by the Government's National Security Strategy. Currently, its operational areas of focus are: (i) Counter-Terrorism; (ii) Counter State Threats and (iii) Protective Security.[7]

34. Section 1 of TACT 2000 defines 'terrorism' as the 'use or threat of action which is designed to influence a government, or international organisation, or to intimidate the public or a section of the public, and where the action or threat is made for the purpose of advancing a political, religious, racial or ideological cause' (s.1(1)). The action or threat must involve serious violence against a person; serious damage to property; endanger the life of persons other than the person committing the act; create a serious risk to the health or safety of the public, or section of the public; or be designed to seriously interfere with or seriously disrupt an electronic computer system' (s.1(2)).

Role in addressing the threat posed by VFIs and NIEV

35. The Home Office does not consider that addressing the threat posed by VFIs/NIEV falls within MI5's functions as set out in s.1 of the SSA, save insofar as it can support police forces and other law enforcement in the prevention and detection of serious crime, to the extent that it is necessary and proportionate. MI5 only provide such support if their

[7] Security Service Act 1989 s.1(2). See also National Security Strategy 2025 p.20 **[JE/002 - HOM000520]**.

assistance is requested. As such, MI5 may potentially assist the police, where MI5's particular capabilities are required. A practical example is where MI5 may provide a level of support to a major incident where a serious crime has (or may have been) committed. Such support may increase, decrease or cease depending on how the intelligence picture develops.

36. Although the majority of VFIs/NIEV threats falls outside MI5's remit, the following summarises the limited ways in which MI5 's capabilities are engaged in relation to the threat by VFIs/NIEV:

    1) **Identifying whether an incident or threat is terrorist in nature.** Fixation or fascination with violence is an increasingly prevalent behavioural characteristic within MI5's national security casework, and identifying whether an incident or threat is terrorist in nature is increasingly difficult. Investigations of individuals fixated with violence may be prioritised by MI5 where there is intelligence to indicate an ideological element, only for this to be discounted subsequently. In cases where a national security threat exists alongside other complex risk factors, the relatively recent Interventions Centre of Expertise (ICE), addressed below, can bring together a multi-agency team of professionals to provide MI5 and CTP investigators with advice on external tools and resources that may be of use in managing the threat, e.g. by providing the individual/s concerned with appropriate support where such support will directly mitigate the national security threat posed.

    2) **Serious crime.** As indicated above, in some circumstances, where non-terrorist activity reaches a 'serious crime' threshold, intelligence and/or information can be shared with the relevant agencies, such as police or the National Crime Agency (NCA), or coverage maintained in support of an ongoing police operation under MI5's remit to support serious crime investigations. In those circumstances, ownership of the investigation would sit with the relevant law-enforcement agency (LEA), with MI5's role limited to providing intelligence support within a LEA command structure.

    3) **Threats to life and individuals at risk of harm.** In the course of MI5 investigations, MI5 may receive intelligence, where violence, killing and serious harm are planned, perpetrated, and celebrated as ends in themselves and may identify threats to life or serious harm. As a public authority MI5 has a statutory

responsibility to take appropriate action to mitigate real and immediate risk to Article 2 (right to life) and Article 3 (right to protection from cruel, inhuman and degrading treatment) ECHR, even where intelligence does not relate to terrorism or is already held by relevant/competent authorities including CTP. MI5 has adopted a number of policies to ensure compliance with this legal duty.

Joint Terrorism Analysis Centre (JTAC)

37. JTAC is the UK's independent authority for all-source terrorism assessment. JTAC is based within MI5 and reports to the Director General MI5, but its assessments are made independently. JTAC brings together counter-terrorism experts from the UK's intelligence agencies, police and government departments. This ensures its assessments are informed by a wide range of knowledge, expertise and different perspectives. JTAC analyses all intelligence relating to terrorism, at home and overseas, and produces assessments of threats and other terrorism related subjects for customers from a wide range of government departments and agencies.

Interventions Centre of Expertise

38. The Interventions Centre of Expertise sits within the Counter Terrorism Operations Centre (CTOC), a joint facility comprising partners from CT Policing, the intelligence agencies and the criminal justice system. ICE comprises a multi-agency team of professionals drawn from both the national security community and wider public services. Its function is to bring a range of professional expertise in managing national security threats in counter-terrorism investigations involving adolescents, mental ill health and other complex risks and vulnerabilities (see: Director General Threat Update **[JE/003 - HOM000180]**). Violence fixation is one of the complex risks that can feature in CT investigations; ICE will engage in those cases where there is an indication of terrorist ideology, and therefore a national security justification to do so.

CABINET OFFICE (CO)

Economic and Domestic Affairs Secretariat (EDS)

39. EDS supports the Cabinet Office in developing, coordinating and agreeing the Government's domestic policy agenda. The Secretariat's involvement in VFIs largely

involved attending cross-government discussions and meetings on VFIs, over the course of 2025.

National Security Secretariat (NSS)

40. NSS coordinates security and intelligence issues of strategic importance across government and supports the Prime Minister and National Security Adviser. This involves supporting the National Security Council, including the relevant collective-agreement process; overseeing the delivery of the National Security Strategy 2025; coordinating key national security and foreign policy matters across government; and ensuring preparedness and crisis response through COBR (the UK government's primary crisis management committee). Through these responsibilities, NSS has played a role in coordinating government's work on VFIs.

National Security Council (NSC)

41. The National Security Council is a committee of the Cabinet. From 5 July 2024 to 20 July 2026 its Terms of Reference were to consider the strategic approach to national security, foreign policy, resilience, international relations, economic security, trade, development, defence and global issues. The Terms of Reference are likely to be updated in due course.

T1D**

****Cabinet Office Body**

42. The **T1D - Cabinet Office Body** produces analysis and insights to support policy and decision-making at the centre of government. **T1D**** provided analytical support to the National Security Secretariat on the VFIs work. The team coordinated work across government on identifying the size of the cohort, the key risk factors and behaviours and the public services that can respond to these, and the key barriers across government on data sharing.

T1D

43. The **T1D** leads on intelligence assessment and development of the UK intelligence community's analytical capability. It provides authoritative, all-source assessment for the Prime Minister, the NSC and senior policy makers to support their decision-making on national security and foreign policy priorities. **T1D** will sometimes work with **T1D**** (see paragraph 139 below) and other partners to provide joint analysis on threats to national security.

FORMER DEPARTMENT FOR SCIENCE, INNOVATION AND TECHNOLOGY (DSIT)

Security and Online Harms Directorate

44. Until 21 July 2026 DSIT had overarching responsibility for online safety policy. This remit was wider than online safety regulation and included responsibility for policies relating to mis- and disinformation, media literacy and online safety technologies which help to make the online environment safer for all users.

Government Office for Science (GO-Science)

45. The Government Office for Science advises the Government on policy and decision-making based on science and long-term thinking. The Home Office has worked with GO-Science to look at the evidence base in relation to VFIs. This included both internal and external roundtables (in which external academics participated).

DEPARTMENT FOR DIGITAL, CULTURE, MEDIA AND SPORT (DCMS)

46. As of 21 July 2026, following the Prime Minister's changes to the machinery of government, the Department for Culture, Media and Sport will be renamed the Department for Digital, Culture, Media and Sport (DCMS). DCMS will have responsibility for online safety policy.

47. In addition, DCMS lead or are involved in a variety of work programmes aimed at young people and invests in funds and projects to support this. This includes programmes that are either aimed at, or have the potential to prevent crime, and to tackle broader risk factors.

DEPARTMENT OF HEALTH AND SOCIAL CARE (DHSC)

48. DHSC, with NHS England, oversees a number of safeguarding duties and statutory responsibilities of a range of organisations that provide NHS and adult social care services across the health system. This includes adult social care, mental health support, support for autistic people and people with learning disabilities and overseeing the implementation of the Prevent Duty for health. The Department has financial

responsibility to Parliament for the operation of the health service, which includes NHS funded services for adolescents and children who have mental health difficulties. DHSC is not involved at an operational level in identifying, assessing, or managing individuals who present risks of serious violence but does commission services and interventions that are relevant to the assessment and management of the risk posed by those individuals.

MINISTRY OF JUSTICE (MoJ)

Youth Justice Policy Unit

49. The Youth Justice Policy Unit is responsible for youth justice policy including early interventions in the justice system.

Counter-Terrorism Assessment and Rehabilitation Centre (CT-ARC)

50. CT-ARC is a national HMPPS body falling under the responsibility of the Ministry of Justice, which was set up in 2019 and has been operational since November 2022. It addresses the evolving nature of terrorist threats through evidence-informed risk management. Using specialist psychologists and probation officers, and engaging with academia, it develops tools for assessing and intervening with individuals throughout the justice process. The team includes a research function that oversees product development and implementation, and a quality assurance function that monitors operational delivery. It has the capacity to understand both the terrorist and terrorist risk cohort and works to assess, manage and reduce their risk, translating this knowledge into resources, assessments, policy advice and interventions which are used across the CT network, including in the Prevent space.

MINISTRY OF HOUSING, COMMUNITIES AND LOCAL GOVERNMENT (MHCLG)

Community Cohesion Unit

51. Working with local partners and other parts of government, MHCLG is focused on strengthening societal resilience through leading work on cohesion/integration, and tackling religious hatred. These work strands support, but are separate to, the delivery of Prevent and CONTEST.

DEPARTMENT FOR EDUCATION (DfE)

52. DfE is responsible for setting the national legislative, policy and safeguarding framework for schools, colleges and local authorities in England. This includes issuing statutory and non-statutory guidance on safeguarding, behaviour, attendance, exclusions, alternative provision, SEND and online safety in schools. Through this role, DfE establishes the expectations, standards and safeguards that support education settings and local services to identify concerns early, assess risk appropriately and respond in partnership with other agencies. In practice, schools and colleges are often the first institutions to identify individuals who may present risks of serious violence, as they have the most consistent day to-day contact with CYP.

COUNTER TERRORISM POLICE HEADQUARTERS (CTPHQ)

53. CTPHQ is hosted by the Metropolitan Police Service (MPS) and consists of officers and staff from across the regions, including both permanent members and individuals seconded from their home forces. CTPHQ provides national oversight of the CTP network and operates under the command of the MPS Assistant Commissioner of Specialist Operations (ACSO) and the Director General of CTP. Operational accountability lies with the Chief Constables of the relevant region. CTPHQ holds a strategic leadership and coordination role but does not possess directive powers, or take over operational command of a local investigation or response, except in a small number of defined circumstances. CTPHQ supports regional Counter Terrorism Units (CTUs) and Counter Terrorism Intelligence Units (CTIUs) in the implementation and assurance of common systems, policies, and procedures. In addition to its policy responsibilities, CTPHQ may facilitate the sharing of CTP resources across the network to provide additional capacity or specialist capability in regions experiencing heightened demand.

(B) NIEV POLICY LEADERSHIP – OVERVIEW

Context

54. Responsibility for addressing the NIEV threat sits across a significant number of departments (and the teams within them) and operational partners. The Home Secretary is accountable for public safety and accordingly NIEV policy leadership sits in the Home Office (as noted above, in the Counter-Terrorism Directorate in HSG). However, it is important to emphasise that whilst policy leadership sits with the Home Office, other

departments lead changes on key areas (for example, DHSC on mental health strategy), and those departments have their own, sometimes competing, priorities and challenges to address. Equally different teams within the Home Office have their own aims and objectives and different areas of shared policy responsibility with other departments.

55. The number of departments and policy teams across government with a role to play means that in developing policy responses to address the NIEV threat we are grappling with a complex landscape of overlapping policy interests, reviews, programmes, and approaches at a national and local level. There are also differences in emphasis between safeguarding (and often a focus on young people/children) and public protection. For example, a DfE Minister has recently proposed commissioning a review (the Terms of Reference remain in draft) of the Children and Young People Youth Crime Prevention, Safeguarding and Youth Justice landscape. This overlaps with the Home Office's NIEV work (see further paragraph 381 below) and discussions are ongoing as to how to manage this.

56. However, our experience – both from the work in 2025 of the VFI Unit and the work of the NIEV Team and Taskforce this year – is that departments, agencies and law enforcement are engaged, willing to share, and talk through issues and challenges, and attempt to come up with approaches or solutions. The Taskforce has had good engagement and there has been challenging but constructive discussion on the scale of the problem and whether future changes should focus on solving issues just related to the NIEV threat or whether more fundamental reform is needed.

57. The initial – short term – structures that were put in place last year, and the process of responding to the Inquiry's Phase 1 recommendations, have allowed us to better understand the relative roles and responsibilities of different parts of government that need to be involved in this work going forward, and informed the new structures that are in place under the NIEV Taskforce

Counter-Terrorism Directorate Leadership

58. Understanding of the nature and scale of the NIEV threat and the potential operational and policy responses to it requires a baseline knowledge and competence in multi-agency risk management and safeguarding. Within the Home Office that knowledge and experience is most readily available in the Prevent Delivery Unit of the Counter Terrorism Directorate. It is primarily for that reason that policy leadership for the NIEV threat sits in

the Counter-Terrorism Directorate. The CT system holds significant experience of engaging with a range of government departments, and with operational partners and practitioners across a range of sectors at the national, regional and local level. This experience in system leadership to tackle serious public protection risk is being drawn on to shape proposals for the policy and operational response to the NIEV threat. This arrangement is also beneficial given that, absent wider reform, the most immediate pressure to respond to the NIEV risk has been felt within the Prevent elements of the CT system.

2025 Arrangements

VFI Unit (March – October 2025)

59. Over the course of 2025 the temporary Home Office led cross-government VFI Unit (see paragraph 15 above) commissioned and undertook work to understand better what systems and powers are already available that are relevant to VFIs. Key aspects of the VFI Unit's work is summarised in the narrative below, namely:

    1) Commissioning an initial mapping exercise by the Home Office Policy Unit as to the existing landscape relevant to VFIs (see paragraphs 73 - 106 and paragraph 130 below).

    2) Reaching preliminary conclusions as to the potential applicability / utility of existing systems (see paragraph 378 to 380 below).

    3) Conducting an initial mapping review of Civil Orders that might be relevant to VFIs to consider the ability to impose restrictions or requirements on VFIs (see paragraph 145 below).

    4) Conducting an initial scoping of a new Violence Prevention Gateway, conceived as a broad multi-agency framework for countering non-ideological extreme violence (see paragraph 144 below).

    5) Considered future leadership of VFI policy, recommending that the Home Secretary ought to continue to provide cross-government leadership on management of the VFI threat (see paragraph 146 below)

Violence Fixated Individuals Analytical Group (VFIAG)

60. As I set out below (see paragraph 122), in early 2025 the initial commissioning of analytical work relevant to VFIs was led by the Violence Fixated Individuals Analytical Group comprising a cross-HMG Senior Analytical Leadership Team and the Chief Scientific Advisor network (VFIAG) This work will now be carried forward by the NIEV Taskforce cross government Analytical Working Group, chaired by HSAI, (see paragraph 69 below) and so the VFIAG has disbanded. The Taskforce will continue to draw on support from the Home Office Chief Scientific Advisor to inform analytical work.

NSC

61. As I address in the narrative below (see paragraph 126 below) the NSC met in March 2025 to discuss T2D and VFIs and agreed a short-term programme of work to cover immediate prioritisation of known risk, early intervention, longer-term management of risk and actions to reduce the risk of online radicalisation and facilitation. Chaired by the Prime Minister, this is main forum for collective decision making on matters of national security, which illustrates the high priority given to addressing the VFI risk (as it was then defined). When actions are assigned by the NSC there is an expectation that progress against the actions is reported back.

Arrangements established in 2026

NIEV Taskforce (cross government) and NIEV team (Home Office)

62. The NIEV Taskforce was announced on 13 April 2026 (the day of publication of the Inquiry's Phase 1 report) and has been created by the Home Secretary in recognition of the need for a concerted effort across Government and with operational partners, to coordinate our approach to NIEV.

63. The Taskforce brings together departments and operational partners, with responsibilities in relation to prevention, online safety, safeguarding, health and social care, policing, and criminal justice. The Taskforce is led by the Home Office, reflecting the Home Secretary's accountability for public safety including the risk of a serious violent incident or attack of the kind seen in Southport, and for driving a coherent response to associated harms, including online offending.

64. The purpose of the Taskforce is to develop effective and proportionate management of NIEV risk in the context of wider public safety and national security threats, by examining the end-to-end system for identification, risk management and intervention.

65. The Taskforce will ultimately aim to provide a clear analysis of options (including costs, deliverability and efficacy) and recommendations for decision to Ministers on the longer-term systems approach to tackling the NIEV threat, including the approach to early intervention, the online environment, and any operational response. This will allow Ministers to consider options and next steps alongside the findings and recommendations made by Phase 2 of the Inquiry and use the Taskforce to deliver change swiftly where required. The Taskforce will also monitor the delivery of Phase 1 recommendations owned by central government.

66. The outputs of the Taskforce are expected to include:

    1) A cross-government evidence base on NIEV that supports the early identification of emerging risks, operational pressures and gaps in the current system;

    2) A coherent cross-government programme of policy development, including pilot activity;

    3) Engagement and evidence to support Phase 2 of the Southport Inquiry, ensuring close alignment between taskforce activity and emerging Inquiry themes; and

    4) Advice to Ministers on key strategic choices, trade-offs, resourcing issues and delivery risks.

Overview of NIEV Taskforce governance

67. The 'NIEV Taskforce Overview' slide **[JE/004 - HOM000515]** sets out the significant level of governance for the Taskforce, to support working through options and challenges at pace, given that decisions will need to be taken on options impacting a wide range of different partners.

68. All Boards and Working Groups (see below) that are part of the Taskforce will be run by Home Office teams and will have cross Government and operational partner membership.

69. The Director General level NIEV Steering Board (which was previously called the Southport Recommendations Steering Board) met on 13 May 2026 and 5 June 2026. From September, is expected to convene quarterly (Terms of Reference will be provided when finalised). The Director-level Strategic Delivery Board, which I chair, first convened in early July and is expected to convene going forward on a bi-monthly basis (Terms of Reference **[JE/004a - HOM000487]**). The Steering Board and the Strategic Delivery Board are supported by five thematic Working Groups and a Practitioner Advisory Group which will meet at varying frequencies:

    1) Analytical Working Group (Terms of Reference **[JE/005- HOM000463]**) – chaired by HSAI;

    2) Early interventions Working Group (Terms of Reference **[JE/006 – HOM000466]**) – chaired by NIEV team;

    3) Online Environment Working Group (Terms of Reference will be provided when finalised) – chaired by ETSSU;

    4) Operational response and law enforcement Working (Terms of Reference will be provided when finalised) – chaired by the NIEV team;

    5) NIEV Practitioner Advisory Group (Draft Terms of Reference **[JE/007 - HOM000489]**) - chaired by the NIEV Team.

<u>NIEV Team</u>

70. The Home Office NIEV team was established in April 2026, subsuming the responsibilities of the previous VFI Unit.

71. The NIEV team is responsible for:

    1) Tracking delivery of Phase 1 recommendations across government;

    2) Co-ordinating the Home Office's evidence and input to Phase 2 of the Inquiry;

    3) Providing the policy development and secretariat functions for the Taskforce.

72. The NIEV team is situated in the PDU, within the Counter-Terrorism Directorate, to allow it to learn from policies and approaches taken to tackle the terrorist threat, explore in detail how any approach to tackling NIEV would integrate with the Prevent system, and understand the operational impact NIEV is currently having on the CT system (see further paragraph 58 above).

(C) EXISTING ARRANGEMENTS RELEVANT TO THE NIEV RISK

73. In addition to core policing capabilities to prevent and detect crime, there is a range of existing frameworks, services and interventions which are used to intervene with and support individuals with risk factors which may ultimately lead to NIEV behaviour. They are summarised briefly in this section:

    1) Prevent;

    2) Community Safety Partnerships;

    3) Violence Reduction Units;

    4) Young Futures Panels;

    5) MASH;

    6) MAPPA; and

    7) Other relevant services.

74. Each of these vary in their design, the nature of the service they deliver and the safeguarding or public safety risks they address, and none is precisely focused on the violence fascination or the NIEV risk.

PREVENT

Overview

75. How and when Prevent has a role in the identification of violence fascination and NIEV risk and the management of that risk has been the subject of detailed evidence in Phase 1, and in particular through the evidence provided by Cathryn Ellsmore (Home Office), DAC Vicky Evans (CTPHQ) and DCS Sarah Kenwright (CTP North West) **[13 October 2025 – DAY 22 – Cathryn Ellsmore Page 1; DCS Kenwright Page 104; 14 October 2025 – DAY 23 – DAC Evans Page 1-115]** and I do not rehearse that evidence here,

but the following summary is provided to assist the Inquiry in understanding the extent of Prevent's current role in dealing with this risk. For clarity, in that content that follows I refer to the following key groups of professionals involved in the delivery of Prevent's objectives:

1) Frontline professionals: the professionals in a frontline role to whom the Prevent duty applies (e.g. teachers, medical professionals, social workers, probation officers etc) and who are the primary source of referrals to Prevent.

2) Prevent practitioners: the professionals involved in the Prevent decision making or facilitating that decision making, i.e. Counter Terrorism Case Officers (CTCOs) and their supervisors, Channel Chairs and their deputies.

3) Intervention providers: the specialist, Home Office approved, mentors who provide support to individuals adopted by Channel.

76. Pursuant to section 36 of the Counter Terrorism and Security Act 2015 (CTSA) Prevent seeks to identify and support individuals in respect of whom there is a reasonable belief that they are vulnerable to being drawn into terrorism. Violence fascination is a potential (but not necessary) risk factor or indicator that someone is on a pathway towards terrorism, even where ideology is not present or is yet to take hold. Violence fascination in and of itself would not alone give rise to the belief that someone is on a pathway to terrorism - other factors as laid out in the Prevent Assessment Framework (PAF), would also be considered to determine whether the referred person was appropriate for Prevent support (see PAF: **[JE/008 -** CTPHQ000127 **]**).[8] However, at the referral stage an ideology is not required. The current Prevent Duty Guidance (2023) **[JE/009 - HOM000014]** states, *"…. it is far better to receive referrals which turn out not to be of concern than for someone who genuinely needs support to be missed"* and recent work (which I address further below) has sought to emphasise to frontline professionals that an ideology is not mandatory for a Prevent referral to be made or adopted.

77. Where the police assess an individual who is fascinated with violence does not meet the legal threshold under s.36 of the CTSA 2015, that individual is not eligible for Prevent support via Channel. A Channel Panel may, on considering a particular case, also conclude that individual is not eligible for Prevent support via Channel. Therefore some

[8] The PAF is the tool used by CTCOs to assess an individual's risk from the time the referral is first assessed until the individual exits Prevent / Channel - see Cathryn Ellsmore's first witness statement at paragraphs 120 to 126 **[JE/001 - HOM000078].**

individuals who are fascinated with violence will be supported by Prevent due to meeting this legal test, and others, where this test is not met, will not.

78. Where individuals fascinated with violence are referred to Prevent and do not meet the reasonable belief test during assessment by CTCOs or after consideration by a Channel Panel, their case will not be progressed in the Prevent system, and so these individuals fascinated with violence could and, in the future should, be referred onwards to other services for support, which can include health, education and frontline policing, or potentially violence reduction pathways, for example through Violence Reduction Units that exist in some local authorities (see paragraphs 99 to 101 below). Current work (addressed further below at paragraphs 345 to 350) is focused on strengthening hand-offs, local pathways and the wider multi-agency response for those cases.

79. NIEV is not yet defined in a way that is operationalised across sectors, policing and other agencies, nor is violence fascination as a risk factor consistently distinguished within Prevent. Current usage broadly captures extreme violence that resembles terrorism (eg. mass casualty attacks such as Forbury Gardens) but falls short of terrorism thresholds because it lacks an identifiable ideological driver. Within Prevent, the most operationally relevant 'type of concern' is Fascination with Extreme Violence or Mass-Casualty Attacks (FEVMCA). I set out below (paragraphs 317 - 323) the further work underway to develop clearer terminology, guidance and referral principles so that frontline professionals can distinguish cases suitable for Prevent from those requiring alternative routes.

Guidance and training

80. Violence fascination has been a prominent and developing feature within Prevent casework for some time. Reflecting this, the Home Office has incorporated learning on violence fascination and related concerns into training for different Prevent practitioners and Intervention Providers. I provide a summary here of the current position but, as I set out in more detail below (paragraph 317(2) below), following the findings of the Thresholds Review conducted in 2025 **[JE/010 - HOM000090]**, the Home Office recently reviewed the training for frontline professionals and Prevent practitioners. This has included consideration of the training around cases where the individual has no clear ideology, and training for both cohorts is being updated in light of the findings of that review, and also to take account of the proposed Interim NIEV Guidance (see paragraph 320 below). The updated training will be available from March 2027.

81. **Frontline professionals**. The primary resource for the very large number of frontline professionals subject to the Prevent Duty is the Prevent e-learning package made available via gov.uk (hosted separately for use by NHS staff). This package consists of four components: the Awareness Course, the Referrals Course, the Channel (or PMAP) Course and the Refresher Awareness Course. Data from gov.uk shows that these training courses have together been undertaken more than three million times since launching in August 2022. Frontline professionals are also able to access additional face to face training which includes more detail on specific risk factors including 'school massacre' type risks which we now associate with violence fascination.

82. The Prevent Duty e-learning courses have been updated following the publication of the Key Principles of Prevent to emphasise that a clear or fixed ideology is not required before a referral can be made where there are concerns about radicalisation. These training courses do not make explicit reference to violence fascination.

83. The e-learning package includes a mandatory knowledge check assessment to test understanding of the key learning outcomes and provide an indication of learning and effectiveness:

    1) Data from Sept 2025 to March 2026 shows average knowledge check scores were 86% for Awareness, 66% for Referrals, and 70% for Channel/PMAP training based on approximately 247,000 Awareness, 32,600 Referral, and 19,800 Channel course attempts from learners.

    2) Learners demonstrated a strong understanding of core Prevent concepts, with 97% correctly identifying what Prevent is and 88% correctly identifying misconceptions about susceptibility and vulnerability to radicalisation.

    3) However, performance was notably weaker from the Referrals course, with only 56% correctly identified the first step following a Prevent referral, and 59% understood when information can be shared about someone of concern.

    4) In the Channel course, between 26% and 33% of learners answered key process questions incorrectly, including questions relating to referral assessment, the Prevent assessment framework, and types of support available.

5) The knowledge check assessments are being updated as part of the wider training refresh to strengthen how understanding is tested and evidenced.

84. The 'face-to-face' training package, including the Extremist Ideology course, was developed in response to the Independent Review of Prevent (IRP), specifically recommendations 22, 23 and 24 to provide a face-to-face training service for frontline staff. It is a Home Office resource designed to provide authorised trainers across the specified authorities access to Prevent training resources to facilitate high quality training sessions. This training is available to both frontline professionals and Prevent practitioners and includes the concept of ideological fluidity, with specific content covering fascination with extreme violence or mass casualty attacks. The devolved 'train the trainer' delivery model currently in use means that the Home Office does not have accurate figures for the number of training sessions delivered and that there is a less comprehensive assessment of the effectiveness of the learning.

85. For **Prevent practitioners**, training and guidance and assessment tools, such as the PAF support the use of professional judgement when considering cases involving fascination with extreme violence or mass-casualty attacks.

86. CTP is responsible for designing guidance and delivering training for CTCOs and their supervisors. The training includes the approach to violence fascination within Prevent casework and FEVMCA. CTP is also responsible for monitoring performance and quality assuring the operational application of policy and training. The exception to this is the PAF training where the Home Office is involved in the development and delivery of training to CTCOs and their supervisors. The PAF tool was developed and is quality assured by CT-ARC and is used to support the triaging of referrals, inform decision-making by Channel panels and prioritise the support offer to individuals on Channel. Anti-social behaviour and attitudes towards violence are captured in the PAF tool, both for initial screening and throughout the susceptibility assessment elements of the tool. PAF training is jointly delivered by the Home Office Channel Quality Assurance team and CTP. It concludes with a pass or fail assessment and CTCOs are not approved to use the PAF until successful completion of this training. The Home Office Channel Quality Assurance team also run briefing sessions for Channel Chairs on the PAF to ensure they have a good understanding of the tool, as the PAF is central to putting in place support plans for individuals adopted on Channel.

87. The Channel Duty Guidance 2023, the statutory guidance aimed at Channel panel members and partners of local panels, provides a case study of an individual with an interest in extreme violence or mass casualty attacks where a Prevent referral would be suitable **[JE/011 - HOM000021]**. It does not provide content relevant to the NIEV risk cohort who do not meet Prevent or Channel thresholds. Further guidance is therefore needed to support consistent decision-making, onward referral and risk ownership for cases where concerns remain, but Channel is not deemed the appropriate mechanism (as to which see paragraph 320 below).

88. The Home Office provides a comprehensive professionalisation programme for Channel Panel members, including Channel Chairs and their deputies. Following a successful pilot in December 2025, there is a new specific training module designed to enhance the knowledge and understanding of those involved in Channel Panel about background factors, drivers and susceptibilities that may influence individuals to engage in violent extremism not associated with a specific ideology. There is further training for Channel Chairs and Deputies that is mandated specific to the chairing role and responsibilities detailed in the Channel Duty Guidance. The effectiveness of the training is assessed through practitioner feedback, and operational assurance as part of the Channel Quality Assurance framework. The Home Office is currently conducting an independent process, outcome and value for money evaluation of the Channel programme, set to conclude in December 2026, the results of which will provide insight into how individuals for whom violence fascination is a risk factor are currently managed in the caseload, and will drive future improvements for policy, practice and training.

89. For **Intervention Providers (IPs)**, the approach to training recognises that support must be tailored to the individual case, as such the provider network of IPs has been developed to reflect experience of working across cases with distinct, or fluid ideologies, or where violence fascination is a significant factor.

90. Home Office IPs receive both guidance and training to support them in their role as a mentor. The current guidance is focussed on how they conduct themselves in their role rather than centering on any specific ideological approach. A variety of training is available which covers a range of ideologies, including fascination with extreme violence and mass casualty attacks. IP's can access this training as and when needed to support their individual cases. The training is provided by specialist commercial providers and includes a number of mandatory elements such as safeguarding, personal safety, report writing and autism awareness. The training is shaped by direct insight into the emerging

threat and risk from Home Office analytical assessments. The effectiveness of the training is measured through IP feedback with a central training log recording completion rates.

91. The Intervention Provider register, which captures specific specialisms in the Intervention Provider cohort to assist Channel Panels in implementing support plans, has recently been updated to make clear which Intervention Providers have worked with and have experience in dealing with violence fascination as a main factor. Within the current cohort of IPs, around 32% list fascination with violence as one of their specialisms with many more having general experience of dealing with individuals with violent tendencies.

Information sharing

92. Cathryn Ellsmore's first witness statement sets out the different stages of decision making and information gathering that take place before CTCOs decide whether to make a s.36 referral to Channel. The Prevent framework, underpinned by s.36 of the CTSA 2015, permits information sharing both at this stage, and when the Channel Panel are considering whether an individual should be adopted (see Cathryn Ellsmore's first witness statement paragraphs 31 – 46, 52 **[JE/001 - HOM000078]**). S.38 of the CTSA 2015 expressly requires cooperation by Channel Panel partners (as defined in Schedule 7 CTSA 2015) with the panel, the police and local authorities. This cooperation includes information sharing but only so far as this is 'compatible with the exercise of the partner's functions under any other enactment or rule of law' (s.38(3)(b)) and information expressly must not contravene data protection legislation (s.38(4)) or include intelligence service information (as defined in s38(5)).

93. Consent from the individual (or their parent/carer) is built into the statutory provisions and applies after the initial information gathering / sharing at the point a decision is taken by the Channel Panel to adopt the individual to Channel (s.36(4)(b)). If an individual or their parent/carer does not consent to Channel support (within 3 months of adoption), then Channel has no legal basis for the case to remain open, and a closure decision will be made. In these instances, CTCOs have the option to consider management in a Police Led Partnership (PLP) to allow for continued oversight of their risk, or in some cases a covert investigation may be opened (i.e. escalation to Pursue). In either case, police powers and data protection legislation will govern any ongoing information sharing. In other cases, where consent is refused or not given, Channel can consider an onward referral to another agency, e.g. health or social care. Explicit provision is made for this in

s.36(4)(e). In those circumstances, ongoing information sharing relevant to any NIEV risk would be subject to the information sharing arrangements of the agency / framework receiving the referral and ordinary principles of data sharing under the Data Protection Act 2018.[9]

94. Thus, the statutory Prevent framework should enable effective information sharing at an operational level. However, strategic, analytical and assurance activity that is undertaken by the Home Office continuously to improve the Prevent system is significantly hindered at present by (perceived) restrictions on information exchange. For example, the Home Office does not have access to pre s.36 data[10] which hinders our ability to improve referral quality and decision making at the referral stage, and identify changing cohort trends and threats. Efforts to resolve this issue within the current legal framework have not been successful to date and are ongoing. In the future it may be appropriate to consider revisions to CTSA 2015 to reference explicitly the Home Office's role in monitoring, analysing and quality assuring the Prevent programme in its entirety in order to strengthen our ability to draw down available operational data.

Community Safety Partnerships (CSPs)

95. CSPs, formerly known as Crime and Disorder Reduction Partnerships, are multi-agency statutory partnerships that were introduced by s.6 of the Crime and Disorder Act 1998. Section 6 requires responsible authorities to work together to formulate and implement strategies to tackle crime and disorder in their communities, reduce reoffending, prevent people from becoming involved in serious violence and reduce instances of serious violence in the area. The responsible authorities are: the police; fire and rescue authorities; local authorities; health partners and the Probation Service. Additional partners are determined at a local level and common additional partners include voluntary and community sector organisations, education providers and community representatives.

96. Since 2013 CSP funding has been directed through Police and Crime Commissioners (PCCs). There are over 300 CSPs in England and Wales, with structures and operating models that vary between areas. CSPs enable partnership members to coordinate responses to crime and disorder and deliver targeted interventions to address identified priorities for the local area.

---

[9] Article 5 UK GDPR and Chapter 2, Data Protection Act 2018.

[10] See Cathryn Ellsmore's first statement [HOM000078] at paragraph 35.

97. CSPs do not have a defined role in identifying NIEV and there is no referral process for individual cases, or case management function, although issues can be raised at a CSP based on specific cases to inform future strategy or raise concerns about systematic failings.

Violence Reduction Units (VRUs)

98. VRUs were established in 2019 under the Serious Violence Fund in the 20 police force areas most affected by serious violence to deliver a public health approach as set out by the World Health Organisation (WHO)[11] to (predominantly) public space youth violence. Then, in 2023, the Serious Violence Duty was introduced under Part 2 of the Police, Crime, Sentencing and Courts Act 2022 (PCSCA 2022), which requires specified authorities in a local area (police, local authorities, health boards, probation, Youth Offending Teams and fire and rescue services) to collaborate with each other to prevent and reduce serious violence in their local area. VRUs do not have a specific statutory function but, in areas with established VRUs, they are frequently part of the mechanism by which relevant services discharge the Serious Violence Duty. Areas without established VRUs can utilise another existing multi-agency structure, often called Serious Violence Duty Partnerships. The longer term outcome objectives are a reduction in violence through sustained systems change and more effective preventative activity.

99. VRUs provide an infrastructure for multi-agency working, the precise mix and mechanism of which is locally defined but is usually made up of PCCs, local government, education and health professionals. They have a board which provides strategic oversight and a team which implements agreed activities (such as the creation a 'strategic needs assessment' identifying the local drivers of serious violence and cohorts of people most affected in the area, and funding/delivery of interventions such as mentoring, sports programmes and social skills training). Many VRUs (and Serious Violence Duty Partnerships) utilise the existing CSP structures as part of their delivery, but it is up to local areas to decide how best to deliver their requirements. Individual cases can be

[11] A public health approach is about the process of addressing the issue
1) Surveillance: define the problem through collecting information and data about violence.
2) Identify risk and protective factors: use research to look at the causes of violence, what's linked to it, risk factors for violence and where interventions could be effective.
3) Develop and evaluate interventions: to find out what works in preventing violence by designing, implementing and evaluating interventions.
4) Implement effective interventions: also monitor the effects of these interventions on risk factors and evaluate their impact and cost-effectiveness

referred onto VRU-commissioned interventions, although referral processes will vary between VRUs and specific interventions.

100. Section 16 of the PCSCA 2022 creates an information sharing gateway to permit disclosure between specified authorities and other relevant authorities (local policing body, education prison and youth custody). Section 17 provides that local policing bodies may request information from these authorities for the purposes of discharging the duty and there must be compliance with such a request.

Young Futures Panels

101. Young Futures Panels[12] are part of the Government's Young Futures Programme, a manifesto commitment which aims to ensure children and young people aged between 10-17 who are deemed vulnerable to being drawn into crime, and in particular are at risk of violence, are identified earlier and supported in a more systematic way, as well as creating opportunities for young people in their communities, through the provision of open access to mental health and careers support. The Young Futures Programme consists of Young Future Hubs, delivered by the Department for Culture, Media and Sport, and Young Futures Panels, delivered by the Home Office, utilising the established frameworks of the VRUs and some Serious Violence Duty Partnerships. The Young Futures Panels have been piloted in 20 areas across the country since late 2025 and evaluation is ongoing. Their focus is on knife crime, anti-social behaviour (ASB) and violence against women and girls (VAWG).

102. Young Futures Panels are multi-agency teams with representatives from childrens services, the police, youth justice, education, health and the voluntary sectors expected to attend. The police make the initial referral to a Panel who will then make a triage decision on whether the child / young person should be referred for support. The child / young person would not automatically receive support, for example if it transpires they are already receiving effective support. Panels can refer children and young people into positive interventions including, for example, mentoring, sports intervention or art workshops, and make statutory referrals (e.g. health, safeguarding, youth justice) in addition to or instead of positive interventions. Panels do not have a case management function.

[12] These have previously been referred to as Prevention Partnership Panels, but Ministers have agreed to call them Young Futures Panels going forward.

103. Young Futures Panels are early intervention programmes. They operate at the lower risk/earlier end of the continuum of risk, which is relevant to the childen or young people they identify for support, the nature of the risk assessment they conduct and the nature of interventions at their disposal. Whilst they may support a child or young person who is showing early signs of NIEV risk (with no immediate threat) they are not set up to identify and support NIEV risk specifically (see Prevention Partnerships Delivery Plan Proposal 12.2.25 **[JE/012 - HOM000261]** and VFI Key Questions: Home Office Response 3.3.25 **[JE/013 - HOM000311]**). The NIEV Advisory Board includes representation from PSG's Prevention Partnerships (see further paragraphs 121 and 360 to 362 below).

Multi-Agency Safeguarding Hubs (MASH)

104. MASH are non-statutory entities which operate within and to the framework of statutory safeguarding duties under e.g. the Children Act 1989, Children Act 2004 and statutory guidance such as Working Together to Safeguard Children. They operate as 'front-door' multi-agency screening processes to facilitate decision making about vulnerable adults or minors who are referred to them. They perform three key functions: (i) ensure information sharing; (ii) complete a risk assessment; (iii) formulate an action plan. Almost all local authorities have a MASH or equivalent, although there is significant regional variation in the structures and mechanisms that MASH utilises.

105. Some MASH may well (although I do not have an evidential basis for this, it seems likely given the interplay that can exist between safeguarding and public protection concerns) play an important role in identifying NIEV risk in their caseloads, and making appropriate onward referrals to other services to address specific needs. However, we do not believe that this is widespread. Our understanding is that, typically, MASH do not play a significant role in managing NIEV risk save where that risk co-exists with other needs or risks that meet safeguarding thresholds. Safeguarding legislation and consequently, threshold assessments continue to be centred on determining whether a person is at risk of harm rather than whether they themselves pose a risk to others. Given increasing strain, both as to caseload and funding, and competing priorities local provision will automatically apply lesser weight to non-statutory commitments. Within that safeguarding landscape, the NIEV risk cohort will not be a 'distinct group or cohort' requiring assessment or support. Such individuals will invariably present with a myriad of other needs and adverse experiences/risks which may or may not meet the thresholds for safeguarding.

MAPPA

106. The Multi-Agency Public Protection Arrangements (MAPPA) is a national system, established by the Criminal and Justice Act 2003 (ss.325 – 327) through which the police, probation services and prison services (each a responsible authority / risk holder) work together to assess and manage the risk posed by serious and violent offenders. MAPPA are designed to protect the public from serious harm by sexual or violent or other dangerous offenders. MAPPA panels are operated locally in the 42 criminal justice areas of England and Wales.

107. MAPPA Panels are not statutory bodies but a mechanism through which agencies can work together and discharge their statutory responsibilities and protect the public. There are 3 levels of MAPPA management, which reflect the level of multi-agency management required. Higher risk cases tend to be managed at higher levels. At Level 1 risks are managed by a lead agency in cooperation with other agencies but without the need for formal multi-agency meetings. Level 2 is for active multi-agency management where the ongoing involvement of several agencies is required and there will be regular multi-agency public protection meetings about the individual and a jointly created and monitored risk management plan. Level 3 is for active enhanced multi-agency management, requiring the involvement of senior people from the agencies who can authorise extra resources (e.g. surveillance, emergency housing).

108. The police and probation services are responsible for ensuring that appropriate individuals are referred onto MAPPA.

109. There are four categories of individuals who are managed under MAPPA.

    1) Category 1 is for sex offenders.

    2) Category 2 is for those convicted of violent offences who have been sentenced to 12 months or more in custody or detention in hospital and are now living in the community.

    3) Category 3 is for persons who have been cautioned for or convicted of an offence that indicates they are capable of causing serious harm and that requires multi-agency management.

    4) Category 4 is for Terrorist or Terrorist Risk offenders: terrorism offenders who are subject to notification requirements; offenders sentenced to 12 months or more or detained under hospital orders following conviction for a terrorism

offence; and those who have committed an offence and may be at risk of involvement in terrorism-related activity.

110. For offenders under MAPPA a risk management plan is created, which includes supervision, monitoring and control, interventions, victim safety measures and contingency plans. The interventions may be mandatory or voluntary and are intended to develop the offender's own ability to avoid and manage risk situations. The supervision may include home visits, office-based supervision, licence conditions, electronic monitoring, contact with healthcare professionals or other measures.

111. Although management under MAPPA Category 3 is potentially the most relevant to NIEV risk, it only applies where a person has been cautioned for or convicted of an offence, so it is not (as currently legislated for) a viable risk management tool for the majority of the NIEV cohort, save where those with NIEV risk fall into one of the four statutory categories. The existing MAPPA Guidance (last updated March 2026) does not reference violence fascination or NIEV risk. MoJ has departmental responsibility for MAPPA. There is no dedicated Home Office lead for MAPPA.

Other Potentially Relevant Services

112. The Fixated Threat Assessment Centre (FTAC) is a joint NHS/police unit which manages 'fixated' individuals who have an obsessional preoccupation with a prominent person (e.g. member of the Royal Family, Member of Parliament or other public figure) or perceived grievance which they pursue to an irrational degree. The Metropolitan Police is the overall risk holder and is funded by the Home Office to staff this unit. The NHS personnel are funded by the DHSC. There is clearly some overlap between these individuals and the currently understood NIEV offender profile as analysis shows (see further paragraph 169 below) that grievances or perceived grievances are a likely risk factor for NIEV, and if unmanaged both cohorts are capable of violence to others. FTAC receives about 1,000 referrals a year and takes action on about 50% of these cases. Referrals can come from the affected individuals themselves, from police forces or from other organisations (such as the Parliamentary authorities). The main interventions FTAC utilises are referrals to health providers for psychiatric care, including hospital admission, or arrest and prosecution where necessary.

113. Integrated Offender Management is a more intensive than usual form of ongoing supervision focussed predominantly on persistent re-offenders whose crime types cause damage and harm to local communities. It brings together a multi-agency response with

the police, National Probation Service and agencies, charities or social enterprises working in the fields of drug and alcohol dependency, debt, health, housing, benefits and education. In most cases this involves burglary or theft but can include those posing a risk of violence. This process applies only to those individuals who have been convicted of a previous offence.

114. Where an individual poses a NIEV risk but has not previously been convicted, it is possible to refer them to a Potentially Dangerous Person (PDP) Panel to share information about their risk and implement interventions to manage that risk. PDPs are a non-statutory policing led programme, underpinned by College of Policing Authorised Professional Practice,[13] which aims to manage cases that do not meet the threshold for management under any of the four MAPPA categories (see above) but whose behaviour gives reasonable grounds for believing that there is a present likelihood of their committing an offence or offences that will cause serious harm. PDP panel membership varies locally, but will usually be led by police public protection officers, include police representation from different investigative and public protection teams, and sometimes other partners including child protection services and probation. However, such panels only exist in some local areas, they are narrowly focused and police forces have to have the necessary, trained personnel to implement any interventions.

115. There is a health / social care pilot of a programme called Integrated Care (Vanguard) Sites, which are units which integrate services around children and young people with complex needs and concerning behaviours (violence, self-harm, harmful sexual behaviour, fire setting) who are at risk of losing their liberty. These provide psychiatrically-informed plans for effective risk and harm mitigation, and vary from local area to local area. There are currently 11 in place, covering 19% of England. Their focus is on children and young people already involved in the justice system. NHS England, which established these pilots, will be best placed to address this model generally.

(D) NARRATIVE SUMMARY OF HMG INITIAL POLICY DEVELOPMENT WORK

116. In this section I provide an overview of the cross-government work to develop VFI (now NIEV) policy in the aftermath of the attack and AR's sentencing, primarily in 2025. This is not intended to be a comprehensive summary, but is provided to assist the Inquiry in understanding the initial workstreams and the progress of HMG's policy development

[13] APP - Potentially Dangerous Persons

over this period. Sections F and G provide more detail about key areas of recent and ongoing work.

July 2024 – January 2025

117. In the immediate aftermath to the attack, it was obviously important for the Home Office to allow the police operational space to conduct what was a challenging investigation. At the same time, the Home Office was concerned to ensure it did all it could to understand what had happened and the implications as soon as possible and what policy changes might be necessary. There was a focus on: changes to Prevent already underway following the 2023 Independent Review of Prevent **[JE/014 - HOM000071]**, the Independent Prevent Learning Review **[JE/015 - HOM000062]** and implementation of its recommendations, the creation of the role of the Independent Prevent Commissioner (whose Report, 'Lessons for Prevent' (**[JE/016 - CTPNW000114]** pp35-50) was published in July 2025) and the Home Office's Mental Health and Neurodivergence Strategic Policy Review ('the MHND Review' as to which see further paragraphs 179 to 181 and 342 below). This work has been addressed in Cathryn Ellsmore's first and second witness statements to the Inquiry **[JE/001 - HOM000078]** **[JE/017 - HOM000223]**.

118. Prior to and during this period there was also focus in Counter-Terrorism on the growing issue of minors (under 18s) being investigated for terrorism related activity – a problem recognised internationally.[14] A cross-government Minors in CT Strategic Oversight Group (SOG) had been established in May 2023 to agree coordinated and strategically aligned efforts across relevant departments and agencies to reduce the number of minors in the CT system. The SOG does not run or own work itself. It was jointly chaired by Prevent and Pursue Deputy Directors, with representation from other departments and operational partners who have relevant policy or operational responsibilities to deliver on identified actions. It met periodically through this period, initially quarterly, moving to bi-annually. The SOG's work was not driven by the Southport attack but has some relevance to the issues for Phase 2 of the Inquiry, as it included increased focus in the

[14] In December 2024 the leaders of Counter-Terrorism for the Five Eyes nations issued 'Young People and Violent Extremism: a call for collective action' which called for a whole society response to help identify and deal with the radicalisation of minors and minors involved in violent extremist activities – especially online – across the Five Eyes nations. The Call to Action emphasised this was a shared responsibility for law enforcement, security and government agencies, the education sector, mental health and social well-being services, communities and technology companies. See: https://www.counterterrorism.police.uk/wp-content/uploads/2024/12/Unclassified-Five-Eyes-CT-minors-paper.pdf

Pursue space on early intervention and on a multi-agency approach for minors. Key challenges identified in January 2025 for prioritisation by the SOG of potential relevance to the Inquiry included a lack of mandatory options to engage with the parents and/or family of minors and sporadic partnerships with social services and youth justice practitioners (see: Minors in Terrorism Strategic Oversight Group minutes 16.1.25 **[JE/018 - HOM000323]** and update slides **[JE/019 –** HOM001006]).

January 2025: post sentencing policy package

119. Following AR's sentencing, a package of cross-government policy measures was identified including improvements to Prevent (addressed in Cathryn Ellsmore's first witness statement **[JE/001 - HOM000078]** at pp46-50 and oral evidence **[13 October 2025 DAY 22/66/24-82/10]**); a review of terrorism legislation; consideration of the extent to which existing civil orders would be suitable for cases involving violence obsession; a review to consider whether a broader CT-system response was required to manage violent individuals, and a pilot of an online referral tool to provide Prevent with an online detection and referral capability.

120. CTP, the National Police Chiefs Council (NPCC) and the NCA made proposals for wide ranging inclusions in the package. The proposals from the police highlighted the need to look at the problem and risks widely (having regard to recommendations made in previous investigations, inquests and inquiries), to appreciate the connection of causes that led to violence, and in particular the impact of violent content online to the lives of children and their isolation from society, and to look at the right strategic interventions being taken across all public bodies (see: Letter from CTP, NPCC, and NCA to Home Secretary dated 28.1.25 **[JE/020 - HOM000254]** and CTP's comments on the Home Office's Post Southport Policy Grid dated 11.2.25 **[JE/021 - HOM000255]**). The factors the police highlighted included in particular:

1) The increased number of referrals to Prevent following AR's attack and conviction and the resulting pressures on the Prevent system;

2) The role other parts of the system – in particular health and education – had to play in the identification and management of risk;

3) The importance of there being clear and definitive ownership for the support provided to individuals and the management of the risk they posed.

121. In early 2025 proposals for Young Futures Prevention Partnerships were developed to identify increasingly vulnerable children at risk of being drawn into crime: these became operational in November 2025. I have addressed Young Futures Prevention Partnerships and Young Futures Panels at paragraphs 101 to 103 above and 360 to 362 below (see also: second witness statement of Cathryn Ellsmore **[JE/017 - HOM000223]**; Prevention Partnerships Delivery Plan Proposal 12.2.25 **[JE/012 - HOM000261]**; VFI Key Questions: Home Office Response 3.3.25 **[JE/013 - HOM000311]**).

March 2025: National Security Council Actions

122. In early 2025 the VFIAG, comprising a cross-HMG Senior Analytical Leadership Team and the Chief Scientific Advisor network, was convened to define the cohort of VFIs and assess vulnerabilities and triggers, the size profile and trajectory of the VFI cohort and the interventions that would most effectively mitigate the threat. The Cabinet Office provided the Secretariat for this group (see: Home Office Southport Policy package paper 29.1.25 **[JE/022 - HOM000387]**; Southport Follow-Up Cabinet Office Summary of Discussion **[JE/023 - CAB000042]**; Terms of Reference: Violence Fixated Individuals **[JE/024 - HOM000250]**); T1D* VFI Analysis timeline **[JE/025 - HOM000265]**).

*Cabinet Office Body

123. The Home Office established a VFI Unit to coordinate policy work arising from the VFIAG, supported by cross-HMG secondees (see: letter from Permanent Secretary of the Home Office to Cabinet Secretary dated 10.2.25 **[JE/026 - HOM000249];** Violence-fixated individuals and wider post-Southport reform: governance **[JE/027 - HOM000386]**).

124. By March 2025 it was recognised that there were challenges in analysing existing datasets on VFIs given the absence of a strict single definition. There were also limitations to data to be drawn from the Prevent Case Management Tracker (PCMT). It was identified that a 2023 report from the US National Threat Assessment Centre drawn from 173 cases of targeted violence contained conclusions relevant to VFI risk factors[15] but despite identifying patterns of risk factors, the study affirmed that there was no single profile for a person who was going to commit an attack and recognised – in line with the UK Prevent approach – that behavioural threat assessment is the best practice for targeted violence prevention (see: US Secret Service National Threat Assessment

[15] The Home Office emphasised that although access to weapons in the US was a distinguishing feature, the US school-shooting data provided a relevant and wide database which should be examined both for risks and effective interventions **[JE/013 - HOM000311]**

Centre 'Mass Attacks in Public Spaces 2016-2020 **[JE/028 - HOM000510]**; Minutes of Violence Fixated Analytical Group 13.2.25 **[JE/029 - HOM000266];** VFI Key Questions: Home Office Response March 2025 **[JE/013 - HOM000311]**; VFI Update and Next Steps Readout of meeting convened by the Cabinet Office on 4.3.25 **[JE/030 - HOM000303]**).

125. On 5 and 6 March 2025 GO-Science convened two cross-HMG round table meetings to address: (i) the state of the evidence around the aetiology (study of causes) of VFIs **[JE/031 - HOM000349]** and (ii) the current HMG capability to identify VFIs and mitigate harmful impacts, and how this capability reflected current evidence **[JE/032 - HOM000348]**. Broadly speaking, these reinforced the difficulty of defining and identifying VFIs and the limitations of data in this regard and evidence for effective interventions. It was agreed that general approaches to violence reduction may offer insights for VFIs but these had limitations and improved identification of VFIs could be achieved through better data sharing and adequately funded multi-agency collaborations.

126. On 25 March 2025 the NSC convened to discuss T2D and VFIs (see: NSS paper dated 21 March 2025 [disclosed by CO] and Actions set **[JE/033 - CAB000053]**). The following actions relevant to VFIs were identified:

- **Action 3**. Confirm to NSS that the following measures (as set out in paragraph 17 of the NSC paper) have been, or are being, implemented in order to reduce the number of individuals susceptible to radicalisation and/or extreme violence:

  a. equipping schools and universities to tackle hate, through the Educate Against Hate programme and relationships, sex and health education (DfE);

  b. proactive efforts to build community cohesion, including driving interfaith interactions (MHCLG);

  c. equipping law enforcement (e.g., through additional legislation) to identify and disrupt extremists in this country, and prevent those preaching values contrary to our own from entering the UK (Home Office);

  d. utilising the Serious Violence Duty to ensure local structures collaborate to tackle the issue of VFIs (Home Office);

  e. joining up with other efforts given overlap in interventions, particularly aims under the Safer Streets Mission and Youth Offending Teams, to reduce knife crime and Violence against Women and Girls including misogyny (Home Office and MoJ).

- **Action 4**. Accelerate a national roll-out plan for Prevention Partnerships and wider complementary work to identify and support minors showing signs of vulnerability towards extreme violence (HO working with DfE, DHSC, MHCLG and MoJ).

- **Action 5**. Update guidance to expand Channel thresholds, with a particular focus on capturing borderline cases and repeat referrals.
- **Action 7.**[16] Local services should prioritise the VFI cohort (individuals who do not meet Channel thresholds, but do represent a clear risk of violence to others) across the national security, social care, health, education, youth justice and law enforcement systems. Any resourcing and financial implications of delivering this should be considered at the Spending Review. This should include:
    - Prioritising local authorities with a high concentration of VFIs for additional funding to address cohesion concerns and complement local delivery of Prevent (MHCLG);
    - Youth Offending Teams should prioritise those at risk of becoming VFIs, noting they are not currently set up for this purpose. This should be informed by the latest evidence on which interventions work (MoJ);
    - Prioritise adapting health services in 11 priority local areas to accept VFI referrals for access to mental health and other services, with a view to expanding further (DHSC);
    - Continuing to invest in, and potentially expand, the Interventions Centre of Excellence to improve handling of CT casework by refining our understanding of which interventions work, how best to deploy them and to ensure we are delivering value for money (CTP to coordinate).

    (CTP, DHSC, DfE, MoJ and MHCLG)
- **Action 8**. Scope further, more ambitious options which go beyond those in Action [7] for how social services can prioritise and support VFIs (DfE, DHSC, MHCLG, MoJ working with HO).
- **Action 9**. Scope a national prevention gateway and case management service for the management of VFIs and vulnerable individuals more broadly (HO, DfE, DHSC, MHCLG, MoJ)
- **Action 10**. DSIT SoS to update NSC with a package of measures, including:
    - How to support Ofcom to go hard on enforcement of the Online Safety Act and strengthen expectations on companies to develop technical solutions to more effectively identify, report and remove illegal content, with sanctions should they fail to do so;

[16] The Inquiry should note that the numbering of the actions from this action onwards is sometimes inconsistent in documents addressing the NSC actions. I will refer to these action numbers in this witness statement.

- Scoping the feasibility and desirability for device-level interventions for terrorism or extreme violence-related material, building on industry-led innovation in other areas;
- Options to extend civil or criminal liability for tech executives whose services fail to identify and remove illegal content and how this approach would compare internationally; and
- Options to go further, e.g., on restricting social media access for children drawn from consideration of international models such as the Australian approach

- **Action 11**. Develop the following legislative proposals, set out in paragraph 34b i-iii in the NSC paper:
  - Update legislation (e.g., TACT 2006) to broaden the definition of illegal terrorist content to reflect the impact of material which is not instructional but contributes to radicalisation; and re-examine the boundaries of illegal material with particular reference to extreme violence and gore;
  - Strengthen the reporting requirements around illegal content to require companies to take reasonable steps to identify users who upload or interact with illegal material on their services; and,
  - Build on the provisions in the OSA to develop a faster takedown regime for disputed content, whereby government or law enforcement could directly issue and enforce notices requiring specific content to be removed.

  (Home Office)

- **T2D**

T1D*=Cabinet Office body

127. On 27 March 2025 **T1D*** circulated a paper providing an analytical assessment of the VFI cohort which addressed the scale of the VFI threat, the working definition of VFIs, VFI characteristics and drivers, implications for interventions and proposed next steps **[JE/034 - CAB000023**. In particular, the paper concluded:

1) The number of VFIs is likely to be in the 'hundreds' (between 100-999) [medium confidence].

2) The working definition[17] of VFIs combined three elements:
   - Fascination with extreme violence;
   - intent to commit extreme violence;
   - where ideology is not the primary driver.

3) It is challenging to identify common pathways towards individuals becoming VFIs, and attackers were likely to differ substantially in their trajectories. It is difficult to develop predictive models.

4) Whilst expert consensus is that neurodivergence is not a risk factor for violence in the general population, in the VFI population it appears to have raised prevalence.

5) Grievances are a likely risk factor but they are not universal. Some cases may not have a clear motivation beyond violence for the sake of violence.

6) Seeking personal notoriety is occasionally a motivation and in these cases the aim of the violent act is to be maximally transgressive.

7) There is limited research on the impact of the internet, social media, algorithms or online radicalisation on VFIs. It is a realistic possibility [low confidence] that platforms amplify pre-existing risk.

8) Case study analysis shows that VFI attacks are preceded by long periods of exploration, research and a growing fascination with violence for violence's sake. It is possible that predatory behaviours can be identified with sufficient scrutiny [high confidence].

T1D*=Cabinet Office body

9) As to implications for interventions **T1D*** recommendations included that interventions should be multi-agency, tailored to individuals and ideally applied early, and assessment of risk should take a threat based approach, not a profile based approach (in line with the threat assessment approach in Prevent).

10) In terms of next steps, **T1D*** recommended: continued work by the Home Office and partners on the definition of VFIs, the size of the VFI cohort and

[17] See paragraphs 7 above and 158 to 168 below which address terminology and definitions.

improving data links across government; the Home Office should develop an assessment framework identifying concerning behaviours; consideration by operational agencies to changing the term VFI to mean 'violence fascinated individuals'; GO-Science to undertake further research to understand the prevalence of neurodivergence within the known VFI cohort; and further meeting convened by the Cabinet Secretary of seniors from across government in Summer 2025.

128. On 10 April 2025 at the conclusion of the cross-government process initiated by the Cabinet Secretary on 29 January 2025, the Senior Coordination Meeting of the VFIAG was convened and further actions were set (Actions **[JE/035 - HOM000327]**). These included:

1) Analysis of Prevent cohort / police data to identify any common characteristics/drivers and to inform further analysis/policy research.

2) Work to enhance the working definition of VFIs by setting out which categories do not qualify as VFIs (e.g. domestic violence, gang-related violence, terrorism).

3) Identifying useful learning that could be applied to the VFI cohort from historical and international research.

4) Analysis of effective interventions for VFIs, drawing on the suggested categories (people with an established mental health diagnosis with well evidenced treatment; people with an established mental health diagnosis with poorly evidenced, ineffective or resource intensive treatment; people with no obvious mental health diagnosis or other relevant developmental or medical condition).

5) The Home Office VFI Unit to provide an update on progress regarding work on potential system touchpoints.

6) The Home Office to ask DSIT to include a focus on the role of social media in relation to VFIs, as part of ongoing wider analytical work on impacts of social media on children and young people. EDS to consider commissioning this aspect of work to be completed to a faster timeline.

Cross-government work to support actions set by the NSC and the VFIAG

129. The VFI Unit conducted a series of workshops to help determine next steps and develop policy options (see: 21 May 2025 on VFI Cohort Definition & Interventions (Slide deck **[JE/036 - HOM000395]** and read out **[JE/037 - HOM000394]**); 29 May 2025 on VFI Policy & System Response (Agenda **[JE/038 - HOM000401]** and read out **[JE/039 - HOM000997]**); 26 June 2025 on Practitioner Perspectives on Policy Proposals (Slide deck **[JE/040 - HOM000995]** and read out **[JE/041 - HOM000994]**).

130. In May 2025, the Home Office Policy Unit, commissioned by the VFI Unit, prepared a report entitled 'Violence Fixated Individuals: Review of Available Interventions' **[JE/042 - HOM000332].** This report was commissioned to review the effectiveness of the Home Office and police-led services and interventions that were potentially available to those within the VFI cohort. The report highlighted in particular the proliferation of local multi-agency partnerships, boards and groups which left the landscape complex and crowded, and at times near duplicative, and the absence of a clear central repository of the interventions to which each service refers cases, which added to the confused picture. Recommendations were made as to the importance of data sharing to ensure interventions of potential relevance to managing VFI risk and their effect could be tracked; preparation of guidance as to the range of available services to VFIs, and the role of Young Futures Prevention Panels and Violence Reduction Units in addressing VFI risk and options for threat management systems.

131. On 19 May 2025 JTAC produced a report on Non-Ideological Extreme Violence to provide an assessment of whether the trend of non-ideological violence was increasing, what the potential risk factors of this type of violence are and why they do not meet the UK definition of terrorism **[JE/043 - HOM000539]**. JTAC judged that NIEV was a growing problem and the cohort of individuals posing a risk of NIEV is increasing. JTAC considered the Prevent data represented the best available proxy dataset in judging the scale of the issue but recognised it only presents a partial picture due to the subjective nature of referrals, categorisation, and changes to the programme since inception. JTAC's methodology was to examine 16 case studies[18] (domestic and international) which did not meet the UK terrorism definition but had some of the elements that would commonly be associated with terrorist attacks. JTAC identified the most common risk factors across the case studies although noted the interaction of these factors was highly

[18] Including the Inquiry's Case Studies C, D and F

likely to be more significant than any single factor and emphasised that potential risk factors were not exhaustive or universal (see paragraph 169 below as to risk factors generally, which include those identified by JTAC).

132. Looking ahead to the next 5 years JTAC judged:

1) That the majority of the potential risk factors are on a worsening trajectory, driving the growing cohort of individuals posing a risk of non-ideologically motivated extreme violence and so further non-ideologically motivated acts of extreme violence are increasingly likely, but events on the scale and impact of Southport would be a rarity).

2) Differentiating these types of incidents from terrorist attacks would remain challenging.

3) Widespread access to online spaces and violent content will continue to encourage an interest in more extreme violence.

133. On 27 May 2025 GO-Science chaired a third round table to discuss 'What evidence exists, or is required, to understand the efficacy of interventions to reduce the risk of VFIs' **[JE/044 - HOM000353]**. Attendees included representatives from HMPPS, MoJ, Forensic Child and Adolescent Mental Health Service (FCAMHS), NHS England, the Home Office, Clinical Psychologists from community mental health teams and social services, with the objective of obtaining input from individuals with expertise across the system who had first-hand experience of identifying and treating VFIs at early stages through to incarceration. The key points that arose from the meeting included:

1) There are a variety of ways / touchpoints by which VFIs come to the attention of public services and agencies which mean a single intervention or triage process will unlikely succeed.

2) Whilst there is limited evidence on the efficacy of interventions emerging insights suggest that existing interventions can be effective, but the system is fragile. Robust evaluations of interventions are critical to target finite resources effectively and avoid unintended outcomes.

3) Most risk predicting tools consider variables in isolation and have proven ineffective, especially for adolescents.

134. On 22 May 2025 GO-Science chaired a fourth round table to discuss "What evidence is there on the role of social media activity and content in the motivation and capability of Violence-Fixated Individuals (VFIs) to commit violent acts", which noted the difficulty of generating statistically meaningful conclusions in light of the very small size of the known VFI cohort and the challenges of designing an ethical and statistically valid study that could establish causation **[JE/045 - HOM000347]**.

***Cabinet Office Body**

135. In advance of a meeting convened by the Cabinet Secretary on 9 June 2025 for **T1D*** and the Home Office to update regarding their VFI work, the VFI Unit had sought to identify with cross-HMG colleagues and CTP, the strategic issues and choices facing the Government. The key issues set out by the VFI Unit were:

    1) Limited evidence on the scope and scale of the threat from NIEV.

    2) A known cohort presents risk but action may not be being taken to address it.

    3) None of the wide range of multi-agency frameworks are adequate for managing cases of NIEV.

    4) Uncertainty about effective interventions to prevent NIEV.

    5) No clear ownership across law enforcement for NIEV.

    6) The online environment is increasingly acting as an accelerant and enabler of NIEV.

    7) There is ineffective information-sharing, both operationally and post-incident, including communications with the public.

136. Significant feedback was provided by CTP and other departments. CTP emphasised that NIEV/VFIs sits outside the scope of the CT system. The impact of bringing the former into the latter or within Prevent (whether in its current or a new form e.g. a National Prevention Gateway) would impact CTP's core mission of addressing terrorism and state threats. There were different professional views about the best approach to addressing the NIEV risk (See: Southport Strategic Issues Paper, with comments from the Home Office Child Sexual Abuse Unit **[JE/046 - HOM000391]**; DHSC / NHS England **[JE/047**

- HOM000345]; MoJ **[JE/048 -** HOM000993 **;** DSIT **[JE/049 - HOM000403]**; CTP **[JE/050 - HOM000351]**).

137. Informed by work within the VFI Unit and at the request of the Cabinet Secretary's Office to be tabled at the 9 June meeting the Home Office provided a 1-page summary of the (unfunded) high ambition response to the VFI risk challenge: 1) A serious and sustained effort to **reduce the risk factors in the online information environment**; 2) **Prevention Partnerships** to reduce the pool of extreme violence risk; 3) **A National Prevention Gateway** backed by efficient and effective multi-agency systems; 4) **Scale and Strengthen Prevent** to handle the sustained surge and broader range of referrals **[JE/050a - HOM000355].** However, by this time the Home Office – in anticipation of the Spending Review - recognised that in the short term at least the work on the future system would need to focus on cost neutral improvements to strengthen existing risk management systems and the links between them, rather than the high ambition proposal (although as set out at paragraph 144 below, in July 2025 the VFI Unit did scope an initial policy proposal for a broader violence prevention gateway).

138. A significant issue remained prioritisation of those who present risk of violence to others for interventions across local services and the need to identify and overcome barriers that were being encountered to this (see e.g. VFI Unit paper for Cabinet Secretary Meeting 9 June 2025 'Progress Update: Measures to Manage the Risk from Violence Fixated individuals' **[JE/051 - HOM000359]**).

*Cabinet Office Body

139. On 9 June 2025 **T1D***, in collaboration with the **T1D** HO, JTAC, CTP, GO-Science and FCDO, prepared a summary of the cross government analytical work on VFIs for the Cabinet Secretary meeting (convened that day) which drew together its previous paper, the 4 GO-Science Roundtables, JTAC's analysis on NIEV, analysis of Prevent Case Management Data by both CTP and the Home Office, CTP research on multi-agency platforms, FCDO's analysis of the Global Terrorism Index data, and cross-government engagement on the topic of data sharing and data sharing barriers **[JE/052 - HOM000367]**. In particular, as to the scope and scale of the threat (as to which see further paragraphs 171 to 174 below), the summary indicated:

    1) Data suggests that since 2021 there are c. 1,500 known individuals that are likely to match the definition of a VFI, with an upward trend over time, although it is not known how much of that upward trend is due to increased awareness and guidance or genuine increase in risk;

2) Whilst there there is no international definition of VFI, in 2024 T2D T2D recorded a 270% increase in attacks where the ideological motivation was unclear or undetermined.

*Cabinet Office Body

140. T1D* made recommendations for the Home Office and DSIT including:

1) Home Office to define the level of VFI risk we accept;

2) DSIT to address data sharing constraints;

3) Home Office to develop a proposal for a National VFI Case Management System – a multi-disciplinary and multi-agency platform requiring significant funding and investment;

4) Home Office to work with others to evaluate effectiveness of interventions;

5) Develop and upskill practitioners in how VFI risk can manifest.

141. At the end of June 2025 the ETSSU confirmed a plan to review existing criminal legislation and the Online Safety Act 2023 (OSA), to identify if there was a need for the creation of a new offence that would cover content depicting extreme violence and gore and its promotion or dissemination online T1B (though emphasising this was not to replace or override platforms' duties under the OSA) (see: ETSSU proposal March 2025 **[JE/053 - HOM000306]**).

142. In July 2025 the Home Secretary received an update from the Home Office regarding the work done against the NSC actions from March 2025 (See: Update on VFI Response (VFI Unit) **[JE/054 - HOM000303]**; VFI Programme Plan setting out governance and programme of work progress and planning **[JE/055 - HOM000369]**; Submission – Prevent Thresholds Review (Prevent Directorate) **[JE/056 - HOM000366]**). This included the case for a National Prevention Gateway to bring coherence to the system for all serious violence concerns regardless of motivation. However, given the scale of the change required (major structural reform across multiple agencies and new legislation and governance frameworks) together with the fiscal context, this was not currently feasible and in the immediate term incremental measures, including strengthening existing frameworks and interventions, would be pursued.

143. Recommended legislative measures included:

1) An offence criminalising the creation and sharing of extreme violence content (now being implemented through the National Security Bill announced in the King's Speech of 13 May 2026) (see paragraphs 265, 267 - 269 below);

2) A harms-based offence categorising extreme violent material as illegal because it is linked to a specific harm or crime (not currently progressing);

3) An offence for the preparation of non-terrorist mass casualty attacks (also being implemented through the National Security Bill - see paragraph 266 below); and

4) T1B

144. Whilst the assessment remained that a National Prevention Gateway model was not feasible at that time, given that it was both an NSC action and a recommendation by Lord Anderson, the VFI Unit scoped an initial policy proposal for a broader violence prevention gateway with the intention of awaiting the outcome of the Southport Inquiry before seeking a final decision on fundamental reform (see: Initial Policy Proposal for the New Violence Prevention Gateway **[JE/057 - HOM000996]**).

145. The VFI Unit also conducted a mapping review of existing Civil Orders that warranted further consideration for VFIs **[JE/058 - HOM000436].** This review indicated that at present there are no existing civil orders which are suitable without legislative changes. The key issues with existing orders included that some had minimum age thresholds, required a conviction as a pre-condition or were designed for specific types of offending that were not applicable to VFIs generally. The new Youth Diversion Orders were identified as the most suitable tool but these were a CT risk management tool and, absent a connection with terrorism, they would not (once in force) be applicable.

146. On 3 November 2025 the VFI Unit provided a further update submission to the new Home Secretary and the Minister for Security, which provided an update against NSC Actions – in particular focusing on prioritisation by local services of those identified as posing a risk of violence to others (limited progress had been made), longer term broader reform,

the online environment and future leadership on management of the VFI threat (Submission on VFIs 3 November 2025 **[JE/059 - HOM000378]**).

147. On 19 January 2026, following consideration of this submission, the Home Secretary wrote to the Prime Minister highlighting, amongst other matters, the importance of support from local services (in particular the NHS) to Prevent's work. The Home Secretary noted that the Below Thresholds Pilot (see paragraph 345 below) had been successful at a local level but to implement it on a national scale would require significant resource investment across a range of services (Letter from Home Secretary to Prime Minister **[JE/060 - HOM000426]**).

148. In early 2026, at the request of the Cabinet Office, HSAI carried out a rapid review of evidence held (drawing on Prevent and police force data, literature review and international evidence) on interventions for VFIs to assist in HMG understanding of the interventions available for VFIs and provide an evaluation of their efficacy (see **[JE/061 - HOM000440]**). With caveats that the review was not systematic, there were limitations to the datasets relied on and interventions in online spaces were not examined, HSAI reported that:

    1) Internationally the evidence supported behaviour based, multi-agency, individual interventions rather than profiling or prediction.

    2) Bystander interventions are a critical prevention resource as most attackers show warning signs prior to attack (i.e. leakage). Bystander reporting should be encouraged by multiple, accessible and confidential channels and timely responses to reports, alongside continuous monitoring and promotion of reporting routes are essential to turn warning signs into early intervention rather than missed opportunities.

    3) Early community based and multi-agency support that addresses people's wider social, psychological and practical needs, building relationships and strengthening community cohesion works better than security-led measures alone. The design of Channel support is based on best practice for interventions in this complex space.

    4) It was very challenging to assess and evaluate the success of interventions designed to prevent extreme or mass casualty violence for a number of reasons (difficulties in defining or recognising success, limitations of evaluation

frameworks – short term or administratively convenient factors such as absence of further concerns, need to consider short, medium and long term impacts of interventions, related challenges in determining value for money of interventions).

5) A more detailed, systematic review would likely yield further insights, as could conducting research on VFIs outside of Prevent / CT programming.

6) When interventions are designed they should have evaluation tools embedded (e.g. indicators of success).

7) Exploration of interventions in digital spaces should be a priority for future work.

149. As set out above (paragraphs 62 to 69), following its announcement on 14 April 2026, the NIEV Taskforce has been established and the first meetings of the Steering Board and Strategic Delivery Board have been convened.

NSC progress update

150. Consistent with the decision that the Home Office holds policy responsibility for the NIEV threat, in June 2026 the CONTEST Unit provided an update on the March NSC actions to the National Security Secretariat (following an action from the Domestic and Border Security Committee) (see **[JE/062 - HOM000473]**). This update provided a brief summary of progress against actions that fell to the Home Office (the substance of which is addressed in this witness statement) and those that fell to other government departments. It should be noted some of these actions are beyond the scope of the NIEV threat. On Action 7 (prioritisation by local services) and Action 8 (more ambitious options for prioritisation of VFIs by social services) the update reflected that this issue had been the subject of ministerial discussions (see further paragraph 358 below) but the Home Office understanding was that named departments had not made significant progress nationally on these issues.

Response to Southport Inquiry Phase 1 recommendations

151. On 3 July 2026 the Government published its response to the Inquiry's Phase 1 recommendations **[JE/063 - ILT000113]**. That response made clear that as Phase 2 of

the Inquiry progresses the Government will follow its emerging evidence and findings to help shape the development of policy and test pilot approaches, continue to strengthen our understanding of the evolving threat from extreme violence and the effectiveness of interventions, and ensure our own policy development is clearly visible to the Inquiry.

(E) KEY THEMES AND CHALLENGES

152. This section summarises some of the key themes and challenges that have emerged through the work that has been done to develop policy responses to the risk posed by NIEV since the Southport attack. It brings together and provides high level summaries of research, papers and workshops generated both by the Home Office and other government departments in 2025 and 2026 to assist with and inform policy development, and some observations arising from issues raised by the Inquiry's request for evidence. The discussion in this section provides some context for the work that has commenced or is under development, as addressed in Sections F to H below.

Definitions, characteristics and risk factors

Definition of the harm we are seeking to address

153. As I set out at the beginning of this statement, as work in this area has progressed, the Home Office has concluded that trying to define VFIs as a particular type of person has fundamental issues and 'VFI' has not been operationalised (in particular, CTP used "FEVMCA" (see paragraph 79 above) in preference to VFI). Efforts to do so over the course of 2025 revealed some of the most significant challenges around this work. Recognising as we do, that the VFI terminology has been central to this policy work to date and in the Inquiry's Terms of Reference for Phase 2 is important to be transparent about definitional constraints, the evolving nature of this category and our preferred language and definitions going forward.

***Cabinet Office Body**

154. As already noted in 2025 **T1D*** proposed a working definition of a VFI as a type of individual who has a fascination with extreme violence and intent to inflict extreme violence where ideology is not the primary driver (**T1D***: Analytical Assessment: Violence Fixated Individuals 27.3.25 **[JE/034 - HOM000404]**).

155. RICU and HSAI have now conducted research to test the application of the VFI definition and evaluated its practical application to Channel cases (VFI Channel Analysis Findings

Report June 2026 **[JE/064 - HOM000491]**). They found the T1D* definition of VFI presents significant limitations and would likely need to be altered to be operationalised in an early intervention context such as Prevent. In particular assessing intent to commit extreme violence at the Prevent stage is inherently uncertain: it relates to someone's mental state; insufficient information about an individual's online activity is a general issue; and in any event, as Prevent is an early intervention programme, intent would not be expected to be fully formed, present or identifiable, and thus application is inconsistent. Furthermore, fascination with violence can occur across ideological and non-ideological contexts, which can be hard to distinguish and risks misclassification.

156. There is broad consensus across government and policing intelligence and analytical teams that violence fascination may be better conceptualised as one feature, that can fit within a broader NIEV framework, rather than a standalone category of person or offender cohort. Violence fascination, when flagged in isolation, will not act as a reliable predictor of risk of mobilising to terrorism or to NIEV: it is one of several risk factors, rather than a sufficient explanation for violence in its own right.

Working definition of Non-Ideological Extreme Violence (NIEV)

157. The Home Office is in the final stages of agreeing the policy definition of NIEV with stakeholders. Our current conceptualisation of NIEV is set out below but is subject to change as work will continue over the coming months. This work will be reflected in the interim guidance that the NIEV team is working to deliver in the autumn of 2026 (as to which see further paragraph 320 below).

158. NIEV involves the use or threat of extreme violence that is not driven by a clear ideological purpose. The extreme violence is communicative and intended to shock, intimidate or outrage an audience beyond the immediate victims. This can be explicit (stated intent) or implicit (due to nature or target(s) of violence).

159. Essential components (must meet all three):

The Act

1) Extreme violence

The purpose

2) No clear ideological purpose
3) (Explicit or implicit) intent to shock, intimidate or outrage wider audience

160. **The Act.** Extreme violence: includes homicide, grievous bodily harm (GBH), or coerced suicide. Typically, this will include mass casualty (or intended) attacks but can include a single-victim if the attack meets the purpose of intending to shock, intimidate or outrage an audience beyond the immediate victim (outlined below, for example through its livestreaming).

161. **The purpose.** No clear ideological purpose: NIEV is not driven by a clearly identifiable ideological purpose. Interpersonal, domestic, gang-related, drug, financial, sexual elements can be present however, as long as they are not the primary driver of the violence.

162. **Intent to shock, intimidate or outrage wider audience**. The violence is communicative and intended to shock, intimidate or outrage an audience beyond the immediate victims, often generating fear in broader society. This can be explicit through a perpetrator's statements, threats or plans. Where this intent is not explicit, but it can be reasonably assumed the perpetrator sought to reach a wider audience, the act can also meet this threshold. This implicit intent may be evident in the choice or location or target(s), method of violence, or the behaviour of the perpetrator(s).

163. These acts may primarily seek to appeal to a smaller in-group (such as violent online subcultures) for recognition, notoriety or social status. However, the impact of the violence often generates fear or concern in wider society due to the extremity or symbolic nature of the violence (although this element is not required to meet the definition).

164. Extreme violent attacks can have significant secondary and tertiary impacts similar to terrorism, beyond direct casualties and injuries to include widespread psychological distress and broader societal impacts such as perceptions of safety, fear, community tensions, public confidence in institutions and copycat or contagion effects.

165. **Target(s) and location.** Targets may be indiscriminate or individuals who represent specific groups. Targets may include those representative of personal grievances (e.g. family members, ex-partners, peer groups at schools), or wider targeting that may, in some cases, mirror the target selection of terrorists (e.g. minority ethnic communities, LGBTQ+). Targets may also be vulnerable sub-sections of society (e.g. children, elderly, students, homeless) and have a gendered component (e.g. women, girls). The choice of certain public locations (such as schools) may indicate an intent to harm wider society or to achieve notoriety (and can mirror locations targeted by terrorists).

166. **Method**. The method may be chosen to maximise the harmful impact of the violence on wider society. This can include weapons chosen (firearms, explosives etc.), the number of victims or the extremity of the violence. Perpetrators may also intend to maximise the harmful impact of the violence through sharing documents which explain their motive, grievances or desired legacy, capturing and distributing images and/or livestreaming the attack (though these elements are not required). These communicative aspects may also suggest a desire to inspire copycat violence.

167. **Violence fascination** is regarded as a feature that is common across NIEV offenders and pathways but it is not required to meet the definition. NIEV offenders often have a persistent, intense preoccupation with violence, violent ideation, or violent acts, this can be accompanied by obsessive rumination, emotional investment, or fantasising about committing violence. Behaviours that manifest include consuming or producing violent content, expressing admiration for past attackers, or repeatedly referencing violent themes in communication. Unlike general aggression or anger, violence fascination reflects a psychological or cognitive pattern that may escalate over time and contribute to the individual's pathway toward mobilisation to extreme violence.

Risk factors and characteristics

168. Input has been drawn from a wide range of sources (both within and external to government, and international comparators, particularly the USA school-shooting data and analysis) to identify potential risk factors and characteristics of NIEV offenders (although domestically this was primarily directed to VFIs in 2025) (see: for example, in chronological order: US National Threat Assessment Centre Paper January 2023 **[JE/028 - HOM000510]**; **TD1** **[JE/065 - HOM000233];**[19] NCA Paper February 2025 'Understanding the Scale and Severity of Online 'Com' Extortion Networks' **[JE/066 - HOM000392];** GO-Science Roundtable 6 March 2025 'What is current HMG capability to identify VFIs and mitigate harmful impacts, and how does this capability reflect current evidence?' **[JE/032 - HOM000348]** **T1D*** Paper 27.3.25 Analytical Assessment: Violence Fixated Individuals **[JE/034 - HOM000404]**; JTAC Report 19.5.25 Non-Ideological Extreme Violence **[JE/043 - HOM000539];** **T1D*** Report June 2025 'Violence Fixated Individuals: Analysis and next steps' **[JE/052 - HOM000367];** HSAI Rapid Review: Interventions for Violence

T1D*=Cabinet Office body

[19] This paper considers radicalisation of minors to terrorism but is included because of the overlap of risk factors, the commentary on limited ideological engagement of some of the case studies.

Fixated Individuals February 2026 **[JE/061 - HOM000440]**); VFI Channel Analysis Findings Report June 2026 **[JE/064 - HOM000491]**).

169. Recognising the definitional constraints and the significant limitations of the data (see paragraph 124 above and 193 to 194 below), and with the important caveat that, as with the wider radicalisation literature, there are no specific factors that conclusively indicate an individual's susceptibility to perpetrating a NIEV attack the following have been identified as potential risk factors or characteristics for NIEV offenders, or in some cases drivers or accelerants. These are drawn from a number of sources and not listed in priority order:

    a. Adolescence
    b. Being male
    c. History of physically aggressive or intimidating behaviours
    d. Experience of early trauma
    e. Dysfunctional family background
    f. Experience as victim of violence
    g. Social isolation/loneliness
    h. Personal grievances
    i. Poor mental health
    j. Neurodivergence
    k. Personality traits (e.g. lack of empathy, desire for notoriety)
    l. Substance misuse
    m. Fascination with violence[20]
    n. Engagement with online information environment
    o. Seeking status or notoriety
    p. Perceived changes in socio-economic or cultural norms
    q. Misanthropic and nihilistic belief

170. These factors do not however, easily lend themselves to predictive models for behaviour. First, the majority of the identified factors, both in isolation or in combination, have a high prevalence in the society at large and the vast majority of people for whom one or more of these risk factors apply will not be at risk of perpetrating a NIEV attack. Second,

[20] In their recent report, HSAI and RICU noted that "the wider literature suggests violence fascination appears to be an important factor among some individuals who have planned or perpetrated acts of non-ideological mass violence", but that it was also likely a factor in some cases of ideologically driven terrorism **[JE/064 - HOM000491]**.

attackers will vary significantly in their individual trajectories and individual factors will present, be weighted and interact differently. Risk factors need to be considered alongside (sometimes corresponding) protective factors. Thus case by case consideration needs to be given to the interaction between the risk factors, characteristics, behaviours, and drivers, so as to ensure that the interplay between these matters is considered and reflected in interventions offered.

Size of the cohort

171. We do not have sufficient data to enable a well-informed estimate of the number of individuals who pose a risk of NIEV. The analytical work over the course of 2025 identified the inherent difficulties in compiling and analysing data about VFIs given the absence of a single definition of VFIs (or an equivalent individual in other jurisdictions), the emerging nature of the threat, the number of potential sources for relevant data (e.g. data from the National Crime Agency, education, MASH, CAMHS and local policing) and the lack of reliable qualitative data.

172. The Prevent dataset is assessed to be the best available domestic proxy dataset in judging the scale of the issue within the CT system. However, it only presents a partial picture because it does not cover individuals who are not known to the Prevent system. In interpreting the data it is important to be mindful of:

1) The subjective nature of referrals, the categorisation of types of concern changes over time (as to which see Cathryn Ellsmore's first witness statement at paragraphs 91 to 97 **[JE/001 - HOM000078]**);

2) The fact that Prevent referrals require that a person may be vulnerable to being drawn into terrorism, not NIEV risk. It is reasonable to expect a system intending to capture NIEV risk may record higher numbers;

3) That cases with a violence fascination risk factor could sit across a number of the Prevent types of concern including, but not limited, to FEVMCA;

4) The practice of utilising only the primary type of concern recorded at the point of referral for analytical purposes;

5) The increase in referrals to Prevent following AR's sentencing;

6) The Home Office's lack of access to pre s.36 data (see paragraph 94 above).

173. With those very significant caveats, taking from the Prevent dataset the number of referrals in the 'Types of Concern' categories more likely to contain NIEV risk (namely (a) FEVMCA, (b) No Ideology, (c) No ideology + Susceptibility) provides the very upper limit of the scale of the issue. On that basis, in the Prevent dataset for the year ending March 2025 the total number of Prevent referrals was 8,778 and an indicative estimate that can be drawn from the referrals is 5,386 (comprising (a) FEVMCA – 469; (b) No Ideology - 3,009, and (c) No ideology + Susceptibility 1,908).

174. In 2025 analysis of Prevent data (by CTP) from the previous 4 year period and of data[21] from 35 (of 43) police force systems estimated there were 1,542 potential cases over that total period that matched T1D* definition of a VFI, and that the trend had been upward over that time – but given the limitations there is not a confident assessment of the scale of the threat (see: T1D* Report June 2025 'Violence Fixated Individuals: Analysis and next steps' **[JE/052 - HOM000367]**).

175. HSAI and RICU have subsequently conducted detailed case analysis on the referrals categorised as FEVMCA and discussed at Channel Panels in the period April 2024 – March 2025 (VFI Channel Analysis Findings Report June 2026 **[JE/064 - HOM000491]**). They identified at least 50 out of 155 cases that would meet T1D* working definition of a VFI (i.e. violence fascination, intent and not primarily motivated by ideology). The research was conducted over a small sample size (it only covered one year's worth of data and was limited to referrals categorised as FEVMCA, which is defined differently to the T1D* definition of VFI) and was not intended to quantify definitively the number of individuals who would meet the T1D* definition of a VFI in Prevent, but to test the T1D* definition and its practical application to Channel cases. Analysis reflected that it was difficult to identify fascination with violence due to a frequent lack of information around online behaviours and media being consumed.

176. HSAI has collated a database of potential NIEV incidents where there has been a fatality, with basic descriptive details mirroring HMG reporting for terrorist attacks. A variety of sources and engagement with stakeholders helped develop this list with multiple criteria used when considering classifying NIEV incidents. Using HSAI's criteria (which are different to the criteria for NIEV included in this witness statement due to the work on the

[21] Which T1D* noted was an indication of the scale of the casework over the UK but was limited due to gaps in returns and limititations of Force systems to identify, extract and interrogate relevant cases.

database commencing prior to the NIEV definition being forumlated) this work found that from 2020 - 2025 there could be 19 incidents of NIEV involving homicide in the UK (involving 21 suspects with 30 fatalities). This includes cases that would be unlikely to meet the definition of NIEV set out within this witness statement, for example a number of sexually motivated homicides are included which are unlikely to meet the 'purpose' element in the NIEV definition **[JE/067 – HOM000962]**. The Inquiry will also be aware of the 10 case studies identified by Jonathan Hall KC in his March 2025 'Independent Review on Classification of Extreme Violence Used in Southport Attack on 29 July 2024' **[JE/068 – HOM000542]** and the (in some cases overlapping) 16 case studies examined by JTAC for its report on NIEV (see paragraph 131 above).

Neurodiversity, mental ill health and NIEV risk

Relationship between neurodiversity, mental health and risk

177. It is important to recognise that at this point in time our evidence base for understanding the interplay between mental health and / or neurodivergence and NIEV risk is limited. However, in the far more mature environment of the CT space, we have greater confidence and it is likely that, as this work progresses, we will continue to draw significant learning from the CT experience.

178. **T1D*** March 2025 analytical assessment concluded that whilst neurodivergence is not a risk factor for violence in the general population, in the VFI population (working to **T1D*** definition) it appeared to have a raised prevalence. That assessment is consistent with the most recent Prevent data which shows that for the year ending 31 March 2025, 48% of Prevent referrals under the Type of Concern 'Fascination with extreme violence or mass casualty attacks' (227 out of 469) had at least one Mental Health Neurodiversity (MHND) condition recorded on the Prevent Case Management Tracker. This compares to around one-third of total Prevent referrals (2,955 of 8,778) where there was at least one mental health or neurodiversity (MHND) condition recorded. This relates to total Prevent referrals, rather than cases discussed or adopted by Channel. **T1D*** did not assess that neurodivergence plays a causal role in VFI pathways – it is better understood as a dynamic context in which several risk factors may unfold (see **TD1*** Paper 27.3.25 'Analytical Assessment: Violence Fixated Individuals' **[JE/034 - HOM000404]**).

179. Recent academic research, which has been reviewed by the Home Office as part of the MHND Review (the final report following the review is in the process of being finalised) suggests that certain neurodivergent traits and experiences may contextualise vulnerability, resilience, and disengagement in unique ways within extremist populations. This finding suggests that neurodivergent individuals within terrorist, extremist and mass murder populations may experience different pathways into these spaces than those experienced by neurotypical populations (see: Salman, N., & Al-Attar, Z. (2025). *A systematic review of neurodivergence, vulnerability, and risk in the context of violent* extremism). This further builds on Al-Attar's previous research (see: Al-Attar (2019) *Extremism, Radicalisation & Mental Health: Handbook for* Practitioners) which emphasised how neurodiversity contextualises, rather than causes, vulnerability in addition to resilience and disengagement. The contextual role will differ between cases, thus its relevance should be established through individual case information. Symptoms and traits are not alleged to make neurodivergent individuals inherently more susceptible to extremist involvement – rather, they may partially explain the unique cognitive and behavioural pathways that may contextualise extremist involvement among neurodivergent individuals.

180. The research also emphasises there are challenges in distinguishing autistic traits (such as hyperfixation, obsessionality, and circumscribed or restricted interests) from genuine threats and ideological commitments. As with the neurotypical population, it is not the case that any interest in extreme or violent topics will necessarily lead a neurodiverse individual to commit acts of violence. However, research has demonstrated that if interest in these topics take on an "obsessional quality", this may "push the individual from transient thinking about interest in terrorism to a fixated pre-occupation with and behavioural acting out of terrorism interest." (Al-Attar, Z. (2020) 'Autism spectrum disorders and terrorism: How different features of autism can contextualise vulnerability and resilience', *The Journal of Forensic Psychiatry & Psychology*, 31(6), pp. 926–949). Some individuals with autism may engage in behaviours that, on the surface, appear to be of concern – however - most often, those behaviours involve no intent and are driven by some of the features of autism. For example, it is common for individuals with autism to pursue their interest or preoccupation repetitively and they can become all-encompassing. This is likely to be inaccurately misinterpreted as a strong indication of an intense commitment to extremism where individuals accumulate substantial amounts of information or data associated with terrorism. Al Attar describes this type of behaviour as "being driven or at least accentuated by obsessionally, repetition, pedantry for detail and compulsive collecting/pursuit, as opposed to evidence of broader or greater

ideological objectives or greater operational involvement". It is therefore important for all factors to be considered to understand if this behaviour is relevant to risk or not.

Operational challenges

181. There remains significant practitioner uncertainty about how neurodivergence and mental health should be factored into risk assessments and, as covered by Cathryn Ellsmore in her witness statements for Phase 1, and below, this is an area of particular focus (see Cathryn Ellsmore's first and second witness statements **[JE/001 - HOM000078]** and **[JE/017 - HOM000223]**). The MHND Review found that cognitive biases and variability in risk assessment are particularly pronounced in cases involving MHND where there is no clear or coherent ideological driver. The review made a number of recommendations that collectively aim to improve how Prevent understands the relationship between MHND and risk and improve the quality of risk assessment for individuals with MHND. I address work following the the MHND Review at paragraph 342 below.

182. For the counter-terrorism system as a whole, including Prevent, the combination of public protection and mental health risk is very difficult to manage. The presence of mental ill-health complicates overall risk assessment. The complexity of MHND presentations across both Prevent and Pursue casework creates a need for specialist clinical forensic expertise to support the effective and timely assessment and management of CT risk among individuals experiencing mental ill-health. The shortage in assessments and support for both neurodiversity and mental ill-health impacts the ability of national security systems to manage cases and reduce risk and vulnerability.

183. Cases with identified terrorism risk are sitting on long waiting lists. The availability of appropriate interventions is limited by admission thresholds, capacity and resourcing issues. In many cases the mental health condition that is part of the risk picture (and the profile of the attacker in the Forbury Gardens Inquests was a clear example of this) may not be assessed as treatable. For a person to be detained under section 3 of the Mental Health Act 1983 for the protection of others it is necessary for appropriate treatment to be available to them. Where mental health conditions are deemed as not treatable, this can leave a gap in our ability to protect the public.

184. Research and practice are increasingly recognising that the relevance of mental ill-health may be most significant when the mental health need is unmet. For example, research on UK data suggested that cases where the mental health diagnosis and its relevance

for CT risk had been misunderstood are more likely to be criminally involved with extremism, suggesting unmet need is most relevant to risk management (see Draft MHND Review **[JE/069 - HOM000530]**).

The impact of extreme violent content online

185. The Home Office recognises the wider shift to online behaviour highlighted in Lord Anderson's July 2025 report **[JE/070 - ILT000106]**. Online activity is no longer a secondary factor. It is central to how risk develops and needs to be treated as a core part of how threats are identified, understood and managed. The Home Office views the online information environment as intrinsic to the threat from a range of harm types, which it can enable and exacerbate. Years of work on child sexual exploitation and abuse (CSEA) and terrorism have convinced the department that these harms could not exist as we know them today without the role of the online information environment. Although evidence is still emerging, the same is suspected to be true of NIEV, not least given the prevalence of extreme violence content (EVC) online and emergence of toxic online communities which thrive on the exchange, consumption and in some cases creation of such content.

186. In Section F below, I explore the Home Office views on the role of the internet and social media in more detail. It is important to note that the online environment is relevant to almost every aspect of the NIEV issue and the work being done in relation to it, but I have dealt with it in one section for ease of reference.

Effectiveness of interventions to prevent non-ideological extreme violence

187. There is no clear evidence based framework for what interventions reduce risk in individuals with violence fascination and / or individuals identified at risk of committing NIEV. Although it is possible on a more granular level (case by case) to identify interventions which have, whilst not fully mitigating an individual's risk, reduced that risk, Some examples of these interventions are supporting an individual to obtain work, identifying mainstream hobbies or interests that provide a positive focus, helping with social integration to overcome social anxiety and isolation, integration into faith communities and supporting positive faith engagement. The task of assessing the success of interventions however is inherently difficult in all fields because a successful outcome is defined by the absence of an event that may never have occurred in any event. Whereas in Prevent there is now a widely understood or agreed approach to changing behaviour or measuring impact over time, that is not currently the case for

NIEV. As a result, local professionals may feel ill-equipped to act, referrals may stall or rely on generic safeguarding provisions and there is a risk that individuals may continue to escalate towards extreme violence (see e.g: VFI Strategic Issues Paper for XWH, Issue 4 **[JE/047 - HOM000345];** GO-Science Internal roundtable 5.3.25 – detection of VFIs **[JE/031 - HOM000349];** HSAI Rapid Review: Interventions for Violence Fixated Individuals February 2026 **[JE/061 - HOM000440]**).

188. Nonetheless, a mixture of anecdotal, clinical and emerging empirical insights suggest that existing interventions can be effective. The evidence supports that behaviour-based, multi-agency, individual interventions that scale with assessed risk are more likely to be effective than predicitive profiling or punitive measures alone. However the system is fragile and dependent on what interventions are available and can be delivered to support those who are vulnerable. There is a need to conduct robust evaluations of available interventions in order that resources are effectively targeted, and that unintended consequences of poorly understood interventions are avoided (see: GO-SCIENCE interventions workshop 27.5.25 **[JE/044 - HOM000353];** HSAI Rapid Review: Interventions for Violence Fixated Individuals February 2026 **[JE/061 - HOM000440]**).

Limitations of powers to require engagement or impose interventions

189. Channel is a voluntary process and there are no powers under the current legal framework to mandate or impose engagement with the process or specific interventions (as to the legal framework see paragraph 93 above). An individual who has declined to engage with Channel and is being managed under a Police-Led Partnership cannot be compelled to engage with a specific intervention. This is also the case for individuals managed under MAPPA, unless there are specific conditions on their criminal sentence or any order managing them in the community, or under Potentially Dangerous Person Panels.

190. In the absence of parental consent the current legal framework does not allow for mandated engagement by children and young people in Channel. The Home Office has considered the possible application of Gillick competency principles (principles in medical law used to determine if a child under 16 can consent to their own medical treatment in the absence of parental consent or knowledge) to permit under 18s (within an age range) to provide consent on their own account, but the restrictions in the Counter-Terrorism and Security Act 2015 do not permit this flexibility.

191. Prevent's aim is to stop people becoming terrorists or supporting terrorism. It does this by helping and supporting those who are assessed to be at risk of radicalisaton, and is premised on the view that this key focus is far more likely to be achieved if an individual engages with the process willingly. However, where an individual's conduct escalates and may pose a risk to others (e.g. a terrorism risk or risk of serious harm to others), there are counter-terrorism tools available that may offer capability to mandate attendance at appointments, including those led by Prevent intervention providers. These include Terrorism Prevention and Investigation Measures (TPIMs), YDOs for individuals under the age of 21 (when in force), and Serious Crime Prevention Orders (SCPOs). It would follow that if ultimately government were to legislate for a new civil order to manage those assessed to pose an equivalent NIEV risk of serious harm there would be scope under such orders to mandate activity requirements, including potentially attendance at appointments, but the efficacy of any such new power as an early intervention preventative tool would be in part a function of the thresholds or qualifying criteria for its use.[22]

Data and information sharing

192. There are two matters I wish to highlight under this heading.

193. First, as I have set out above, we are trying to develop a policy response to NIEV risk on limited evidence - not about the existence of the NIEV threat, but about the scale of it, how it manifests, whether it is growing and how the risk can be mitigated. We assess that this is a relatively new and emergent threat, that is changing at pace as the online environment evolves, but another issue is the challenge we have in drawing on data outside of Prevent, which may be held across a range of public services.

194. Thus our ability to identify, collectively, NIEV risk in casework, and associated risk factors, characteristics and behaviours or to assess the utility of interventions is inhibited by issues with data sharing and data synthesis across central and local government and public services. As **T1D*** explained, some of the most significant barriers to data sharing are cultural (e.g. risk aversion as departments or organisations do not trust each other

***Cabinet Office Body**

[22] The thresholds for civil orders vary by context. Some require conviction or proof, to the civil standard, of an act that is criminal. For others, the threshold is more flexible. For example a Sexual Risk Order (s.122A of the Sexual Offences Act 2003) provides for conditions to be imposed on individuals who have not been convicted of a sexual offence but who have, on the balance of probabilities, engaged in an act of a sexual nature, and that as a result the court is satisfied it is necessary to make an order for the purpose of protecting the public from harm.

with their data or misalignment of incentives, where the department or organisation sharing the data or funding the resource to undertake it does not always benefit), or technical (e.g. differing data quality, interoperability of systems), but some are perceived legal and governance issues (e.g. convoluted data sharing processes that are difficult to understand can lead of themselves to risk aversion, lack of understanding or confidence in other's arrangements) and ethical (e.g. fear of stigmatising individuals) (see: T1D* Report June 2025 'Violence Fixated Individuals: Analysis and next steps' **[JE/052 - HOM000367];** Letter of 28.1.25 to Home Secretary from ACSO, NPCC and NCA **[JE/020 - HOM000254]**).

T1D*=Cabinet Office body

195. Second, our efforts to prevent extreme violence (and to learn from it when it occurs) are severely hampered by poor information sharing. The root of some of the issues are the same as those I have identified above, in particular:

1) As the failures in relation to AR demonstrate, cultural reluctance concerning preventative information sharing continues to be a problem (see e.g. VFI Strategic Issues Paper for XWH, Issue 7 **[JE/047 - HOM000345]**).

2) The technical / practical barriers are likely to be signficiant. Our current understanding is that across different safeguarding, public protection and health systems there is no common standard for recording or sharing information about individual cases. Thus, even where information is shared it is not easy to process, and usually has to be done manually because systems are not interoperable. The challenge is therefore partly one of capacity to process information as much as willingness to share it. That is not an easy problem to solve. Although superficially the problem points to the attraction of some sort of national case management system for violence it is hard to see how that could be achieved practically. No one organisation or structure is mandated to hold such information for the benefit of others, and even if there were a mandate, the attendant challenge is that no one organisation can afford to make the necessary investment to develop, and operate, an appropriate technical solution which would – by the very nature of the breadth and sensitivity of information it would hold about a large number of individuals, require significant controls and assurance. This challenge in particular is relevant to my later consideration in section H of Lord Anderson's recommendation in relation to the proposal for a 'Big front Door'.

3) Related to the above, there are legal questions as to how a multi-agency central repository, presumably accessible to those outside law enforcement, holding the personal data of non convicted persons, could meet the requirements of Article 8 of the European Convention on Human Rights (ECHR) and data protection legislation.

Regional variation

196. It is clear there is significant regional variation both at a structural and operational level in the frameworks and practices that may play a role in mitigation of NIEV risk. The Below Thresholds pilot (which considered onward support provided to individuals who did not meet the Prevent threshold and where a risk of violence or a concerning interest in mass violence has been identified - see paragraphs 345 - 348 below) demonstrated the variance of local operational landscapes and practitioner experience (see Below Thresholds Pilot Evaluation Report February 2026 **[JE/071 - HOM000445]**).

197. However, it is important to emphasise that one of the strengths of Channel is that there is a specialist team (CTP officers) to receive referrals and progress those referrals into a local multi-agency forum that is underpinned by a statutory duty. While local capabilities and capacity do impact how cases are managed and how interventions are applied, the regional infrastructure developed for Prevent is an advantage in case management. Consequently, as we work to develop consistent practice it will be necessary to develop clear frameworks and standards that allow for sufficient flexibility for local practitioners to determine the most appropriate mechanisms for management of the risk, based upon local resources and structures.

Law enforcement challenges

198. The challenges to law enforcement connected with non-ideological violence are significant and it is critical that government works closely with law enforcement partners in developing the framework for identifying and managing the risk. These will be addressed in detail by CTP and other police colleagues in their evidence to the Inquiry but at a high level they include:

1) The pressure on the CT system and in Prevent teams, caused by various factors including competing priorities, the increase in Prevent referrals following

the Southport attack and the lack of clarity over management of NIEV risk cases, and the attendant risk to the quality of decision making;

2) The increasing challenge in distinguishing between terrorist and non-ideological violence cases;

3) The ongoing challenges, in part due to existing statutory thresholds, in securing prioritisation by local services for the NIEV cohort per the NSC's decision;

4) The difficulties in detecting planned acts of NIEV as it is generally less networked, the less sophisticated attack methodology reduces opportunities for detection;

5) Existing civil orders (and the prospective YDOs) and the controls/risk management function they provide do not sufficiently cater for the NIEV cohort, primarily because they are only available to those who are over 18 or who have already committed criminal offences.

(F) THE ROLE OF THE INTERNET AND SOCIAL MEDIA

199. In this section, I describe first the Home Office's current understanding of the role of the internet and social media in influencing and enabling NIEV offenders to prepare and carry out violent attacks, particularly the impact of EVC online. I explain the work that has been done and continues to be done in relation to terrorism, from which lessons are likely to be applicable to NIEV. Finally, I set out the further work which is currently underway and which is planned on these issues.

Extreme Violence Content (EVC) online

200. There is a huge volume of EVC online, defined in this context as material which depicts real-world acts of violence and resulting injuries against humans or animals, depicted clearly and in graphic detail.

201. Examples may include first-person perspective videos of mass casualty attacks such as the Christchurch shootings, high quality CCTV footage of stabbings or other attacks, or animal torture content produced for sale online. Consumption of EVC has become more mainstream, including on platforms such as Instagram, where posts sharing EVC and gore material have millions of views. Bespoke platforms for EVC, often referred to as

'gore websites', also exist to share particularly graphic EVC, often with little or no safeguards or access requirements. Recent research indicated that the top 24 gore websites collectively receive over 1 million monthly visits from UK users.

202. EVC is strongly linked to a number of violent and dangerous online communities (VDOCs), which is an umbrella term currently used by the UK to capture a range of overlapping online threats such as those posed by Com groups, communities interested in nihilistic violence or misanthropic violence, and others obsessed with violence for the sake of violence, rather than for a political, nationalistic or religious end-goal. EVC is a prominent feature of VDOCs including including mass killing fandoms, sadistic online extortion networks and gore networks, whether as a blueprint for violence (such as livestreamed attacks), a form of social currency, or to shock, entertain and desensitise users to graphic violence.

203. While the role of EVC in driving, motivating or encouraging violent acts is unclear, the prominent role of gore in several recent NIEV cases, such as the Inquiry's Case Study C, suggests a connection. These individuals show a persistent, intense preoccupation (or fixation) with violence, violent ideation or violent acts, often accompanied by obsessive rumination, emotional investment, or fantasising about committing violence. While fixations of this type pre-date the internet in the behaviours of violent perpetrators, the ability of susceptible individuals to access, create and share this material, and the potential to reinforce fixated behaviours, has become immeasurably easier.

204. The operational experience, in particular of CTP, is that there is "*a direct line of sight between online consumption of harmful materials and the risk someone poses*" and there is consensus that the online environment acts as an accelerant and enabler to the risk of both ideological and non-ideological violence, but there is work to be done to understand better the correlation between exposure to violent material and the motivation and capability of individuals to commit extreme violence and in what circumstances that risk is more likely to materialise (see: CTP comments on VFI Strategic Issues Paper for XWH 29.5.25 **[JE/072 - HOM000350]**; Kings Speech 2026, p.117 (National Security Bill) **[JE/073 - HOM000509]**).

205. An ongoing preliminary synthesis of the literature being conducted by CT-ARC at present suggests that violence fixation / fascination more broadly is pathway relevant but not universal across cases of mass violence (NIEV) and terrorism offending. Its relevance to risk assessment should focus on its function (for the individual) and its role in escalation or mobilisation to violence. Important research gaps remain regarding psychological

processes around violence fixation, how they relate to escalation and what it means for interventions.

206. In some cases, repeated exposure to EVC may lead to desensitisation and seeking more violent content. However, desensitisation has not been established as a causal factor in violence and the evidence for the impacts of exposure to EVC online is sparse and of low quality. Most people exposed to EVC do not commit violence. Research on exposure to violent media more broadly suggests that any effects are unlikely to be direct: instead they are likely to be mediated or moderated by person-based factors and environmental variables. Factors such as engagement with specific online communities, the context behind consumption of EVC, or collective consumption of EVC should be considered (see: NCA Paper February 2025 'Understanding the Scale and Severity of Online 'Com' Extortion Networks' **[JE/066 - NCA000019]**).

207. Known NIEV offenders comprise a very small cohort, making it unfeasible to generate statistically meaningful conclusions from their actions, even if extensive data is gathered on those individuals. While some associative links have been identified through case study analysis, the rarity of extreme violent acts again makes statistically meaningful conclusions difficult. It is highly challenging to design an ethical and statistically valid study that could establish causation and effect sizes between online and offline behaviours for any kind of violent outcome (see: GO-Science VFI Extreme Violence Impacts Roundtable Note **[JE/045 - HOM000347]**).

208. Equally, whilst long periods of online exploration and research of violence may be a predictive indicator in an individual, broad online surveillance alone is unlikely to generate useful predictive value for non-ideological violence because there is now so much EVC online. Additionally, an approach of broad online surveillance is highly impractical due to the scale of this material and engages the UK's responsibility to protect fundamental rights and freedoms under the ECHR. The use of covert investigatory powers must be justified on the principles of necessity and proportionality. For example, under Part II of the Regulation of Investigatory Powers Act 2000, relevant public authorities can seek a directed surveillance authorisation to undertake pre-planned covert surveillance that is likely to result in the obtaining of private information about a person. However, its use must be considered necessary under specific statutory grounds (e.g. preventing or detecting crime) and the proposed activity must be proportionate to what is sought to be achieved.

The effect of online platforms and communities

209. In light of this, the Home Office has been doing work to understand the ways in which online platforms, algorithms, design features, recommendations, systems anonymity and niche online communities may contribute to fixation, escalation and attack planning.

210. We have a broad understanding of the ways in which the online environment may contribute to NIEV, beyond those who might be fixated with extreme violence. Based on existing evidence, perpetrators of NIEV range from those heavily engaged in violent online subcultures, to those who more passively engage in those spaces or with violent material online, to those with a limited online footprint. The way in which platform features and dynamics contribute to fixation, escalation and attack planning is therefore highly individualised.

211. **Algorithms and recommender systems** may drive online users towards increasingly extreme content that reinforces their inferred interests. As a primary ecology shaping young people's environment (especially for vulnerable individuals), online platforms may play a role in shaping their behaviour through normalisation and personalisation of violence. This may happen through at least three common features and design choices. First, algorithms that push more of the same or similar content to users to what have actively sought out. Second, algorithms that push more extreme or intense versions of those forms of content. Third, algorithms that push to users content that is not related to what they have sought out at all.

212. This dynamic has been catalysed since the adoption across platforms of the 'For You' style page (used prominently by TikTok but now also used by many other platforms) where feeds are curated by algorithmic amplification rather than the accounts followed. This has intimately shaped an individually tailored experience for all social media users whose personal interests and in some cases grievances, however extreme or problematic, are facilitated through the design of algorithmic reinforcement. Users can be fed increasingly extreme content (due to its tendency to be more engaging) without the need actively to seek it out. This has likely driven the growth of highly personalised and hybridised extremist belief systems. TD1 TD1 **[JE/074 - HOM000497]**; TD1 TD1 **[JE/075 - HOM000496]**) indicated this dynamic is present for youth accounts on TikTok and that extreme non-ideological content such as that glorifying school massacres is actively fed to users (although note this predominantly reflects the experience of accounts that have actively sought this content out, rather than assessing

exposure risk for ordinary users with no prior interest in extremist or violent content). However, further research is needed to understand the role of these dynamics in contributing to escalation of harms or violent mobilisation.

213. Escalation towards NIEV offending does not have to be tied to any one distinctive violent subculture, but there are some observable trends in how violent **online communities** appear to have contributed to NIEV attacks. Violent online communities likely mobilise individuals to violence through offering powerful solution-oriented frames for individual-level grievances and unmet needs. Prominent online subcultures that have been associated with offline violence in the last 10 years including violent misogynistic spaces, school massacre fandoms and coercive online networks. These subcultures are characterised by misanthropic framings that seek to instrumentalise the grievances of vulnerable online youths, primarily social isolation, resentment, and fatalism. They are participatory communities that can offer agency, power and notoriety to those willing to perpetrate extreme violence. The influence of these online communities (especially incel and True Crime communities) has been made explicit in the manifestos, diaries and attack methodologies of some mass violence perpetrators who signal their desire to be memorialised and celebrated by their subcultural ingroup. In these cases, violence appears to be driven by an individualised desire for notoriety rather than in pursuit of any ideological goal.

214. Risks emerge not just from the consumption and sharing of EVC online, but its aestheticisation, commodification and gamification within violent online ecologies which can shape and incentivise harmful behaviours. This is a particular feature of some sadistic and coercive online networks where the suffering of victims is turned into content which can be traded for other content or for status within the social network. This incentivises the creation of self-harm and even suicide content that can be-repackaged into accessible compilations of harm (called 'lore books'). These networks simultaneously create competitive gamified dynamics where players compete for 'points' which are awarded for progressively extreme acts. See further, for context on the Com network, for example, **TD1** **[JE/076 - HOM000498]**.

215. In these violent subcultures, violence is often trivialised through the use of memes and humorous edits that celebrate perpetrators of mass casualty attacks and mock their victims. Visual aesthetics become a primary medium of belonging where the creation of unique and engaging violent content signifies an individual's identity and position within the social hierarchy. Escalating anti-social behaviours are also shaped through the 'gamification' of violence. 'Saints culture' (the veneration of mass casualty perpetrators)

for example has infused across a range of violent subcultures including incels and school shooters, which is characterised by a competitive dynamic where "high scores" (how many are killed) shape a hierarchy of violence, encouraging the desensitisation towards and trivilalisatoin of, extreme violence. Real-life violence becomes a video game where online audiences value entertainment, inspiring copycat violence that is necessarily performative and spectacular.

Pathways from online activity to real-world harm

216. Understanding of the pathways between online activity and real-world harm is still developing (see Clemmow & Ors 'Pathways into Violence-focused Online Communities: Examining Configurations and Temporal Patterns of Motivational Drivers and Risk Factors' **[JE/077 - HOM000500]**). Existing understandings of pathways is orientated primarily towards terrorism. Research specific to the NIEV cohort, both internal government research and external academic, is limited and still in progress. The NIEV policy team will be working with CT-ARC to think through risk assessment and indicators for the NIEV cohort in the coming months. A working assumption has been that many of the mechanics governing the NIEV cohorts and pathways to violence will be similar to those for terrorism cohorts.

217. A key principle within terrorism research is *equifinality* (see e.g Clemmow and Ors 'The Whole Is Greater than the Sum of Its Parts' (2024) **[JE/078 - HOM000532]**) the idea that there are multiple pathways to common outcomes such as terrorism or other forms of mass violence. Online activity is highly likely to play different roles in different cases. Online participation may vary greatly between cases. Some attackers may be heavily embedded in online subcultures, others may be passive 'lurkers', still others may arrive at their attack plan independently of any online influence, drawing instead on previous attackers documented through mainstream media.

218. Research considered by RICU on school massacre suggests that the ultimate goal of such violence is in the restoration of agency TD1 TD1 **[JE/079 - HOM000390])**. In many cases attackers may view themselves as marginalised and victimised by individuals, institutions, and wider society. Crucially, this rests on self-perception rather than objective measurement. In the school massacre fandom previous attackers are memorialised, and in some cases celebrated, as examples of actors who took violent action to address their grievances. Attackers can take inspiration from previous attackers with whom they identify. It should be noted that some of the content in school massacre spaces is 'dual use'. Well-meaning content such

as documentaries and research can easily be repurposed by participants in digital subcultures to further populate the subculture.

219. In some cases, online activity can more directly drive real-world harms. The 'Com' networks (see further below at paragraph 253) incentivise participants to engage in real-world harms ranging from online extortion to encouraging suicide and livestreaming murder. In this subculture providing such extreme content is often required for group membership and to remain active within groups. Although group membership may appear insignificant to outsiders, for those invested in the subcultural aspects of Com groups it can provide significant psychological rewards such as recognition by peers and a chance to demonstrate mastery.

220. The Home Office has engaged in some analysis to develop a better understanding of indicators of escalation towards violent mobilisation. This analysis will be published in August 2026. It is focused on proximal warning behaviours: late-stage indicators that a case may be moving towards violence. This analysis draws on threat assessment type approaches to risk management. Such approaches recognise that there is no single profile of a potential attacker and instead focus on identifying behavioural indicators that a person may be preparing to engage in violence.

221. The available research evidence suggests that leakage (defined variously in the research evidence base but understood here as the accidental or deliberate disclosure of information about a planned attack), is relatively common amongst a variety of lone mass attackers (e.g. Gill and ors, 'Pre attack behaviour in mass shooters' (2017), **[JE/080 - HOM000340]** see numbered page 712). Research on school massacre perpetrators in the US, carried out by the US Secret Service, based on a sample of 41 incidents between 2008 and 2017, found that most of the attackers (n = 29, 83%) shared verbal, written, visual, or video communications that referenced their intent to carry out an attack, threatened the target, and/or threatened others (U.S. Secret Service National Threat Assessment Center, 'Protecting America's Schools' (2019) **[JE/081-HOM000495]** at numbered page 37).

222. There is less evidence available on other potential warning behaviours such as acquiring weapon and hostile reconnaissance of targets although such behaviours are present in commonly used frameworks for terrorism threat assessment such as Terrorist Radicalisation Assessment Protocol 18 (TRAP-18), a structured professional judgment tool for assessing individuals who may engage in lone-actor terrorism **[JE/082 -**

HOM000499], or the list of mobilisation indicators published semi-regularly by the FBI **[JE/083 - HOM000493]**.

223. The analysis RICU are undertaking referred to in paragraph 220 above (due to be published in Augsut) will also consider the importance of encouraging bystander reporting and the multiple potential barriers to reporting concerns to authorities. These include a potential lack of trust in the authorities, a desire to avoid incriminating individuals, and the risks of siloing between authorities. See on this topic, for example, Grossman and Thomas 'Reporting on Terrorism: Bystanders Vs Social Intimates' (2020) **[JE/084 - HOM000531];** Thomas and Grossman 'Community Reporting Thresholds' (2017) [**JE/085 - HOM000536];** Eisenman and ors, 'Bystander Reporting to Prevent Violent Extremism and Targeted Violence' (2024) **[JE/086 - HOM000533].**

224. This analysis will also examine how different threats can be triaged and which threats are more credible, cautiously suggesting that greater weight should be given to threats that are more detailed, and behaviours that demonstrate practical preparation.

225. Finally, this analysis will offer some insight into why individual attackers leak information, even where it may damage their planned attacks. For those planning mass casualty attacks as a way to restore agency in the face of perceived indifference and humiliation, issuing threats offer an opportunity to try out new and more powerful identities before engaging in an attack.

226. Although members of sadistic online harm networks do not typically engage in the kind of mass violence seen at Southport, many of the actors within them may potentially fit the definition of NIEV. Research specific to the Com network is also beginning to emerge (see: Clemmow & Ors 'Pathways into Violence-focused Online Communities: Examining Configurations and Temporal Patterns of Motivational Drivers and Risk Factors **[JE/077 - HOM000500]**), although it is still at an early stage. Recent work by University College London (which has not yet been published) has begun to explore pathways into different aspects of the Com network, albeit through a small sample of 29 individuals (**[JE/077 - HOM000500]**).

Sharing of information by police, Prevent and other agencies about online behaviour

227. There are reasonably well-developed mechanisms for sharing information about concerning online behaviour where it emerges in the course of a live investigation by police or other agencies. For example, if the NCA are leading an investigation into CSEA

and come across worrying patterns of behaviour, then information will be shared with local police forces to enable them to take appropriate action. A similar approach is taken in relation to terrorism and other harms.

228. However, the Home Office is not aware of any systematic attempt to analyse post-conviction offenders' online behaviour prior to their offences, nor to make that available in any meaningful way that could inform policy formulation. The Home Office does look at the sentencing remarks of, for example, those convicted of terrorism offences, to spot any patterns in the material offenders have been viewing, but this is limited in terms of the analysis that can be performed. There is also ad hoc engagement with the police on specific cases at times. However, there is nothing more consistent, system-wide or in-depth in place.

229. This is due to practical problems in terms of collating and analysing the relevant data. There are also significant resource constraints on police and other agencies, who understandably and rightly prioritise finite resources on live operations and ongoing investigations. It would take considerable additional funding and organisation to put in place a system, but it is an area for potential improvement were that to become available.

Existing work on online harms in relation to terrorism

230. The Preventing Radicalisation Online (PRO) team works to prevent individuals from becoming radicalised by reducing the availability and accessibility of radicalising content which is used to radicalise, recruit or incite terrorism, reducing permissive spaces for terrorist and extremist activity and identifying individuals susceptible to radicalising narratives, in order for the appropriate support to be provided. PRO does this by engaging directly with industry partners, the online safety regulator (Ofcom), UK law enforcement and agencies, international partners, the private sector more widely, and civil society organisations. It includes monitoring the availability and prevalence of terrorist and violent extremist content across major platforms, working directly with companies to secure the removal of radicalising content that breaches their terms of service, and working directly with law enforcement to help restrict access to terrorist material. It also includes work in gaming and other online social spaces, where there is evidence that extremists exploit platform features, content and communities to reach vulnerable people.

231. Alongside that, PRO is piloting a number of ways to better spot people online at risk of radicalisation and intervene early to ensure they receive appropriate support, diverting

them away from the risk of terrorist offending. Taken together, this work is aimed at reducing exposure to terrorist and extremist content, making online spaces less permissive to extremist activity, and improving our ability to identify and support people who may be at risk of radicalisation.

232. In practice, the work is delivered through a combination of evidence-gathering, direct engagement with platforms, and targeted interventions. This includes commissioned reporting on the availability of terrorist and violent extremist content, work with the Counter Terrorism Internet Referral Unit (CTIRU) and broader law enforcement, engagement with platforms where content appears to breach the law or their own terms of service, and pilot activity to identify people at risk online and test earlier interventions.

233. This work has developed over several years, through phases of engaging with industry and setting the overall legal framework, then working with the regulator to support them in implementing that framework, preparing iterative improvements to the system, and then more specific projects and measures targeting individuals or particular problems. I do not want to suggest that in relation to terrorism the Home Office considers the current system is sufficient. On the contrary, our view is that there remains much to do and the picture is always evolving. However, we have learned a lot and developed a lot of thinking through this work.

234. While PRO's efforts are focussed on radicalisation to terrorism, the Home Office assesses that similar activities would also go some way to addressing the NIEV risk online; in particular, the efforts to reduce exposure to online content and to identify individuals susceptible to radicalising narratives, in order for the appropriate support to be provided. For that reason I provide here a significant level of detail about the current work of PRO (see: summary from 19 February 2026 **[JE/087 - HOM000504]**).

<u>Reducing exposure to online content which is used to radicalise, recruit, or incite terrorism</u>

235. PRO has commissioned an ongoing series of reporting relating to the accessibility and prevalence of Terrorist and Violent Extremist Content (TVEC) across several "Big Tech" social media and gaming platforms to understand fully the threat faced by platform users. These reports focus on platforms that have a large UK userbase and extensive audience reach. This reporting enables PRO to baseline accessibility and prevalence of TVEC, and to measure changes on platforms over time. It also provides an evidence base for engaging tech companies, to enable fruitful conversations and meaningful change to

reduce the accessibility to likely TACT (Terrorism Act) breaching content across these platforms.

236. PRO continues to work with platforms to secure the removal of TVEC as it relates to violation of platform Terms of Service (TOS), in the absence of a clear statutory definition of illegal terrorist content at present. An example of how PRO does this is through sharing a list of content directly with platforms, following a recommendation made by the Independent Reviewer of Terrorism Legislation in 2021. This list, owned by CTP, provides details of content that has formed the basis of successful prosecutions (that is, a defendant has pleaded guilty or been found guilty by a court of a terrorism offence based on this content) under s.2 of the Terrorism Act 2006 (dissemination of terrorist publications) and s.58 of the Terrorism Act 2000 (collection of information for terrorist purposes). These documents cover topics ranging from ideologically motivated propaganda to munitions and homicide methods. This is not an exhaustive list of terrorism content.

237. Where harmful but lawful radicalising content may breach a company's terms of service (TOS) we share the evidence and our concerns about its potential impact and ask companies to review the content against their TOS with the expectation that they will act in line with their stated policies.

238. However, we recognise that the fundamental issue is one of scale. The volume of potentially harmful terrorist content available online vastly exceeds the capacity of governments and law enforcement to identify it reactively and then seek its removal. Therefore, we are taking forward a pilot to be delivered by the end of the 2026/27 financial year that will use innovative AI tools to identify proactively terrorist content at scale and then bulk refer this content to technology platforms for removal in line with their terms of service, working with a civil society organisation subject to commercial processes, with the relevant expertise (see e.g. Information To Note 19.2.26 'Proactive approach to target and takedown extremist and illegal terrorist content' **[JE/087 - HOM000504]**, paragraph 5). The pilot will help evidence the problem, support implementation and enforcement of the OSA and inform longer-term decisions on in house Home Office capability.

239. PRO manages a URL Filter List. This is a dataset containing approximately 15,000 URLs assessed by the CTIRU as breaching UK terrorism legislation, which vetted organisations can use to identify and restrict access to terrorist content online. It is provided free of charge to vetted organisations, including local authorities, education and

healthcare bodies, as well as selected private companies, to support them in meeting their Prevent duties.

240. The CONTEST Unit and DfE are working on a project to strengthen both the consistency and safeguarding application of filtering and monitoring software in schools. With schools already using filtering and monitoring tools to generate alerts on harmful or extremist content, the project work is focused on ensuring clearer national expectations for how these alerts are acted upon, including their regular consideration by Designated Safeguarding Leads and school leadership. The project aims to strengthen guidance, standards-setting, and support for schools, to drive greater consistency in how filtering and monitoring are implemented and how insights from them are used to identify risk. This is complemented by wider work to build resilience to online harms through curriculum, teacher training, and resources such as Educate Against Hate so that schools are better equipped both to detect and respond to emerging concerns. These measures complement wider government action, including the recently announced ban on social media for under 16s and that certain harmful features on other online services like livestreaming and strangers contacting children will be restricted for under 18s.

241. The Home Office works closely with the CTIRU to maintain and fund a website which allows members of the public to report, anonymously, online material promoting terrorism or extremism.

242. Another aspect of PRO's work focusses on gaming. Online games and gaming adjacent services are social spaces and provide generally beneficial experiences, but also opportunities for harm as they can provide access to a large group of highly engaged individuals, including young people. Research into violence in video games has not found there to be a direct correlation to off-line violence (see e.g Przybylski and Weinstein 'Violent video game engagement is not associated with adolescents' aggressive behaviour' (2019) **[JE/088 - HOM000521]**; American Psychological Association (APA) Task Force on Violent Video Games October (2019) **[JE/089 - HOM000522]**), but there is evidence of terrorists and extremists being active in and exploiting gaming spaces, and the presence of extremist and terrorist content. For example, terrorists and extremists have been known to build their own games, modify existing games, gamify extremist content, exploit connectivity functions for recruitment and take advantage of the financial incentives some games provide.

243. As youth radicalisation within gaming spaces rarely begins with overt ideological content, work with gaming companies includes supporting the identification of coded signals,

recreations of violent attacks and profiles and characters that glorify previous attackers, including school shooters – all of which can signal in interest in terrorism and act as an entry point towards radicalisation. T1B

T1B

244. PRO has compiled evidence of the availability of extremist and terrorist games and modifications on various gaming marketplaces and distribution services. These games and modifications allow players to re-enact mass shootings and terrorist attacks, or introduce extremist and terrorist related symbols or uniforms into existing games. PRO is now exploring the use of different voluntary and regulatory levers to seek their removal. For example, a user modification of a published game may breach a service's acceptable use policy or intellectual property laws. T1B

T1B

Reducing permissive online spaces which allow for terrorist and extremist activity

245. PRO continues to develop its relationships with a wide range of platforms, including those identified T2D through in-house analysis as posing the greatest terrorist threat online. PRO actively pursues the takedown of terrorist content, groups and channels across platforms of concern, sharing evidence to support platform enforcement with the aim to make platforms more hostile to terrorist groups and their activities.

246. PRO has developed a dedicated workstream focused on Terrorist Operated Websites and is currently assessing best-practice approaches used by international partners to inform how the UK counter-terrorism system can most effectively disrupt them. T2D

T2D

T2D PRO leads engagement with Internet Service Providers to disrupt these websites at source, focused on platform removal as a primary goal.

247.

T1B

T1B

248. Ofcom's duties and powers under the Online Safety Act 2023 play a critical role in preventing radicalisation online by holding platforms to account and driving improvements in systems and processes that reduce users' exposure to terrorist and violent content and activity. PRO shares regular updates on specific examples of content that breach the law or platform TOS, platform specific evidence and insights on terrorist exploitation online to inform Ofcom's risk assessments and to help the regulator set out more robust and proactive recommendations in its codes of practice.

Identifying individuals susceptible to radicalising narratives, in order for the appropriate support to be provided

249. Identifying susceptible individuals online is a significant area of development. Anonymisation online makes it very difficult for third parties to identify individuals, even where it is established that an individual online user should be referred to Prevent. This challenge can be exemplified by the fact that, for example, a child may be identified and referred to Prevent in the light of concerning behaviours in a educational setting, but the same child might display those same concerning behaviours online, in open forums, and might never be identified as a risk, let alone referred for support or intervention.

250. PRO has secured funding for T1B, E, F to be delivered by the end of the 2026/27 financial year, aimed at identifying individuals online at risk of radicalisation to violent extremism through behavioural indicators (see: paragraph 4 of Information To Note 19.2.26 **[JE/087 - HOM000504]**). T1B, T1E, T1F T1B, T1C. The T1B, E, F pilot (independent of industry) will leverage paid advertising by deploying specially designed content across multiple platforms to reach at-risk audiences and concerned bystanders, connecting them to confidential, non-law enforcement support. T1B, E, F

T1B, E, F

T1B, E, F The pilot will be designed to generate robust evidence on how

different intervention models perform in practice and on the role of online communities and active bystanders, such as parents, in enabling early identification and intervention.

251. PRO T1F supported work by the Christchurch Call Foundation to develop and roll-out two UK tailored digital bystander awareness raising and support projects for gaming. The first provides advice to parents, caregivers and educators on the risks of harm associated with gaming and offers tips on how to talk to children about their experiences of online gaming. This is being widely shared via the Department for Education's Educate Against Hate website. The second provides a toolkit for Discord community managers (employed by game companies) and gaming community moderators (volunteer administrators) on how to identify and respond to harmful behaviours within the communities they have adopted a responsibility to keep safe and fun. This includes when it is appropriate to escalate to the platform for more robust action.

252. T1B

T1B Gaming spaces provide an opportunity to intervene before a relationship is moved into a more private space and before a crime may be committed or harm caused, but much of the behaviour in this space may seem relatively innocuous and, therefore, more difficult to detect.

253. The Home Office has also been examining so-called "Com networks" (see Draft Submission (not provided to Ministers) - Proposed Home Office Response to disrupt and dismantle the Com Network' 2.2.26 **[JE/090 - HOM000409]**; Final Submission for Security Minister - Home Office response to disrupt Com Networks 1.7.26 **[JE/091 - HOM000417]**; TD1 **[JE/076 - HOM000498]**). These are online communities associated with a range of serious harms, including child sexual abuse, cybercrime, violence and exploitation. They are often not driven by traditional ideology, but by factors such as status, notoriety and belonging. They represent a distinct but related challenge. Law enforcement leads the operational response to these networks, supported by the Home Office. These networks are associated with a wide range of serious offending, including child sexual abuse, sextortion, cybercrime, fraud, self-harm and suicide encouragement, and in some cases live-streamed violence. The Home Office is working to strengthen the evidence base, develop policy options and consider

further disruption activity. Given the international nature of these networks, this also includes engagement with international partners.

Challenges in identifying concerning patterns of online behaviour

254. PRO shares intelligence products and information on trends such as typical content moderation evasion techniques with companies to support improvements to their trust and safety detection systems. And we expect companies to report credible imminent threats to life / serious harm that may be detected through these systems, or reported by other users, to the police. Many of the challenges which arise in this context are applicable to the NIEV risk as well.

255. More specific challenges for police forces in monitoring and responding to terrorism related pre-attack planning include that evidence may be incomplete or still developing and attribution to an individual can be challenging online. Policing partners have raised significant concerns about the prevalence of online material which may further radicalise NIEV risk offenders. For example, on 28 January 2025 a joint letter to the Home Secretary from ACSO, NPCC and the NCA summarised significant concerns about, and indicated that they were developing thinking on, two new operational initiatives:

> "We will consider whether there is value in better coordinating or consolidating our approaches to Prevent in relation to online crimes, including terrorism, cyber crime, child sexual abuse and other serious crimes – which are currently at very different levels of maturity.
>
> We will explore establishing a multi-agency task force, supported by a fusion cell to bring together an all-source intelligence collection capability, including potentially with industry, against this range of increasingly overlapping online threats." **[JE/020 - HOM000254]**

256. The joint letter also emphasises the need to address the 'supply side', including harmful online content. In response to the concerns raised by operational partners, the Home Office has treated Southport and the Inquiry's findings as requiring a joined-up, system response across prevention, operational disruption, safeguarding and the online environment. This has included work to assess and close gaps in the criminal and regulatory framework (including the work to develop new EVC offences), alongside work with operational partners to strengthen the identification and management of risk where individuals' pathways are shaped by online activity, but do not sit neatly within the statutory tests or operational structures for counter-terrorism.

257. The Home Office ran pilots in 2025 and 2026 seeking to identify people at risk of being drawn into terrorism online (see e.g OSINT (Open Source Intelligence) Pilot Report

19.8.25 **[JE/092 - HOM000442]**). A priority driver of this work is the increase in under 18s engaging in terrorism related activity, and committing terrorist offences, many of which are committed online. Therefore the pilots were focused on identifying people at risk of radicalisation to terrorism and referring them to Prevent. Limitations on this work include the need to operate within all relevant legislation and not stray into surveillance. A further limitation on the possibility of extending this model to NIEV could be a lack of clear signal to look for: there is currently no NIEV equivalent for s.58 TACT, for example.

258. **T1E**

T1E **[JE/093 - HOM000507]).**

Current work on online harms in relation to NIEV

The National Security Bill

259. Following the Southport attack, one workstream for the Home Office involved consideration of the attacker's engagement with EVC online prior to the incident. The distinction between lawful but harmful content and unlawful content, and the thresholds for intervention based on intent and risk, are longstanding features of UK law, particularly in counter-terrorism, where public protection needs to be balanced against freedom of expression. Existing frameworks leave some highly harmful non-ideological violent content outside clear criminal scope. The Southport attack brought renewed attention to this gap, sharpening the case for reassessing where the criminal threshold should sit.

260. The policy work on EVC identified that some of the most extreme forms of real-world violent content can circulate online without falling clearly within existing criminal offences. As a result, such material may remain available online, even where it depicts serious harm and has no clear public interest purpose. Examples include first-person footage filmed during the Christchurch attack by Brenton Tarrant which, when circulated without accompanying ideological messaging or encouragement, does not always fall within the scope of terrorism legislation, despite depicting an act of terrorism.

261. Since July 2024, the overall approach of Government has been to stabilise and implement the OSA as the foundational regulatory regime, whilst in parallel testing

whether additional criminal justice, enforcement or system-level interventions are also required to address harms not adequately mitigated by the OSA alone. The OSA gives Ofcom powers to regulate internet services and places new duties on social media companies and search services to implement proportionate "systems and processes" to reduce risks that services are used for illegal activity and to takedown illegal content. However, it does this by defining illegal content by reference to specified offences found in other legislation.

262. It is vital, therefore, that Government takes urgent action to address potential gaps where particular content, currently not covered by existing criminal offences, is assessed to be causing or inspiring real-world harm. For example, certain types of content depicting extreme violence and gore, including material known to have been consumed by the Southport attacker, would not currently be captured by any risk mitigation measures that platforms must have in place under the OSA. As such, the Home Office has reviewed criminal legislation to identify the creation of a new offence that would cover this type of content and its promotion or dissemination online. In developing this proposal, the Home Office recognised that measures in this area are likely to face challenge, including on:

    1) freedom of expression and civil liberties grounds (including potential Article 10 ECHR challenge), particularly depending on where the offence threshold is set;

    2) whether the definition of EVC is sufficiently precise and workable in practice, including "edge cases" and ensuring appropriate safeguards for legitimate activity (e.g. journalism, documentary reporting, education, research and evidential material);

    3) the strength and limitations of the evidence base, including the difficulty of demonstrating direct causality between exposure to violent content and real-world offending;

    4) the impact on the likely cohort engaged with EVC, including the risk of disproportionate effects on children and young people and the need for appropriate defences / exemptions to avoid over-criminalisation; and

    5) practical deliverability and coherence with the OSA regime, including the timeframes and dependencies involved in designating any new offence as a priority offence and the risk of delay or non-delivery.

263. In response to this problem, the Home Office developed proposals for new EVC offences (see **[JE/053 - HOM000306]; [JE/094 - HOM000364]**). The proposed offences focus on the creation and sharing of content depicting extreme and graphic real-world violence, and synthetic content where it is indistinguishable to real-world violence with the aim of closing a gap in the current law and providing clearer powers for law enforcement.

264. The Government is taking this work forward through the National Security Bill planned for introduction in the second Parliamentary session, as announced in the King's Speech on 13 May 2026. The Bill contains two measures related to the Southport attack.

265. The **first** is the criminalisation of the dissemination and creation of extreme violence content online. The intention is to stop the spread of content that glorifies, trivialises, or normalises serious violence. The measure will enable law enforcement to disrupt individuals who are encouraging violence.

266. The **second** is the criminalisation of planning a mass casualty attack. This will close a gap in the current law by capturing cases where a lone individual undertakes preparatory steps towards a mass casualty attack without an ideological motive. This is not currently covered by existing conspiracy, attempt, or terrorism offences. By closing this gap, the Government intends to strengthen operational partners' ability to disrupt the most serious threats posed by NIEV, and to intervene before such plans result in real-world harm.

267. The Home Office is progressing the first EVC offence measure as a Home Office-owned provision within that Bill, and the Ministry of Justice is responsible for the second measure to criminalise the planning of a mass casualty attack.

268. Home Office officials are working with Home Office Legal Advisers and Parliamentary Counsel to develop the draft clauses, while Ministers consider the detailed design (including thresholds, penalties and safeguards/exemptions) and how the offences will interact with the OSA regime. The Home Office is working with DCMS on the route for ensuring any new EVC offences can be treated as "priority offences" under the OSA, so that platforms' illegal content duties apply once the offences are commenced leading to a reducation in the circulation and supply of this material online at scale. The Home Office is also working with DCMS so that violent content that falls below this EVC offence threshold is considered for upgrade within the Children's Codes in the OSA, from 'Priority Content' to 'Primary Priority Content' which would activate further duties on online platforms to ensure that this material cannot be accessed or viewed by children **[JE/095 - HOM000411]**.

269. Subject to these steps, current planning assumptions propose introduction of the National Security Bill early in the second session. The Home Office continues to draw on the findings from Southport as the Inquiry progresses and as further work is taken forward across government on the online environment, including how EVC is identified and addressed.

270. There are crossovers between EVC and policy development in other harm areas, which may lead to the criminalisation or removal of EVC when linked to other specific harms such as CT. ETSSU is not progressing a distinct piece of work on EVC linked to specific harms or crimes. However, officials have been working on plans to strengthen the removal of terrorist content online (TCO) by updating sections 3 and 4 of the Terrorism Act 2006 as described below.

Takedown powers

271. **T1B**

[JE/053 - HOM000306]. Currently, Government and law enforcement lacks powers to compel a provider of online service to take down specific pieces of illegal content. This leaves the Government or law enforcement potentially exposed in responding swiftly to significant or rapidly evolving harm. This is most relevant where:

1) There are specific high impact pieces of content, for example those which have gained public notoriety or are intended to do so, which have not been caught by existing systems and processes and where it is assessed that swift removal would likely reduce harm to the public;

2) Platforms are unable to adapt their systems and processes swiftly enough to deal with new or evolving types of illegal content and activity; or

3) Where international partners alert the UK authorities to illegal content which warrants consideration of swift removal.

272. There is precedent in existing legislation (Crime and Policing Act 2026) regarding the sales of illegal knives which could provide a basis to update legislation to fill these gaps. In doing so, it should be clear that the primary responsibility for removing illegal content should sit with platforms, for both practical reasons and to be consistent with the current approach in the OSA but introducing a removal notice regime would operate as a backstop in case a platform did not act proactively or refused to remove illegal content

following voluntary engagement. Any new power would not replace or override platforms' duties under the OSA.

273. There is also precedent in US law, where if platforms identify child sexual abuse they must take it down and report it to the National Centre for Missing and Exploited Children (NCMEC) in the US. NCMEC then pass on reports to relevant organisations in other jurisdictions across the globe – in the UK that is the NCA. The OSA also creates NCA as the Designated Reporting Body for referrals of non-US based companies. The Internet Watch Foundation in the UK (funded by tech companies) also has authority to receive reports from the public and to proactively search for CSA material and then work with companies to take down that material.

274. Two options have been considered:

1) Option 1: reform existing powers in the TACT 2006 for terrorism related content. The Home Office has reviewed the operation of section 3 TACT which currently applies to content which would breach offences under section 1 and 2 of TACT 2006. This review concluded that the power had never be used, it was difficult to see how it could practically be used within a modern context (recognising the procedure for using the power was now twenty years old and was unsuitable to the nature of online platforms now), and reform should be considered. In the absence of an effective statutory power to compel technology companies to remove illegal terrorist content, CTP have relied on a voluntary referral model. **T1D** **T1D** (see **[JE/096 - HOM000503]**).

2) Option 2: a broader power which could apply to other types of illegal content, beyond terrorism-related content. **T1B** **[JE/097 - HOM000546]**, **T1B**

T1B

275. **T1B**

T1B **[JE/098 - HOM000406]**. **T1B**

T1B

T1B

276. T1B, T1C

T1B, T1C [JE/099 - HOM000545], T1B, T1C

T1B, T1C

T1B, T1C [JE/100 - HOM000408] T1B, T1C

T1B, T1C.

277. In relation to Option 1, the Home Office has been working on plans to update sections 3 and 4 of TACT 2006 to provide a relevant authority with an enforceable power to require technology companies to remove specific terrorist content from their platforms. This would create a statutory definition of online terrorist content to underpin an enforceable Content Removal Notice (CRN) regime. Initial advice was submitted to the Security Minister on 8 July 2026 regarding the scope of the regime. T1B

T1B

T1B (see [JE/101 - HOM000501]).

The OSA and potential amendment or extension to its powers or duties

278. The OSA provides a significant framework for illegal content and child safety duties. However, the position is more complex for violent ideologies or material that is harmful but lawful, particularly for adult users. Where material crosses a criminal threshold, for example terrorism, threats, incitement, hate crime or other relevant offences, it may be addressed through the illegal content duties. However, this depends on the provider having reasonable grounds to infer that the content is illegal and acting on that assessment. If the Home Office or law enforcement considers material to be illegal, but

the platform does not reach that view, it will not be captured by the platform's illegal content processes or taken down under those duties. The police may investigate and prosecute the person who posted the information but even in those cases there are no powers to enable HMG to enforce the removal of the specific pieces of content if the company disagrees with our assessment. Instead Ofcom enforcement focuses on whether the platform's systems and processes are effective as a whole. The platforms may reconsider where the content is signposted by law enforcement or through other routes.

279. There is also a jurisdictional limitation: the Act applies only to in-scope services with the necessary UK link, so some material relevant to NIEV may appear on overseas, smaller, closed, encrypted or niche services where the Act's legal or practical reach is more limited. Where material is harmful but lawful, the OSA's treatment is more limited and depends on the age of the user, the category of service, terms of service, user empowerment tools and transparency requirements.

280. Some material relevant to NIEV may sit below existing criminal thresholds while still contributing to fixation, grievance, desensitisation or escalation. That creates a policy challenge: broadening regulation could help address harmful ecosystems, but would need to be balanced against freedom of expression, legal certainty, proportionality and enforceability.

281. In particular, the need to protect the right to freedom of expression means that the general approach at present in relation to harmful but lawful content or activity is for the Home Office and other partners to alert providers and platforms to the presence of such material and its potential impact, and then invite them to consider it in light of their TOS.

282. The Act significantly improves the framework but may not fully address all NIEV relevant harmful-but-lawful material, especially where that material contributes to fixation or escalation without meeting a criminal threshold. Further work is needed with DCMS, Ofcom, law enforcement and legal advisers to assess whether additional measures are necessary and proportionate.

283. The OSA's categorisation duties may contribute to the challenge of 'harmful but lawful' content. The legislation sets out additional regulatory duties for some online services that meet the thresholds set out by government (Category 1, 2A and 2B). Ofcom has now published the register of categorised services and is consulting on codes of practice and guidance for industry which sets out how these should meet these additional duties.

284. Category 1 services (now confirmed as Facebook, Instagram, Pinterest, Quora, Reddit, Roblox, Snapchat, TikTok, WhatsApp, X and YouTube) must give adult users more tools to control their online experience, and manage their exposure to certain content and unverified users. These user empowerment tools give adult users the choice to filter out suicide, self-harm, eating disorder, and hateful and abusive content (mirroring some of the protections for children under the OSA's child safety codes). These duties are not yet in force and it will be some time before government can speak to their efficacy. Ofcom are aiming to have their final policy statements on these duties, and corresponding codes and guidance, published by mid-2027 at the latest, though this is only an estimate.

285. To date DSIT has held primary responsibility for the OSA and its implementation, although as set out above (paragraph 46), as part of the Machinery of Government changes announced on 21 July 2026, this will now move to the newly expanded DCMS. The Home Office is responsible for dealing with online harms and threats to national security, so a degree of tension between the Home Office and DSIT perspectives was therefore to be expected. These differences are taken into account when Government as a whole is considering the regulatory environment.

286. On potential amendments to the OSA, DSIT (although see above regarding the intended transition of responsibility for OSA to DCMS) will be able to provide the definitive update on the current government position and any live or proposed changes. There are various potential policy options for consideration, including: expanding priority illegal content where justified; strengthening design / risk duties around recommendation systems and amplification; improving transparency around how platforms handle violent-but-lawful material; and strengthening child protections where violent material is not clearly illegal but is plainly inappropriate for children.

287. Although some wider proposals suggested by the Home Office have not been taken forward at this stage, the recently announced plan to ban social media access for under-16s and other developments such as device level interventions are going a considerable way towards meeting some of the concerns the Home Office has identified. I describe below how the position in relation to the OSA and potential amendments or additional measures has developed over the past two years in a little more detail.

288. In February 2025, officials in DSIT provided advice to Number 10 setting out proposed next steps for online safety policy. The DSIT paper proposed the development of three green papers covering further measures on child safety, issues described as "societal harms", and reducing regulatory burden.

289. While the Home Office agreed that the OSA represented a significant milestone in the Government's approach to online safety, the Home Office view was that the paper did not fully reflect the scale and immediacy of several online enabled risks, and whether the OSA would address them. On that basis, the Home Office prepared and issued a separate paper setting out its position at the end of February 2025, which set out an alternative assessment of the policy landscape and the Government's potential future direction. This included the position that the OSA should be treated as a starting point for further action, rather than the limit of the Government's response, considering emerging evidence and recent events, including the Southport attack of 29 July 2024.

290. Following the submission of the two papers and the differences in approach they highlighted, in July 2025 Number 10 commissioned the Home Office and DSIT to produce a single joint paper. The intended purpose of this paper was to set out a shared view of the Government's broader technology and online safety ambition, and to provide the basis for a future, substantive discussion on online safety with the Prime Minister. This initiated a process lasting several months. **T1B**

T1B

T1B **[JE/100 - HOM000408].**

291. The Prime Minister met with DSIT in November 2025 and indicated support for banning 'nudification apps' and for legislating to expand and tighten definitions of the most harmful terrorism and EVC, while expressing caution about further interventions at that stage, and requested further advice from both DSIT and the Home Office. Following this, a Director General-level discussion was held between the Home Office and DSIT to clarify the input required from each department, and improve cross-government governance to ensure both the Home Office and DSIT were involved in discussions with Number 10 on these policy issues. Home Office advice to the Home Secretary was subsequently updated to reflect the Prime Minister's steers, with a January 2026 readout requesting more specific and targeted proposals. As a result, follow-up work proceeded through implementation-focused advice on specific policy issues and ongoing engagement with DSIT, rather than a single consolidated resubmission to the Prime Minister **[JE/102 - HOM000230]**.

292. Since that time there have been several further developments, primarily the proposed social media ban on under-16s and the announcement of a proposed introduction of device-level interventions focused on CSEA.

Social Media Ban

293. The proposed social media ban represents significant progress in the online harms space, moving from reliance on platform-led safety measures towards a more preventative model of child protection online. The Government has committed to banning social media companies from offering services to under-16s, using a model similar to Australia, and to restricting high-risk features across a wider range of online services. This recognises that risks to children are driven not only by harmful content, but also by platform design and functionality, including algorithmic recommendation, livestreaming, infinite scrolling, stranger contact and AI chatbot functionality. Given the seriousness of the potential harms to children, the policy is also consistent with a precautionary principle: where there is credible evidence of risk, government should act to reduce exposure and prevent harm, even where the full scale or causality of those harms cannot yet be proven with certainty.

294. We assess that the ban is likely to reduce children's exposure to some forms of violent and harmful material by restricting access to major user-to-user platforms, including TikTok, Instagram, Snapchat, YouTube, Facebook and X. It is likely to reduce passive exposure to harmful content on mainstream platforms, which can act as discovery, amplification and normalisation layers for violent, exploitative and age-inappropriate material. In the Home Office's assessment, this is also likely to reduce younger children's exposure to content linked to violence, knives and offensive weapons, grooming pathways, exploitative criminality, and extreme or harmful material which can draw vulnerable users into more serious online ecosystems.

295. The rationale for the ban is not just that children access harmful content on social media, but that harmful features can increase the likelihood, frequency and intensity of that exposure. The Government's proposed approach therefore goes beyond a simple platform-level ban by also restricting harmful features across adjacent services, including gaming and AI chatbots, where similar risks can arise. The Government is also introducing measures to protect 16- and 17-year olds from a damaging cliff-edge by requiring platforms to switch off harmful features such as infinite scrolling, livestreaming and stranger contact by default for this age group. This also includes proposed default overnight social media curfews between midnight and 6am, which users would be able to override.

296. The Home Office has worked closely with DSIT throughout policy development, including through cross-Whitehall engagement and feeding into DSIT-led deep dives with

a cross-Home Office position rooted in operational evidence. The Home Office has supported the overall objective of strengthening protections for children online, while lobbying for the policy to go beyond a simple platform-based restriction. In particular, it has pressed for a broader, harm-led approach which captures high-risk features and functionalities and ensures gaming, AI chatbots and adjacent services are not treated as safe by default where they contain social-media-style or harmful features (see: letters of 11 June and 12 June 2026, which set out the Home Office support in principle but also some concerns **[JE/103 - HOM000505]** and **[JE/104 - HOM000508]**).

297. A key Home Office priority has been ensuring the regime is effective in practice and resilient to circumvention. Robust age assurance and effective enforcement by Ofcom of the ban, as well its existing responsibilities under the Online Safety Act, will be critical. The Home Office has also pressed for greater consideration of VPNs, alternative services, workarounds, enforcement costs and deliverability. Without these safeguards, there is a risk that restrictions may be too easily bypassed, limiting the impact of the policy **[JE/105 - HOM000412]**.

298. However, some of the most serious online harms occur on platforms that are encrypted or designed around high levels of user privacy. This includes both mainstream services and smaller, more niche platforms, making harmful activity harder to detect, assess and disrupt. Large open platforms including popular social media services may act as entry points, but the most serious harm largely occurs after migration into private messaging, encrypted spaces, gaming adjacent environments, lightly moderated forums or other services where safeguarding, moderation and law enforcement visibility are more limited. The Home Office is therefore continuing to work with DCMS (formerly DSIT) to identify how to mitigate displacement risks so that the ban reduces overall harm rather than pushing children into riskier spaces.

299. The next stage is to move from announcement to detailed design and implementation. Further work will be needed on scope, exemptions, high-risk functionalities, age assurance, VPN and circumvention risks, and enforcement. Ofcom is expected to play a central role, including on what constitutes highly effective age assurance, with the first regulations expected before the end of the year and implementation currently expected in Spring 2027. The Home Office will continue to support the direction of travel while pressing for a comprehensive, enforceable and future-proofed regime.

Device level interventions

300. The Government has announced[23] that smartphones and tablets should implement comprehensive nudity detection by default at operating system level – to prevent the taking, sharing and viewing of nude imagery – coupled with age assurance for users to switch it off by proving they are over-18 (see details in **[JE/106 - HOM000512]** and **[JE/107 - HOM000513]**). This builds on existing partial implementations of nudity detection in Apple iOS and Google Android, and device OS-level age assurance on Apple iOS. As such, government is currently engaging with tech companies. The former Prime Minister announced in June that, if companies do not take sufficient action, the Government will legislate **[JE/108 - HOM000336]**.

301. The OSA regulates user-to-user and search services (and pornography providers), requiring those services to assess and mitigate risks and, in some cases, implement age assurance. The Home Office's device-level proposal complements that approach by addressing a different part of the technology stack: the operating system itself. The proposal is an upstream and preventative measure: seeking to stop harmful content being created, shared or viewed in the first place.

302. Much child sexual exploitation, grooming and sextortion begins with the creation of a first nude image. If that image cannot be created, saved, shared or viewed on a child's device, many exploitation pathways become significantly harder to initiate or sustain. Internal law enforcement assessments have highlighted that device-level controls could disrupt grooming, sextortion and self-generated indecent imagery by removing the initial image that offenders rely on for coercion and control (see research at **[JE/109 - HOM000337]**). The proposal is intended to minimise impacts on ordinary users in three ways:

1) Adults can still access legal content if they choose, by proving they are over 18 through age assurance.

2) Detection takes place entirely on-device, with no reporting to government, law enforcement or the company operating the device, and no images leaving the device.

[23] New plans to stop children taking, sharing or viewing nude images - GOV.UK

3) The intervention focuses on preventing some of the highest-harm outcomes associated with child sexual exploitation and abuse, rather than monitoring general online activity. The classifier simply detects nudity.

303. In short, the aim is a highly targeted intervention against a severe harm category, with strong privacy protections and minimal impact on device use.

304. While the proposal has been developed specifically to tackle CSEA and the creation of nude imagery, it may also provide useful insights into the potential role of preventative interventions built into devices themselves.

305. Additionally, age assurance at device-level has significant further potential. Although, for this policy, it is tightly bounded to the deactivation of nudity detection, there are potential other uses for device-level age assurance – for example, reading across to the app store, and as a more secure means to prevent children from accessing social media under the ban. Device-level age assurance may prove to be more convenient, effective and privacy preserving. We are in ongoing discussion about this potential with DSIT counterparts, given we have developed significant policy thinking on this subject.

Longer-term or wider work on online harms of potential relevance to NIEV risk

Age verification for VPNs

306. The issue of how achievable age verification for the use of VPN software would be (or other methods to prevent VPNs from being used to circumvent the age related protections in the OSA) is primarily a question for DSIT (now DCMS) as they lead on online safety policy, but the Home Office can offer a risk-based view.

307. The OSA places duties on in-scope services to protect users from illegal content and children from harmful content, with Ofcom responsible for regulation and enforcement. The Government's Online Safety Act material states that platforms have duties to reduce risks their services are used for illegal activity and to protect children from harmful and age-inappropriate content; Ofcom's material similarly emphasises illegal content risk assessments and safety duties for in-scope providers.

308. VPN use can undermine age-assurance and age-related protections where individuals use VPNs to circumvent safeguards. If VPNs become a significant route through which children bypass age-based restrictions, measures to restrict children's access to VPN services could help reduce this risk. However, VPNs also serve a range of legitimate purposes, including privacy, security and personal safety. Any proposal would therefore

need to consider proportionality, privacy, feasibility, enforceability, potential unintended consequences, and the extent to which restrictions would reduce harmful activity in practice rather than displace it elsewhere.

309. Where VPNs are used to circumvent age-based protections, restricting children's access to VPN services has the potential to provide a significant mitigation against that form of circumvention. Nevertheless, VPNs have a range of legitimate uses and any intervention would need to balance child safety benefits against privacy, security, feasibility and proportionality considerations.

Restricting certain aspects of online access for children in schools

310. The Children's Wellbeing and Schools Act 2026, which introduces various provisions relating to the safeguarding of children including online harms inserts into the Online Safety Act 2023 a new power for the Secretary of State to make regulations requiring providers of specified internet services to prevent or restrict access by relevant children[24] to internet services (or to specified functionalities or other features of such services).[25] The new section 214A of the OSA enables the Secretary of State to make such regulations for the purpose of protecting relevant children from a risk of harm. Section 214A(9) of the OSA imposes a requirement on the Secretary of State to exercise this power to make such provision as they consider appropriate following the conclusion of the "Growing up in the online world: a national consultation" (taking into account the responses to that consultation). The expectation is that the DCMS Secretary of State will be responsible for exercising this power.

311. The Home Office view is that, although this is obviously not a NIEV-specific power, it may help reduce some risks associated with NIEV pathways, particularly for children and young people, if the power is used to restrict access to features that increase exposure to violent material, harmful recommendation loops, contact with unknown users, or other high-risk functionalities. While it is not possible to determine the impact with certainty in advance of implementation, the measures are likely to reduce children's exposure to some forms of violent and harmful content and reduce exposure to online features that can amplify harmful content or facilitate contact with unknown users.

[24] "Relevant children" means a child who is of, or under, a specified age (to be specified in regulations).

[25] Section 70 of the Children's Wellebing and Schools Act (amending the Online Safety Act 2023, inserting new section 214A).

Potential civil orders

312. In principle, the Home Office is interested in considering the introduction of civil orders that could be used to restrict or monitor access to the internet by a person assessed as presenting a risk of NIEV, if a significant threshold was passed concerning the risk they may pose to others. There is precedent for this in relation to both terrorism (in the form of Terrorism Prevention and Investigation Measures (TPIMs) under the Terrorism Prevention and Investigation Measures Act 2011, and part of the forthcoming Youth Diversion Orders, introduced under the Crime and Policing Act 2026) and CSEA (in the form of Sexual Risk Orders (SROs) under Part 2 of the Sexual Offences Act 2003).

313. To restrict civil liberties there needs to be a strong legal basis and so a clearly defined and sufficiently high threshold is crucial. That threshold is easier to set in relation to terrorism. There may well be some NIEV risk cases that would meet the threshold for the orders which are already available but there will also be a large proportion of such cases that will not.

314. The NIEV Taskforce will include work to consider the use of civil orders to mitigate NIEV risk, including the option for such orders to be used to restrict access to the internet. There are many issues to weigh up. For example, does a new order need to be created or can existing orders be utilised (via e.g. amendments to existing legislation)? Should restrictive interventions be mandated or voluntary. (Channel is a strong example of voluntary intervention whereas TPIMs and YDOs (once implemented) are mandatory.) The extent of intervention could also range from restricting access to certain websites to, at the higher end of the scale, removing access to electronic devices completely.

(G) MEASURES THAT HAVE BEEN IMPLEMENTED OR ARE BEING DEVELOPED

315. This section provides a summary of the measures that have been implemented or are being developed that are or may be relevant to NIEV risk. It separates the work by areas of policy responsibility as far as possible, but there are of course areas of overlap – both within the Home Office and with teams across other government departments.

HOMELAND SECURITY GROUP

Prevent Thresholds Review

316. Cathryn Ellsmore's witness statements for Phase 1 of the Inquiry (first witness statement at paragraphs 31 and 171 **[JE/001 - HOM000078]** and second witness statement at paragraphs 11 to 13 **[JE/017 - HOM000223]**) address the purpose and conclusions of, and the recommendations by, the Prevent Thresholds Review **[JE/010 - HOM000090]** ("the Thresholds Review"). The Thresholds Review's conclusions included that the legal threshold for Prevent is in the right place to intervene early and tackle the range of terrorism threats we see today, but that Prevent concerns are too often dismissed where there are issues around mental health, neurodivergence, or where there is an absence of ideology – despite someone being susceptible to terrorism.

317. The Thresholds Review made 9 recommendations in respect of which Ms Ellsmore's second witness statement contained a progress update up to the date that statement was finalised. Since then there have been further updates to the work arising from that review that are relevant to Phase 2's Terms of Reference. These progress updates are relevant to the thematic sub-headings in this section, but to assist the Inquiry in tracking what has been done against the recommendations I summarise the update here, and refer back to this section as appropriate:

    1) Recommendation 2 was for Prevent to review the 'Notice, Check, Share' process and guidance. It is used to advise frontline professionals subject to the Prevent duty on when and how to make referrals, including where there is no ideology present. In December 2025 the Home Office, working with the Verian Group (a commercial supplier), concluded a review of the current guidance, Phase 1 of the review was to better understand how the Notice, Check, Share procedure and guidance is interpreted and applied among frontline professionals and Prevent Practitioners. Phase 1 identified areas for improving and strengthening the guidance **[JE/110 - HOM000481]**. Phase 2 was to test potential changes and new materials based on feedback. A draft report of the second phase of the review was received at the end of May **[JE/111 - HOM000486]**. Drawing on these findings the PDU is working with frontline Prevent partners and across government to finalise new guidance which we expect to publish in September 2026.

2) Recommendation 4.2 was for Prevent to review the training for Prevent practitioners and frontline professionals on ideology, with a particular focus "unclear" or "no ideology" and "Islamist Extremism / Terrorism". The work to address the recommendation was conducted through the same two phase review with the Verian Group described above. Phase 1 of the review identified some practical and substantive areas for improvement for training, particularly for frontline professionals who wanted more concise training with a more practical focus, and more current content on emerging trends, particularly 'no ideology' threats. Phase 2 provided some clear recommendations for improvements relevant to the (different) priorities for frontline professionals and Prevent practitioners. The findings of these reviews will inform the full review and refresh of Prevent Training products which we expect to roll out in March 2027.

3) Recommendation 6 was for Prevent to strengthen local, regional and national collaboration with consistent information sharing and best practice, particularly for referral feedback. To strengthen regional and national collaboration, the Home Office and CTPHQ have initiated joint regional briefings, on a quarterly basis, for Prevent Practitioner networks covering policy and operational updates.

4) In addition, the Below Thresholds pilot (which covered approximately 50 cases over 12 months) has now been evaluated and has provided further insight that will be used to inform development of the Interim NIEV Guidance (as to which see paragraph 320 below).

5) Recommendation 7 was for Prevent to create a single authoritative repository of guidance and policy. The Review found that across all the sectors delivering Prevent, there is a range of different guidance, reports and policy updates, mainly disseminated via email, and recommended the Home Office establish a central portal. In April 2026 the Prevent Practitioner Portal was launched for a period of 12 weeks of user testing. This Prevent Practitioner Portal (which is for Prevent practitioners, rather than frontline professionals) provides a single repository for guidance and policy material relevant to Prevent. This will help improve practitioner confidence, consistency, and provide readier access to a record of how policy evolves over time. It will ensure that the full Prevent knowledge base is available for all Prevent practitioners, regardless of

organisation and agency, in one place. From October 2026 the portal will also house, on a temporary basis, the training materials that currently sit in a separate training portal whilst work continues on a more sustainable long-term digital platform that can house both the training and the guidance and policy in one place.

Addressing violence fascination risk in individuals who are suitable for Prevent support

318. To address risk arising from individuals fascinated with violence who are suitable for Prevent support, the Home Office has clarified existing policy and guidance, piloted new approaches to identifying and assuring risk, and reviewed existing policy and practice to identify further areas for improvement.

Identifying cases for referral

Support for Frontline Professionals making referrals

319. The Key Principles of Prevent document, together with FAQs and Case Studies, published in February 2026 (having previously been circulated to Prevent networks in September 2025), is part of the effort to ensure frontline professionals are clear on what basis they should make a referral. The Key Principles do not introduce new policies or expectations but clarify practices that have been operational since 2019. The Key Principles have been widely tested with Prevent practitioners and frontline professionals and are drawn directly from existing guidance and training. In particular it clearly states that frontline professionals should make a referral (using the National Referral Form) if they believe someone *may* be at risk of being drawn into terrorism and they are not required at the point of referral to determine the individual's ideology or the type of concern.

320. The Home Office is developing interim guidance on NIEV which will set out what NIEV is (see paragraphs 157 to 167 above) and to advise frontline professionals on referral routes for individuals they are concerned pose a NIEV risk ("the Interim NIEV Guidance"). The Home Office intends to issue this guidance by the autumn of 2026, Specifically, it will:

1) Address terminology and risk factors for NIEV;

2) Make clear when a referral should be made to Prevent;

3) Make clear, in cases where a Prevent referral is not appropriate, what other routes may be available locally to raise a concern;

4) Reflect findings from the Below Thresholds pilots, and set out possible options for onwards referral where referred cases have been referred to but subsequently assessed as not suitable for consideration within Prevent and Channel, or not suitable for Channel support. This will include cases where there is violence fascination, but where - as there is no vulnerabilty to being drawn into terrorism - the s36 CTSA threshold has not been reached.

321. The Interim NIEV Guidance will be distributed via Prevent and practitioner networks as additional operational guidance, and also to professional networks via other government departments, including in particular DFE and DHSC. The audience for the guidance will, in significant part, be the frontline professionals subject to the the Prevent statutory duty. It will also be distributed to Prevent practitioners (CTCOs, Channel panel members) to support their decision making around onward referal of cases which have been assessed as not suitable for Prevent / Channel support.

322. The Interim NIEV Guidance will sit alongside and be consistent with the updated guidance on Prevent's 'Notice, Check, Share' process (see paragraph 317(1) and will also be reflected in the updated Channel Duty Guidance which is scheduled for December 2026 (see further paragraph 333 below)).

323. As set out above (paragraph 317(2)) the Home Office is currently conducting a full review of its Prevent training provision for frontline professionals applying the duty as part of their day-to-day roles. It is anticipated the refreshed training will: (i) reinforce the Key Principles of Prevent to aid decisions about making a Prevent referral; (ii) highlight and ensure awareness of the updated Notice, Check, Share Guidance; (iii) address, where relevant, the training issues and recommendations identified by the two phase Verian review and in particular aim to give practitioners more confidence on when a violence fascination risk might be suitable for a Prevent referral; (iv) address issues identified with and any changes to the PAF; and (v) reflect, when it is available, the Interim NIEV Guidance.

Identifying referrals online

324. The Independent Prevent Commissioner, Lord Anderson KC, made clear recommendations in his July 2025 report, 'Lessons for Prevent', drawing directly on learning from the Southport attack. He clearly called for better capabilities, so that Prevent can spot young people online who are engaging with extreme content, as well as tools to help police understand young people's online activity so they can better assess any risk they might pose once they are referred to Prevent (Recommendation 4).

325. To improve early identification and support, the Home Office is piloting a number of approaches to better spot individuals at risk of radicalisation online. A priority driver of this work is the increase in under 18s engaging in terrorism related activity, and committing terrorist offences, many of which are committed online. These pilots bring together data, analytics and operational insight to test how risk signals can be identified earlier across a range of online environments, including social media and other digital platforms, and how these insights can be translated into timely, proportionate interventions. This includes exploring how partners can work together to triage online behaviours of concern, strengthen referral pathways into Prevent, and ensure vulnerable individuals are diverted into appropriate safeguarding support before risks escalate. These pilots are ongoing, with early results expected by late 2026, but provisional findings of one small scale pilot suggest that it is possible to engage people in Channel support based on their risk of engaging in terrorism-related activity online. CTP are conducting separate activity to examine an individual's online footprint post referral to Prevent (see paragraph 328 below).

<u>Improving quality of information available to Prevent on or following referral of an individual</u>

326. The Key Principles of Prevent document directs frontline professionals to make referrals to Prevent using the National Referral Form (NRF) (as to which see paragraph 26 of Cathryn Ellsmore's first witness statement **[JE/001 - HOM000078]**). The NRF is designed to assist referrers provide better quality and more consistent information at the point of referral by providing questions that will help them explain the reasons for their concern and the wider context. In early 2026 the Home Office commissioned Verian to carry out qualititative research to gather information on and identify recommendations to improve use of the NRF for referrals into Prevent, so as ultimately to improve the quality of referrals received ("the NRF evaluation") **[JE/112 - HOM000479]**. The NRF evaluation concluded in May 2026 and identified areas for improvement of the NRF, primarily

practical rather than substantive. PDU and CTP are considering these recommendations and anticipate an updated versions of the NRF will be issued in the autumn of 2026.

327. There is an ongoing programme of work at a regional level which aims to make sure Prevent is receiving the right referrals. Regional strategic meetings have been stood up in partnership with CTP, DfE and DHSC to assess regional/local referral data and develop an action plan to improve quality of referrals into the system. The approach allows for bespoke plans to be formed, to reflect regional variation. The majority of quarterly meetings are now underway.

328. It is a priority for Prevent that the system is better able to understand an individual's online activity and behaviour, so that informed assessments can be made by CTCOs and Channel Chairs to support decisions around case management and interventions required. I have raised this matter consistently as a priority for the Prevent System Board,[26] and asked that CTP identify a clear plan to address technical, legal and process issues, as well as any significant challenges, to take forward this work. As set out in the response to the Phase 1 recommendations, CTP, supported by the Home Office, is currently considering making a number of actions mandatory including: assessment of a subject's online presence in all Prevent cases rather than only those cases that pass the initial triage stage; assessment of a subject's digital media devices in all cases where they are already in police possession; and assessing online activity records attributable to subjects held by statutory partners in cases that reach the information gathering stage. These potential changes are currently subject to legal consideration and will require further consultation before a confirmed policy position is reached.

Making decisions on cases in Prevent

329. As the Inquiry is aware from Phase 1, the roll out of the new Prevent Assessment Framework (PAF), jointly developed by the Home Office, CTPHQ and CT-ARC (see paragraph 50 above), was completed for all regions in January 2025.

[26] The Prevent System Board aims to maximise performance against CONTEST objectives and ensure the effective delivery of transformation programmes that sit wholly or partially in the Prevent pillar. It is the principal decision making forum for the Prevent System. It is guided by evidence from CONTEST risk and performance data alongside input from Prevent system partners. It sits below the CONTEST Board, and escalates strategic and cross cutting issues to the CONTEST Board where necessary. I chair the Prevent System Board and board members are senior Prevent community members from across government and operational partners (see: Terms of Reference for the Prevent System Board June 2026 **[JE/113 - HOM000478]**)

330. Before using the PAF, CTCOs are required to complete the formal, evaluated training sessions organised by CTP. This training is designed to ensure they are proficient in completing the PAF and fully understand its integration within existing procedures. The training has been embedded in CTP's Prevent foundation curriculum, and Quality Assurance processes take place to ensure adherence to guidance, consistency and support practitioner development.

331. The Home Office and CTP, alongside CT-ARC, are conducting an ongoing evaluation of effectiveness of the PAF, the results of which will be considered early next year (2027) with phased interim findings this autumn. In April 2025 CT-ARC also concluded a rapid review of whether the PAF produced different outcomes for cases that had an ideology vs cases where ideology was not clear or present **[JE/114 - HOM000478]**. The Home Office was aware of reported concerns from CTCOs that in cases where ideology was less clear, or not present, the PAF was less likely to assess people as susceptible to radicalisation (where there was a radicalisation risk) and so wanted to confirm that the PAF tool did not produce different assessment outcomes due to this. The review concluded (although subject to a note that findings should be interpreted with caution due to the small sample size) that the PAF was suitable to address the full range of types of concern and did not produce different outcomes for cases based on whether ideology was present, not present, or unclear. CT-ARC's rapid review results are reassuring as they indicate (although subject to the conclusions of the more in depth review) that it is possible to design a tool that works for both ideological and non-ideological concerns and to use this in the CT space.

332. As set out in Phase 1 of the Inquiry, in early 2025 the Home Office worked with CTP to put in place (i) Guidance relating to repeat referrals (CTP Guidance on Multiple Referrrals Version 2.0, 2025 **[JE/115 - HOM000095]**; and (ii) Guidance to drive consistency in the assessment and progression of Prevent referrals where the primary type of concern was 'Fascination with Extreme Violence and Mass Casualty Attacks' **[JE/116 - CTPNW000016]**. Following consultation, and taking into account the recommendations of Lord Anderson (in particular recommendation 2), these policies have been made permanent (as of November 2025). In May 2026 CTPHQ issued updated Prevent Standard Operating Procedures which clarify CTP's approach to assessing FEVMCA cases (see: Chapter 22 **[JE/117 - HOM000516]**).

333. I am aware that that since April 2026 CTPHQ Business Assurance have been conducting an assessment to understand how Prevent Case Management records are progressed

through each stage: the Prevent Gateway Assessment, information gathering stage, the s.36 CTSA referral and the Channel adoption decision. The purpose of the exercise (termed a 'threshold test') is to gauge levels of consistency across regions and between partners at those key decision-making points. This will include consideration of how the FEVMCA policy is applied. This exercise, which asks CTCOs and Channel Chairs to apply a next steps judgement on 8 scenarios, is expected to run through to the end of 2026. It will inform the need for further training, policy and guidance to drive consistent practice and raise standards. The Home Office has been asked to collate views from Channel Chairs and Home Office Prevent staff to support CTPHQ's review.

334. CTP's development of the FEVMCA guidance was iterative and it is important to raise for the Inquiry's awareness one aspect of the final version of the guidance where there is a divergence of views between CTP and the Home Office, which I raise because it has some relevance to the question the Inquiry will be considering about the role Prevent plays / will play in managing the risk from NIEV. In the final version of the policy CTPHQ introduced the word "committing" to the definition of FEVMCA cases (i.e. 'evidence of a fascination in committing extreme violence and mass casualty attacks') (see: Prevent SOP, Chapter 22 **[JE/117 - HOM000516]**). I understand this addition reflected feedback from CTP regions but the PDU was not consulted on this particular addition and have some concerns about the impact of the change. In summary PDU's concern is that requiring evidence that a person is fascinated with "committing" extreme violence and mass casualty attacks may risk being interpreted as raising the threshold for a referral to Channel under s.36 of the CTSA ("reasonable grounds to believe that a person is vulnerable to being drawn into terrorism"). Evidence of a person intending to commit or being interested in committing is not required for other types of concern under CTCO guidance. By the time there is evidence of intention to commit the individual may well not be suitable for Prevent, as this would move them into the Pursue space. These concerns have been explained to CTP, but CTP have maintained the inclusion of the word "committing".

335. In the period since the Southport attack, as an interim measure to assist with the approach to FEVMCA cases, a letter issued to Channel practitioners in March 2025 explained CTP policy updates for FEVMCA referrals, which endorsed panel adoption of these cases where there were concerns that the person was on a pathway to terrorism (see Cathryn Ellsmore letter 13.3.25 **[JE/118 - HOM000100]**). At the same time a policy addendum to the Channel Duty Guidance was issued which stated that where Channel made a decision not to adopt a referral there is a requirement for onward signposting

where there is a residual vulnerability, which could include highlighting any public protection risk to local policing (see Channel Duty Guidance Addendum 13.2.25 **[JE/119 - HOM000476]**).

336. The Channel Duty Guidance will be updated later this year to reflect policy and strategy developments including on repeat referrals, Prevent relevant FEVMCA and exit pathways / signposting. The guidance will remind panels of Prevent's Key Principles and recording requirements to inform auditable decision-making and set out the latest position on NIEV. We expect to launch this updated guidance at the end of the year (likely December).

337. The full roll out of the Prevent Practitioner Portal, which I have explained at paragraph 317(5) above will also be an important tool to improve consistency of decision making and delivery of Prevent , by ensuring practitioners can readily access the most up to date assessments, policy, guidance and training materials.

Intervention provision for Prevent cases

338. To reflect the increasing complexity in casework across the range of Prevent programmes (Channel (England and Wales)/Prevent Multi-Agency Panel (PMAP – Scotland), Police-Led Partnerships (PLP) and the Desistance and Disengagement Programme (DDP), and to reflect the fact that ideology may be unclear or not present in some cases with violence fascination concerns, the Home Office has been piloting an expanded range of interventions. These pilots have been agreed via the new Prevent Interventions Board, which looks at programme improvement across Channel, PMAP, PLPs and the DDP to ensure strong intervention routes, and the right range of specialist interventions are available. The Prevent Interventions Board is chaired by the Deputy Director of Prevent, and includes senior representatives from across government, devolved administrations, as well as key operational and delivery partners (see Prevent Interventions Board Terms of Reference **[JE/120 - HOM000475]**).

339. Following work to build an evidence base around interventions gaps in autumn 2024 the Home Office introduced a practical mentoring pilot, which ran from 1 August 2025 to 31 March 2026, which extended the use of practical mentors used in DDP casework to make them available on a limited basis to PLP, Channel, and PMAP cases (see paragraph 16 of Cathryn Ellsmore's second witness statement **[JE/017 - HOM000223]**). Practical mentoring was made available for up to 50 Channel/PLP and PMAP cases during this period, and an evaluation of uptake and impact of this pilot commenced in April 2026.

This made use of existing Intervention Providers contracted to provide Prevent support under DDP, and existing CTP Prevent budgets to fund practical mentor provision for each case. HSAI are undertaking the evaluation of the practical mentoring pilot, and anticipate this will be completed at the end of August. Although the pilot has closed, practical mentoring support is still available across the Prevent programmes. These cases will not form part of the evaluation process.

340. As addressed in Cathryn Ellsmore's second witness statement, in January 2026 the Home Office introduced a new family support service pilot (paragraphs 18 to 19 **[JE/017 - HOM000223]**). This was initially to run until 31 March 2026 but has been extended to 31 August 2026. This pilot sees support offered across Channel, PMAP, PLP and DDP and provides tailored support to family members including partners, and significant others of individuals receiving Prevent support. This includes guidance to help families understand the risks associated with radicalisation and how best to support their loved ones. Such support might include family mediation, mentoring advice, and signposting to help families understand radicalisation risks, strengthen online safety, and build protective factors. The pilot is available to all families of individuals referred to Prevent. Early feedback from the pilot has been positive, with family mentor suppliers reporting that the pilot is working well in practice. Referrals have been received across Prevent programmes and ideologies, and anecdotal feedback suggests the intervention is filling a key gap in provision, improving family engagement, and strengthening support in areas such as online safety. A fuller assessment of the intervention's impact, effectiveness and outcomes will be captured through a formal evaluation.

341. Finally the pilot of psychological advisory services (see Cathryn Ellsmore's second witness statement at paragraph 17 **[JE/017 - HOM000223]**) commenced in February 2026.

    1) Under this pilot four expert psychologists provided by HMPPS (each a Chartered and Registered Forensic Psychologist with expertise in mental health and neurodiversity) offer advisory support to Intervention Providers working with individuals referred to Prevent where mental ill-health or neurodivergence may contribute to vulnerability to radicalisation.

    2) The psychologists work collaboratively with Intervention Providers to identify effective approaches for engagement, highlight potential challenges, and recommend appropriate methods of support.

3) Two strands of provision are currently available: case-specific advice and general advice. For Intervention Providers working on DDP and PMAP cases, case-specific advice can be sought directly from a psychologist. However, for Intervention Providers working on Channel and PLP cases, only general advice is currently available, as case-specific discussions are not permitted due to the requirement for formalised data protection and data sharing arrangements; however, these have not yet been finalised.

4) The pilot is still running but the case numbers have been very small and therefore not enough to conduct an evaluation. However, albeit from a very small number of cases, we believe we have seen clear benefits of this service and therefore we are looking to end the pilot soon and bring this service within our standardised intervention offer for Channel, PLP, PMAP and DDP cases.

Mental Health and Neurodiversity Review and Prevent

342. Prevent has continued working to meet the recommendations in the MHND Review:

1) Internal and external cross-government/partner steering groups have been maintained to drive the recommendations forward and provide strategic direction alongside meetings with Wales & Scotland to discuss the application of the MHND recommendations.

2) We have facilitated further sessions with (i) Prevent practitioners (local authority leads and Channel / PMAP chairs) and (ii) with Intervention Providers, DDP mentors and Prevent commissioners on mental health and neurodivergence in order to better understand what works to support people with mental ill-health or who are neurodivergent, as well as to understand their challenges. The feedback from these sessions have been drawn together and recommended next steps identified, which include proposals for improving Prevent Practitioner training on these issues, embedding MHND informed practice, addressing systemic blockers for Intervention Providers (such as delays accessing MHND assessment and support for individuals) and strengthening access to MHND expertise.

3) A range of resources including policy documents, guidance and research on MHND have been added to the new Prevent Practitioner Portal. This will strengthen practitioners' access to consistent information that supports effective management of MHND within Prevent.

4) As already addressed, the Psychological Advisory Service Pilot has commenced (see paragraph 341 above).

5) Prevent has supported the development of revised DHSC guidance ('Guidance for Mental Health Services in Exercising Duties to Safeguard People from the Risk of Radicalisation') for healthcare practitioners that will clearly outline roles and responsibilities for managing radicalisation risk in patients that present with mental ill-health or neurodevelopmental conditions. This will be published soon once approved by DHSC Ministers.

6) DHSC is engaging with NHS England to review and revise NHS Prevent training to bring it up to date with the latest Home Office guidance around Prevent referrals and in particular the Key Principles of Prevent.

7) The Home Office is working with DHSC to improve the provision of MHND assessment and support for Prevent cases. DHSC have been asked to review how the provision of MHND support and wider health related interventions can be prioritised for individuals that pose a risk to public safety, where existing multi-agency assessment and risk management processes have identified a clear need. There is a shortage of forensic clinical expertise which needs to be addressed, DHSC have also been asked to identify a sustainable long-term funding solution for FCAMHS.

8) In March the Home Office launched a consultation phase with Prevent stakeholders (to include a wide range of stakeholders such as NHS clinicians, DHSC, DDP Policy Team, Intervention Providers, Practical Mentors, Channel Chairs, CTP, CTCOs, FCAMHS, CCS, ICE, Commercial, CT ARC, JEXU, Interventions Policy & Ops, HMPPS Psychologists). An initial roundtable with NHSE clinicians was held, primarily exploring feasibility of options for improving access to neurodiversity assessments or support for cases in Prevent.

9) Finally, research remains underway in collaboration with CT Policing's Clinical Consultancy Service to improve our understanding of the complex relationships between mental health, neurodiversity and radicalisation, as well as how best to support people with mental ill-health or who are neurodivergent.

The Prevent system's role in managing violence fascination risk in individuals who are offered Prevent support, but do not consent

Exploring risk for individuals with violence fascination risk risk without consent to intervention

343. Following publication of the most recent Prevent statistics in November 2025, the Prevent System Board highlighted the risk around those individuals who were progressed for discussion at Channel and were adopted as a case, but where consent was not received for Channel support. Consent rates for FEVMCA Channel cases are higher than for other ideologies, albeit based on a smaller base. The Prevent statistics for the period April 2024 to March 2025, indicated that, where it was specified, the percentage of cases consenting to engagement with Channel[27] for FEVMCA cases was 67% (76 out of 113 cases) whereas for all Channel cases where Consent was specified 55% (767 out of 1383 cases) had consented to receiving support. We do not have clarity on how the non-consenting cohort (including FEVMCA related cases) is disposed following their non-consent. The next statistical release, which will cover the 12 month period ending 30 September 2025, is due to be published in August 2026.

344. The Home Office is planning work to improve consent rates in Channel, including sharing best practice amongst regions, improving communications about Prevent and considering obtaining feedback during the consent process. We are also in discussions with CTP about carrying out an analysis of non consenting cases to better understand this cohort.

[27] The Inquiry should note there are some caveats to this data. The Prevent Case management Tracker (PCMT), launched in May 2024, introduced a systematic method for recording consent status data within the Prevent cohort. Data in the current statistical publication covering the period 1 April 2024 to 31 March 2025 was produced using this new reporting feature within PCMT. Data quality and completeness are expected to improve over time. Consequently, trends observed in the early years of reporting should be interpreted with caution, as improvements in data coverage and recording practices may affect comparability. Additionally, whilst in Channel an individual can remove their consent at any time. For the published statistics, the consent outcome is the latest outcome at the time of data extraction.

Addressing the risk from NIEV risk individuals who are not suitable for Prevent support

Assurance for cases that are not progressed to Channel, or not adopted to Channel

345. As Cathryn Ellsmore covered in her oral evidence in Phase 1 of the Inquiry, and provided more detail about in her second witness statement (see **[13 October 2025 DAY 22/70/21-71/11]** and Cathryn Ellsmore second witness statement at paragraphs 29, 31-43 **[JE/017 - HOM000223]**), between March 2025 and March 2026 the Home Office conducted its 'Below Thresholds Pilot'. The driver for the pilot was the concern that the high number of cases CTP assessed as not meeting the threshold for referral to Prevent but signposted to other agencies for support were not in fact being routinely or sufficiently managed by other mechanisms or agencies. In the year ending 31 March 2025, 4,363 referrals fell into this catgory. Prevent does not have any means to follow the progress of these cases once they are signposted to other services, nor any understanding of whether the individuals go on to receive support to address any potential risk or harm.

346. The pilot was launched to provide assurance over the onward support provided to individuals who did not meet the Prevent threshold and where a risk of violence or a concerning interest in mass violence has been identified. The pilot tested mechanisms in 9 local authorities for onward referral to other local services for those cases. Areas were instructed to establish monthly multi-agency panels to assess the referrals and identify which local agency would be best placed to provide support in each case and consider routes of access. There were also instructed to conduct 3 month check-ins to monitor, and where appropriate, close cases to the pilot.

347. The pilot has now been evaluated (Below Thresholds Evaluation Report February 2026 **[JE/071 - HOM000445]**). 50 individuals were discussed between March and November. They were typically young males exhibiting a range of (non-CT) vulnerabilities and were mostly already known to other mainstream services. Pilot areas felt cases were generally appropriate for the pilot, however most partners felt the overall caseload had been low and was lower than expected, with the number of new cases brought to panel reducing over time.

348. Despite the rapid set up of the pilot and lack of a clearly defined legal framework, the multi-agency pilot panels ran smoothly, with strong partnership engagement in the pilot, supported by information sharing. Panels mostly adopted a similar structure to Channel panels, with significant overlap in partner attendance, but held completely separately

from Channel. Unlike Channel, panels were only asked to provide additional oversight and assurance that cases were being appropriately signposted to onward services for support, rather than provide ongoing case management. That said, some panels identified additional safeguarding actions could be taken as part of the assurance process. Panels were typically well attended although some areas faced difficulties identifying the right personnel from other mainstream services to engage. These services included (but was not limited to): social care, CAMHS and wider mental health services, local/neighbourhood policing and schools. The majority of individuals discussed were already known to mental health services, including CAMHS/FCAMHS, Community Mental Health teams, Community Psychiatric Nurses (CPNs), psychologists and psychiatrists.

349. CTCOs saw the benefit of bringing cases to a multi-agency panel for further oversight, improving their confidence that the consideration and management of non-CT risk had been strengthened in comparison to the usual approach. However, it was unclear whether the (non-CT) vulnerabilities had been better managed under the pilot, with mainstream services having high thresholds for the provision of support. Discussions often strayed beyond assurance of the handoff into case management and were often longer than needed, with some actions being handed back to Prevent, despite cases being closed to Prevent. Panels did not have the power to direct other services to complete actions, when cases had been handed off.

350. The learning and recommendations from the Below Thresholds Pilot concerning measures to strengthen onward referral of individuals not deemed suitable for Prevent will be incorporated into the wider work of the NIEV Team and NIEV Taskforce.

Interim NIEV guidance

351. As explained above paragraph 320 - 321 the Home Office will develop Interim NIEV Guidance to be issued in the autumn of 2026. This will build on the Key Principles of Prevent guidance that was first issued in 2025 and published in February 2026, by setting out what NIEV is and provide frontline professionals with advice on the existing referral routes open to them for raising concerns about NIEV risks, or when to make a referral to Prevent. We are working with key partners, including members of the Early Interventions Working Group (see paragraph 69 above), to agree an approach to developing this guidance, including what it should include, which will be signed off by the NIEV Taskforce Strategic Delivery Board in September. As interim guidance, it is

likely to focus on clarifying expectations about how NIEV risks can be managed within existing safeguarding and public protection frameworks. Implementation of the Interim NIEV Guidance will be determined at a local level as each local area will have different processes and routes for raising concerns, and managing risks. The NIEV Taskforce Practitioner Advisory Group be will also be asked to provide input into the Interim NIEV Guidance, and what it should include to help manage NIEV risks at a local level

352. Following publication of the guidance referral numbers to Prevent and Channel case adoptions will be monitored to consider any impact of providing professionals with greater clarity on alternative referral routes in terms of reduced referral numbers to Prevent.

Identifying risk of non-ideological extreme violence online

353. As I have addressed above (at paragraph 325) the Home Office is working with law enforcement to develop an online capability pilot to identify and disrupt emerging threats online, including high risk individuals engaging with extreme violence content. The approaches will be similar to approaches taken to other crime types, for example Child Sexual Abuse offending online.

Oversight and assurance of Prevent's role in managing the risk from violence fixated individuals

Prevent Casework Assurance

354. In 2025 the Home Office and CTP conducted an assurance exercise to identify any individuals previously referred to Prevent, who had been closed at referral stage or following Channel discussion, who presented a VFI-type risk (as it was then defined) and reconsider whether they ought to be adopted to Channel and / or re-referred to other local services for prioritised support. The assurance exercise included historical cases (some dating back to 2021) and more recent cases. CTP analysed 1,002 cases that had not been referred to Channel pursuant to s.36 CTSA and the Home Office analysed 563 cases that had been referred to Channel but not adopted. Of the 563 cases analysed by the Home Office 42 were re-examined for case assurance on decision making and onward referral. The additional assurance was progressed due to poor case recording by CTCOs. The 42 cases (spanning 21 local authorities) were re-examined using various methods including deep dives into the casework, checking minutes and one-to-one discussions with Chairs. These checks provided the required assurance that they had been handled appropriately. This review concluded in July 2025 (see Case Assurance of

Historic Chnnel Cases with VFI indicators (2021-2025) slides **[JE/121 - HOM000441]**).[28] As part of the CTP analysis, active cases were also re-assessed and interventions prioritised to mitigate risk.

Independent oversight of Prevent

355. In January 2025 the Home Secretary appointed Lord Anderson KC as the Interim Independent Prevent Commissioner. On 13 April 2026, following an open competition, Tim Jacques was announced as the new Independent Prevent Commissioner (IPC). The role of the IPC is to provide an independent strategic oversight and review function for Prevent to ensure that it can meet its objectives as effectively as possible.

The Prevent system's role in supporting risk management in Pursue casework where violence fascination may be a concern

356. As the Inquiry is aware, since January 2025 individuals under overt investigation in the Pursue space can be adopted onto Channel in order that multi-agency support and specialist intervention can be provided (see: Cathryn Ellsmore first witness statement at paragraph 150 **[JE/001 - HOM000078]**; Channel Routes To Interventions Guidance **[JE/122 - HOM000476]**). This reflects the Home Office and CTP's assessment that in some cases a multi-agency holistic approach can be effectively utilised to manage risk even for cases that are very high risk and under active investigation. In cases where violence fascination is a risk factor, this approach means that specialist interventions can, with consent, be delivered to address this risk alongside other relevant factors in an individual high-risk case.

Emphasis on multi-agency working

357. Multi-agency case working, to help identify and manage risk, has long been a feature across the CT system. CONTEST 2023 recognised the need to expand this multi-agency approach in particular when managing high risk cases. In addition to the measures described at paragraph 356 above, which relate specifically to Channel interventions, there have been wider efforts to increase the range of interventions available to mitigate risks in high-risk CT casework.

---

[28] Although there will be significant overlap, this assurance exercise did not encompass all of T1D* approximated 1500 individuals who would meet the definiton of VFI (see paragraph 139 above), as T1D* drew on wider police systems data as well as Prevent data.

358. The challenge presented by the prevalence of mental ill-health and neurodiversity in the CT risk cohort is a helpful example of this work. There has been close engagement between DHSC and Home Office Ministers about the importance of health in some CT work and the need for DHSC and the Home Office to work together to counter radicalisation risk, particularly given the increasing number of Prevent referrals involving individuals, particularly young people, who displayed a fascination with violence. Consideration is being given to strengthening shared knowledge and relationships across relevant teams.

PUBLIC SAFETY GROUP

Knife Crime

359. There has been, and is ongoing, significant work on making our approach to knife crime more robust. Nick Hunt will provide the Inquiry with evidence to explain the work that has been undertaken and is continuing to achieve ministerial priorities on knife crime and youth offending by the Knife Crime Unit and the Young Futures Delivery Unit within the PSG. The importance of the teams responsible for NIEV risk and for knife crime sharing information and policy development work and proposals is well recognised, particularly around prevention / early intervention, and is reflected in the structures of the new NIEV Taskforce Working Groups (the NIEV Early Intervention Working Group includes representation from the Youth Futures Unit).

Young Futures Prevention Partnerships

360. In the early part of 2025, pursuant to the Government's manifesto commitment to deliver a Young Futures programme, the Safer Streets Mission in the Home Office prepared provisional proposals for the roll out of Young Futures Prevention Partnerships, initially in those 20 police force areas with a Home Office funded VRU, and ultimately to be rolled out nationally (see also paragraphs 98 to 102 and 121 above). Although there was pre-existing partnership infrastructure (VRUs, Serious Violence Duty Partnerships), where there was an opportunity to go further was in the earlier identification of the right young people. Key to this was the development of a 'prevention panel', a multi-agency panel who would be responsible for identifying, assessing and referring into support those young people who were showing early risk factors for criminal involvement. These panels are now referred to as Young Futures Panels.

361. By February 2025, following an external engagement process, the Home Office concluded there was a need for a programme to meet the needs of children who are at risk of being involved in crime but either do not meet thresholds for support (for example, the risk of harm is not sufficient for Children's Services to establish a Child in Need plan or a Child Protection plan, or their offending history does not meet the levels for Youth Justice Services intervention) or where the support being provided is not sufficient (so, for example, the fact that a child was on a Child in Need plan would not automatically rule them out of the programme). By October 2025 the first pilot panels were rolled out, initially intended to have at least one panel per VRU area operating at local authority level. This rose to a total of 52 in the first 6 months and rose again to a total of 65 pilot panels operating by July 2026.

362. If the Young Futures Panels prove successful there will then be a policy discussion about how best they could be rolled out nationally: whether the learnings from the pilots can be incorporated into the existing partnership infrastructure or whether, funding dependent, the should continue as bespoke panels. Most of the testing is being done through the VRUs, which are central to any planning scenario.

WIDER GOVERNMENT

363. Other departments will provide the detail of the work they have progressed to the Inquiry but I flag two areas under development by the MoJ.

New offence of planning a mass casualty attack

364. In April 2025 HMG accepted the recommendation of Jonathan Hall KC, the Independent Reviewer of Terrorism Legislation (IRTL) to retain the existing definition of terrorism under s.1 of the Terrorism Act 2000 but to consider creating a new offence, adapted from terrorism legislation, to deal with non-terrorist attack planning by an individual. Policy in relation to this prospective new offence is being developed by the MOJ and I am aware that the initial policy development stages have concluded. As announced in the King's Speech in May 2026, the Government committed to bring forward this measure via the National Security Bill, which will be brought forward as soon as parliamentary time allows.

Youth justice reform

365. In February 2026 the Ministry of Justice published its Policy Paper 'A Modern Youth Justice Service: Foundations Fit for The Future' which set out the Government's reforms and plans to modernise the youth justice system. This includes a commitment to reforming the role of the Youth Justice Board. In recognition of the increasingly complex caseloads of youth justice services, including worrying trends emerging or worsening, including in respect of knife crime, violence against women and girls, and online harms, the government is committed to examining how it can better support frontline services and be more accountable for doing so. Further reforms were announced on publication of the Government's Youth Justice White Paper in May 2026, setting out a programme of reform to modernise the system, establish a clear direction toward earlier intervention, improving consistency, and ensuring custody is only used where necessary, moving the system to a more preventative, joined-up and evidence-led approach.

(H) LONGER TERM REFORM – CONSIDERATIONS AND CHALLENGES

366. Our current understanding of the NIEV threat indicates strong intersection with a range of other public safety and national security threats. We observe this increasing hybridisation of threats and the way they are enabled and exacerbated by technology through the online information environment as a defining feature of our work to protect the United Kingdom. Thus concerns about risk factors relevant to NIEV, including the age of perpetrators, social isolation, exposure to violent material or extremist ideology, mental ill-health and neurodiversity, desire for notoriety and so on are also felt in counter-terrorism, the sexual exploitation of children and, to a greater of lesser degree, in a range of other threats.

367. Although concerns about NIEV are increasing and fascination with violence is certainly a factor in some ideologically motivated cases incidents of NIEV currently appear to be thankfully rare. But we know from tragic experience that the impact of such cases on victims, communities and society at large can be devastating. This is particularly the case where, as with AR, opportunities to identify the risk and intervene to prevent the attack are missed. Multi-agency efforts to rehabilitate offenders or support those deemed to be at risk of criminality, including violence, have become a staple feature of a justice system which has increasingly seen prevention as an effective and efficient tool for public protection, but these efforts remain fragmented. The counter-terrorism system which came together under a common strategy in the wake of the attacks of 9/11 and 7/7 offers a worked example of the development and integration of an holistic prevention pathway for what many consider to be the apex violent threat to society, but that in itself has not

been an easy road. The placing of Prevent on a statutory footing through the CTSA 2015 was a major milestone and the subsequent implementation of the Prevent Duty, in particular through Channel, has required significant cultural shifts, dedicated resource, research, innovation and ongoing cross-system learning – a process which is absolutely vital, and which will never be complete.

368. In this section I will look ahead, drawing on our current understanding of the NIEV threat, our experience of how the counter-terrorism system has developed as part of that complex multi-agency landscape and an understanding of the tools and levers available to government to explore options and considerations for longer term reform of efforts to counter the NIEV threat. This will include highlighting areas of work, including pilot activity, where success is far from guaranteed, and the consideration of very significant reform, delivery of which may or may not prove proportionate, practical or affordable.

369. Much of this work is being conducted through the NIEV Taskforce, of which I chair the Strategic Delivery Board. As this work progresses in the course of the period of the Inquiry we shall ensure that the Inquiry receives timely and substantive updates on all relevant workstreams. In due course I anticipate that the conclusions of this Inquiry and the work of the Taskforce will enable Ministers to make clear decisions on options to tackle the problem of children and young people being radicalised to extreme violence.

370. In this section I look to assist the Inquiry with what provisional options are under consideration and – to the extent I am currently able – the advantages and disadvatanges of those options. I also address the range of NIEV relevant challenges inherent in the online information environment and considerations on how they might be addressed.

Designing an approach – overview of Home Office position

371. A range of referral routes, assessment approaches, risk management mechanisms and risk owners, together with relevant interventions, are being examined by government. However, we are not yet at the point where government has a clear view on what system or combination of systems would be the most suitable, effective and deliver value for money at this stage. This is partly because further detailed policy work and testing with delivery partners is required to understand the scope for strengthening existing arrangements (reflecting the scale and complexity of the challenge), partly because of the realities of the very significant funding pressures which meant progressing the

extensive work required to model and assess the viability and utility of a National Prevention Gateway was not feasible, but also because we see obtaining the views of the Chair as an important element of this long-term piece of work. It is not the case that we currently hold a clear view that a single system approach is what is needed, but equally we do not rule it out. Our aim is to provide Ministers with choices, and we recognise that in making those choices Ministers will need to balance the risks we are seeking to address here against the panoply of national security and public safety risks as well as other government priorities. Any proposals for reform that involve signficiant public spending will need to achieve value for money, which is defined as the balanced judgement about the optimial use of public resources to achieve the objectives of a proposal.[29]

372. It is instructive to contextualise the challenge by drawing on general principles and learning from the evolution of the Prevent system.

373. Prior to the CTSA 2015, Prevent operated on a non-statutory footing. Delivery and implementation varied between different areas, and it was at times difficult to make sure that local multi-agency partners were prioritising efforts to stop people being drawn into terrorism.

374. Placing Prevent on a statutory footing required active prioritisation from local authorities, active participation from multi-agency partners, and provided a clear basis for information sharing to manage public protection risk. It also provided a clear underpinning for referrals to be made to Prevent. The CTSA 2015 placed a more general duty on specified authorities, which meant they had responsibility more generally to address extremism and terrorism in their area or sector, including preventing permissive environments and building resilience to extremist and terrorist narratives and influence.

375. When looking to manage individuals who pose a public protection risk, there are degrees of frameworks that can exist, ranging from guidance only (e.g. VRUs), through to a statutory duty with leeway on how this is implemented at the local level (e.g. CSP and MAPPA) to more prescribed statutory frameworks with a national case management capability and ongoing business assurance and performance management (e.g. Prevent). Existing frameworks have been developed to manage different types of public protection risk or safeguarding requirements, with the relative scale of caseload being relevant to their design. Variations in local risk profiles or requirements are also relevant

[29] HM Treasury Guidance: The Green Book (2026)

here, as is the degree to which national oversight of a system is desirable and can be achieved in practice. While Prevent retains a national case management system and centralised capabilities for intervention, performance and assurance, the number of referrals to Prevent and adopted Channel cases are relatively low when compared to other risk management frameworks. This high degree of structure and oversight within the Prevent system relative to case volumes reflects the nature of the risk Prevent manages, and the implications for cases that escalate to requiring active investigation, or which result in an attack.

376. A systems approach to managing the risk from individuals fascinated with violence, plus potentially a wider range of current, emerging and future non-ideological harms, will need to be calibrated appropriately for the seriousness of the potential harm, volume of 'cases' (if a case management approach is taken), capacity, capability and willingness of multi-agency partners to engage and the degree to which capabilities need to sit at a national, regional or local level.

377. It is helpful to set out here, at a high level, the key, although not exhaustive, elements of a system approach. I address these elements in more detail at paragraphs 389 to 411 below.

1) Support to frontline professionals to identify NIEV risk – as they would other public protection or safeguarding risks.

2) A way of raising a concern to an agency or multi-agency structure that can take action to provide support to an individual and manage the NIEV risk.

3) A way of assessing whether someone does pose a risk of NIEV or is being drawn in to NIEV, and what support or intervention is required to reduce this risk.

4) An appropriate level of management for individual cases appropriate to the risk, to enable the exchange of information between relevant parties and appropriate actions and mitigations to be identified.

5) Suitable support and intervention options, which would include multi-agency support (based on the likely complex and varying needs of each individual),

plus specialist interventions which may not be readily accessible at the local level.

6) Clear consideration of online elements, including how to identify people online who are at risk, considering someone's online behaviour and interactions when assessing risk, and having sufficient understanding of the online information environment to deploy the right support and interventions to manage the NIEV risk linked to an individual.

7) Appropriate governance, management and performance oversight consummate to the risk being managed.

8) A culture that prizes shared risk ownership and management over the transfer of risk between organisations (which I expand on in paragraphs 401 to 404 below).

Pros and cons of potential changes to existing arrangements or development of new mechanisms

378. As the summary in Section C above demonstrates, there are a number of existing frameworks and services that it may be possible to utilise or adapt to identify and manage the risk posed by the NIEV cohort.

379. A Home Office scoping exercise sought to identify – on a very preliminary basis - some of the main pros and cons in relation to some of those options, and the options for more fundamental change (see: VFI Unit paper 2026 'VFI multi-agency management summary' **[JE/123 - HOM000384]**, replicated below for ease).

Potential change	Pros	Cons
Expand MAPPA Category 3 to allow individuals assessed as posing a high risk of serious violence to be included even without a conviction.	• Builds on established statutory framework for MAPPA Category 4 terrorism-related risk • National consistency and governance	• Requires legislative change • Increases pressure on MAPPA resources • Requires robust proportionality considerations for those without convictions

Put the PDP scheme on a statutory footing	• Addresses gap below MAPPA threshold • Consistent national practice created • Police-led model familiar to police forces	• Requires legislative change • Risk of duplication with MAPPA • Requires new national infrastructure and training
Put MASH on a statutory footing	• Strong early safeguarding and information-sharing • Consistent national baseline	• Not designed for sustained management of high-risk violent individuals • Significant structural reform and cost • Risk of mission creep
Expand remit of Prevent to include serious violence risk more broadly	• Strong early intervention capability • Established multi-agency model	• Requires legislative change • Fundamentally redefines Prevent, risk of diluting its core counter-terrorism purpose • Politically sensitive and high risk
Expand role of Youth Offending Teams (YOT) to cover wider serious violence risk management for children	• Existing statutory, multi-agency framework for CYP • Strong engagement with families and education	• Limited to under-18s • YOTs already stretched • Requires new duties, mechanisms and funding
Expand Framework for Integrated Care (Vanguard) sites, largely health-led, to support individuals with complex needs linked to risk of violence	• Strong multi-disciplinary, psychologically informed model • Particularly relevant for CYP	• Limited to pilot areas, not national • May be overly health-focused and would require redesigning to support public protection aims
Expand [Youth Futures] Panels from their pilots in 20 areas	• Strengthens upstream prevention • Builds on existing VRUs and local authority structures	• Limited to pilot areas, not national • Not designed for managing high risk of serious violence.

	• Strong links to education, health and youth services	
Expand Prevent Below-Threshold from their pilots in 9 areas	• Builds on Prevent infrastructure • Addresses 'falling between systems' problems	• Limited to pilot areas, not national • No statutory power to convene or compel information sharing • Unfunded and unsustainable without legislation
Create local or regional multi-agency hubs for real-time intelligence sharing and risk escalation, distinct from all existing frameworks	• Responsive and locally tailored	• Likely to lead to variable practice • Risk of duplication with existing frameworks • Requires new governance and funding
Create a Violence Prevention Gateway as a single national front door and framework	• Addresses system fragmentation • Potential long-term efficiency and coherence	• Requires significant legislative change • Very high cost and complexity to set up • Major infrastructure and workforce reform required, with significant disruption to existing systems

380. The Home Office has not yet conducted a detailed assessment of the existing multi-agency structures, services and programmes outside of Prevent to understand how NIEV risk cases are progressed and how effective those existing arrangements are at identifying and managing that risk. The Home Office will be following the Inquiry's evidence and seminars closely to inform our understanding, and in parallel the NIEV Team will be undertaking a further, more detailed, review of the multi-agency landscape which will take place between August 2026 and March 2027.

381. As I indicated earlier in this statement (see paragraph 55), we are considering with DfE the extent to which this work might be conducted in tandem with DfE's safeguarding landscape review so as to avoid duplication and have a common understanding. The programme of work is therefore not yet settled, but broadly we anticipate:

    1) The first stage of this work will be to develop a set of criteria for a NIEV risk multi-agency arrangement by reviewing the emerging evidence base and consulting with internal and external stakeholders.

    2) The NIEV team will use these criteria to test existing multi-agency arrangements and develop a shortlist of viable options, drawing on the Taskforce working groups and the practitioner advisory group, and obtaining senior level agreement through the NIEV Strategic Delivery Board.

    3) Viable options will then be tested through more detailed engagement with practitioners and ongoing consideration of the evidence obtained by the Inquiry. We will also seek to learn from emerging approaches in local areas, and from a programme of pilot approaches which we will run in partnership with a small number of local areas from the autumn.

    4) A comprehensive costing exercise will be carried out ahead of ultimately making a recommendation to ministers.

382. We will keep the Inquiry updated as to the progress of this work. Following the conclusion of this review we will have a much clearer view of how these arrangements currently work and may in the future work to address the NIEV risk, and the advantages and disadvantages of the potential options.

383. However, to assist the Inquiry the Home Office's early, high level, views on expansion of existing arrangements are:

    1) Prevent and MAPPA are the only formal (i.e. underpinned by statute) existing multi-agency risk management frameworks that are set up to identify, assess and manage the risk a person poses to others.

    2) Under existing guidance, only Prevent specifically considers whether an individual's risk (of being drawn into terrorism) includes or is driven by

fascination with extreme violence or mass casualty attacks. No other multi-agency risk management frameworks currently have, to the Home Office's knowledge, guidance that addresses NIEV risk.[30]

3) Prevent will continue to manage the risk from violence fascinated individuals who are vulnerable to being drawn into terrorism as those individuals meet the s.36 CTSA threshold for support. It would not be logical to exclude from Prevent individuals who meet that threshold for support because violence fascination was a risk factor. Whilst it is recognised that if another mechanism is adapted or established specifically to manage the threat from NIEV outside of Prevent, then some cases may be picked up under this mechanism which are currently managed by Prevent, this would not represent a change to the statutory threshold, assessment tools or national approach, but may reflect changes in practice for borderline cases.

4) Expanding Prevent's remit so that it becomes the default route for NIEV risk would require legislative change (most likely to the scope of Prevent, rather than to the definition of terrorism), and would need careful consideration to ensure clarity of purpose, proportionality, and the right fit with existing safeguarding and public protection frameworks. Such a change would also be subject to capacity and resourcing considerations.

5) Our expectation is that other police and local-authority led safeguarding structures may (i) support the identification of NIEV risk and (ii) play a key role in the management of NIEV risk, but:

    a. The local delivery, both of established national frameworks and more localised schemes, will vary considerably, with different structures, guidance and local working relationships.

[30] I note that DfE's current consultation on updating Working Together to Safeguard Children and the Children's Social Care National Framework (June – September 2026) includes consideration of changes to the framewoek and guidance to strengthen practice in responding to potential extreme violence by children. See: p.55 DfE June 2026 Consultation

b. Current levels of understanding about this risk are low and will require strengthening through guidance, training and potentially amends to local policies.

6) Expanding MAPPA's remit to include NIEV risk individuals would require legislative change, either by the introduction of a new category (to section 325(2) of the Criminal Justice Act 2003) or amendments to category 3 (section 325(2)(c)). It would also involve drawing into MAPPA a fundamentally different cohort of individuals who pose risk, as MAPPA is for and designed around convicted offenders. There are a range of calls to extend the cohorts captured by MAPPA through extending those captured by notification requirements (e.g. child abusers, animal abusers, stalking and domestic abuse offenders). Independent reviews and a succession of HMICFRS inspections have identified that police resources are already overstretched in managing the current MAPPA cohort with the ratio of offender managers to those managed above recommended levels. The key consideration in this space is accordingly focusing statutory obligations for offender management against capacity to ensure resources are focused on highest risk individuals.

7) The Potentially Dangerous Persons (PDP) scheme is an early prevention mechanism. At present PDPs are primarily, although not exclusively, police driven and whilst in areas where they operate they may be part of the mechanism by which the Serious Violence Duty is discharged they have no statutory underpinning. Putting PDPs on a statutory footing would require consideration of thresholds for support and how best to define their remit. Current guidance indicates that they can deal with a broad range of public protection risks and so there may be implications for other areas of prevention policy, and particularly if any duties were placed on frontline professionals to make referrals which may be necessary given the early prevention/intervention nature of PDPs, and that NIEV related risk may be identified outside of policing.

8) For MASH to play a consistent and clearly defined role in the management of NIEV risk a fundamental change to statutory safeguarding thresholds under the

Children Act 1989 (ss. 17 and 47)[31] and Care Act 2014 (s.42)[32] would be required. It is likely that wider legislative change to place MASH on a statutory footing covering children and adults and to clarify their specific role would also be needed. This could include provision for a triage function, requirements around assessments, and potentially a case management function.

9) We do see however within the Prevent system how MASH systems (or similar, where they exist) frequently play a role in initial consideration of Prevent cases, in parallel with CTP, and we are aware anecdotally of some local areas where MASH is being used to provide support for some individuals at risk of NIEV. We will seek to learn from emerging practice at the local level to inform policy development and pilot activity as referenced above.

10) The bars set for both child and adult safeguarding intervention are high, and centred predominantly on the risk of harm posed to a person, rather than the risk they themselves pose to others. A person with complex needs who poses a public protection risk, even where managed by a multi-agency structure such as Prevent, may not meet the statutory criteria for support from particular services, or may not have sufficiently serious needs that they are prioritised for support (e.g. assessment and treatment by healthcare), making it challenging to manage this risk. Consequently, any legislative change to place multi-agency safeguarding arrangements on a statutory footing would also require a fundamental policy and culture shift across social care to ensure the threshold assessments give sufficient weight to individuals posing a public protection risk. Consideration would also be needed around prioritisation of access to services, in particular healthcare assessment and treatment. As with other existing

---

[31] Section 17 makes provision for the general duty of local authorities to safeguard and promote the welfare of children within their area who are in need, namely children who are unlikely to achieve or maintain a reasonable standard of health or development without local authority services, their health or development will be significantly impaired without those services, or they are disabled.

Section 47 sets out the circumstances in which the local authority is under a duty to investigate to decide whether to take action to safeguard or promote a child's welfare, namely when the child is the subject of an emergency protection order, in police protection, or where they have reasomable cause to suspect th child is suffering or likely to suffer serious harm.

[32] Section 42 sets out the circumstances in which the local authority is under a duty to conduct safeguarding investigations for adults in its area, where the adult has needs for care and support, is experiencing, or is at risk of, abuse and neglect, and as a result of those needs is unable to protect himself against the abuse or neglect or the risk of it.

systems, MASH and social care operate within an already overstretched system, so capacity and resourcing considerations would apply here.

11) Finally, existing multi-agency structures will not have an understanding of the online information environment, how this acts to drive public protection risk, and how best to assess the role it plays in an individual's risk. Given the pace with which the online information environment can change and evolve, both in the context of safeguarding and public protection risk, this is a significant task.

A National Prevention Gateway or 'Big Front Door'

384. Lord Anderson's 'Lessons for Prevent' Report considered in Chapter 5 a proposal for a wider violence reduction strategy advancing *"a proposal . . . to place Prevent within a comprehensive safeguarding and violence prevention strategy, behind what is sometimes referred to as a big (or wide, or agnostic) front door"* and making a recommendation that *"A Cabinet Office task force should be established to lead exploratory work into the possibility of formally connecting Prevent to a broader safeguarding and violence prevention system."* Responding formally to Lord Anderson's Report, via letter to the current Independent Prevent Commissioner, Mr Tim Jacques, the Home Secretary noted that in response to this recommendation the NIEV Taskforce had been set up and, working alongside the Inquiry, would consider the range of existing multi-agency and safeguarding arrangements, how they interact with Prevent and what more might be needed **[JE/124 - HOM000529].**

385. Accordingly, given that the testing of Lord Anderson's proposition is both central to the current and planned work of the NIEV Taskforce and also highly likely of significant interest to the Inquiry, I think it appropriate to set out here the department's current thinking on this, including areas which may prove to be particularly challenging (noting that Lord Anderson's Report provides a helpful initial analysis of the potential advantages and challenges such an approach might entail). I should emphasise that, given that the department has not yet been able to prioritise a full and detailed assessment of this proposition this current thinking is necessarly subject to change, not least because the work of the Inquiry may very helpfully make a significant contribution in this regard.

386. We currently understand the proposition to be composed of three broad elements:

1) First, that a 'Big Front Door' could be designed to replace the current requirement for frontline professionals to direct referrals to a variety of different agencies or multi-agency groups with a requirement to direct referrals, irrespective of the type of concern, to a single triage function which could assess against a range of risk factors and refer onwards to a suitable specialist intervention pathway.

2) Second, that multi-agency risk management of particular sets of risk (for example those relating to the risk of abuse in the home, those relating to the potential to become involved in criminality, those relating to terrorism etc) could be brigaded around a series of specialist intervention pathways along the Prevent and Channel model.

3) Third, that a capability would need to exist to manage the onward transfer of individual cases within and between those specialist pathways according to the assessment of risk at a particular point, thus ensuring the right interventions were available for the right person at the right time.

387. On the face of it this is an attractive proposition although, as Lord Anderson notes *"the difficulties and complications should not be underestimated"* and one which the NIEV Taskforce will test in the course of its work. Turning briefly to each broad element:

1) On the First, we consider that the operation of a 'Big Front Door' type model would highly likely need to be based on locally delivered triage of referrals relating to a defined set of risks. There would be choice about which particular sets of risk were within scope of such a service – including the potential to frame exclusively around the potential for there to be risk from an individual (public protection risk), as opposed to risk to an individual (safeguarding risk). This proposition would still require cases sent down the public protection risk referral route to receive the necessary safeguarding support as part of risk management, as already happens in Prevent and Channel, for example. Where wider safeguarding referral routes remain in place relating to risk to the individual, these would of course require safeguarding practitioners to remain alert to any signs that that individual did in fact post a risk to others, and act accordingly.

2) Lord Anderson's specific suggestion that MASH might be an appropriate framework through which to conduct such locally based triage across a range of risks (both from and to a person) raises the particular challenge of the statutory position of MASH and generally, although with some exceptions, the current focus of MASH exclusively on risk to an individual.

3) On the Second, we consider that such pathways already exist to a greater or lesser extent (as explored in Section C, and paragraphs 379 - 383 above) but that there would be significant challenges involved in placing them all (or a sub set) on a broadly equitable footing in terms of their ability to absorb, assess and agree appropriate risk mitigation measures for individuals referred to them. Given the potentially wide variety of risks in play, and that intervention takes place at earlier or later stages of this risk playing out it may be considered that (as at present) varying degrees of legal status, national standards, resourcing and so on would continue to be accepted as proportionate responses to different risks – but this may exacerbate the challenges set out on the third component. On the particular treatment of NIEV risks such an arrangement would not resolve the outstanding question of the most suitable specialist intervention or risk management pathway, although it would not preclude continuation of the current model, where some cases with a violence fascination risk factor are suitable for Prevent and others are not, nor, alternatively, the routing of cases to a particular pathway based upon that risk factor alone.

4) On the Third, in line with comments made by the Chair in his opening statement, we consider that there are potentially significant practical and cultural barriers which would need to be overcome. Perhaps the most significant is likely to be the provision of mechanisms to track a potentially very large number of complex and sensitive cases (depending upon the agreed scope of such a system) through an extremely complex patchwork of IT systems in such a way as to meet all relevant legal requirements and to enable the seamless transfer of all of the information necessary to make informed decisions about risk over the lifetime of a case.

388. Stepping back, it is foreseeable that the work undertaken by the NIEV Taskforce may identify further potential advantages and challenges with this very significant proposal.

We do not at this stage rule out a proposition for Ministers which draws on some or indeed all of these elements to a greater or lesser extent.

Wider work that will inform conclusions

389. In this section, drawing on the key elements of a system approach that I have identified (paragraph 377) I set out some of the wider work that will be progressed by the NIEV Taskforce and will inform our conclusions on the appropriate systems approach. Assessment of costs, proportionality and deliverability will be fundamental to our work in developing propositions for Ministers. At this stage we have not costed options.

The harm we are seeking to prevent

390. We need to test our definition of NIEV with policy and operational partners. This will involve continuing to draw on case study examples where it could be considered that non-ideological extreme violent acts have been committed, learning from frontline practitioners (including Prevent practitoners) who are identifying NIEV risk and will need clear and practical definitions in order to direct operational activity, and working with international partners to draw on their insight and expertise. A key challenge is distinguishing NIEV from other types of harms, e.g. gang violence and general knife crime. We will aim to ensure that our articulation of the harm we seek to prevent is capable of dealing with different types of new/emerging threat. We should also take into account new proposed criminal offences linked to EVC and preparation of a mass casualty attack.

391. A clear understanding of what the NIEV threat and resulting harm we are seeking to prevent is and its intersection with other threats will provide the basis for assessing the effectiveness and relevance of existing and proposed interventions.

Equipping frontline services to identify NIEV risk

392. Any systematic effort to address NIEV risk must ensure that such risk is identified at an early stage, appropriately assessed and escalated to a mechanism which can consider and as necessary deliver appropriate interventions. Identification is the first stage. Our experience with Prevent tells us that frontline professionals in education health, social care and policing who have day to day contact with children and young people as part of

their core professional responsibilities are uniquely well placed to identify a range of safeguarding and public protection risks, and there is no reason to suppose that NIEV risks will be any different in this regard.

393. Whatever approach is ultimately adopted, whether it is adapting or extending existing structures or developing a new system targeted specifically at NIEV risk, and in either case what the referral routes look like, it will be necessary to strengthen awareness and capability across existing frontline services to ensure frontline professionals are better equipped to identify, record and escalate NIEV risk to a forum capable of managing it. In the Prevent space this is achieved by the Prevent Duty and the associated training that we offer to frontline professionals (including Notice, Check, Share). In considering how best to equip frontline professionals to identify NIEV risk we will draw on our experience of Prevent, and look to the wider public safety space where there may be further experience and learning to draw from (for example, gang violence or child exploitation). Any approach will need to address the importance of being alert to relevant online behaviours.

394. We must also ensure appropriate advice and guidance is available for others who may wish to report a concern, to support them in identifying behaviour of concern. This could include family members, friends, members of the wider community or the general public. Options to raise awareness within online communities and spaces could also be explored here, including around potential reporting routes.

Understand referral routes

395. We need to develop our understanding of existing referral routes for individuals who pose a NIEV risk. There are currently many different ways that a safeguarding or public protection concern can be raised, considered, and 'referred' to an appropriate agency or multi-agency structure for support. Cases of concern can also be referred onwards between different agencies or multi-agency structures to ensure they are considered for the most appropriate form of support, or additional forms of support for the risk identified. Alongside this, we must also identify where there are gaps that might mean a referral concerning a person who poses NIEV risk does not get picked up. This developed understanding will inform our consideration of the most appropriate 'referral route' or way to raise a concern about an individual who may pose a NIEV risk, noting that what sits behind a referral route – or which agency or multi-agency structure receives a NIEV

referral and is equipped to deal with this risk – will to a great extent inform the referral mechanism itself.

Ability to assess risk

396. The Inquiry Phase 1 report highlighted that the absence of a common risk assessment mechanism leaves a significant gap in the ability of the public services to provide protection for the public from those who pose a real threat of serious harm. The Inquiry recommended that Phase 2 consider the development of a shared multi-agency risk assessment tool that is clear, accessible and suitable for use across public sector services.

397. Any system needs to have an appropriate framework to assess risk, which in Prevent is the PAF but there are a range of other tools used in public protection contexts (e.g. OASys in probation). The Home Office is clear that development of a risk assessment tool for NIEV risk would be advantageous to strengthen early intervention and diversion for individuals, and provide consistency for decision making. The tool will look at risk factors, characteristics, behaviours and indicators, to inform decisions as to where the risk should be managed and what disruptive or supportive interventions are required.

398. As with the PAF, any tool would need multi-agency collaboration for completion and result in a shared plan for intervention/support. The Home Office assesses that to ensure expertise, clarity, consistency, case formulation and accountability, any assessment using a risk assessment tool would benefit from being conducted with input from multi-agency partners, and within the appropriate multi-agency structure. This could see a designated individual responsible for completion if required – with appropriate training and guidance to support. Use of a tool within a multi-agency structure would mean an assessment could take account of all of the relevant information and insight into the risk posed by an individual, and draw on a comprehensive range of options and interventions to manage this risk under a support plan. Any such tool may benefit from a strong legal basis (e.g. duties to share information / power to collect information) and/or be supported by statutory guidance. This approach would be preferable to a tool used within separate public sector services to assess NIEV risk – as this would not benefit from multi-agency input and expertise.

399. The early stages of development work for this tool have commenced but will take time. Development of the tool will need a robust evidence based, drawing on up to date

research and evidence by experts in this field, and implementation will require comprehensive training and guidance for users. HO is in discussions with CT-ARC about developing a NIEV risk assessment tool, drawing on learning from development and delivery of the PAF for Prevent referrals and Channel cases.

Ownership of risk

400. Ensuring that the system makes clear where responsibility for management of the risk lies will be key to any proposal we identify, and will inform development of referral routes and risk assessment tools.

401. We know from existing risk management systems, whether they relate to safeguarding, early intervention or prevention, or public protection – that a multi-agency approach is preferred, due to the often multiple and complex needs an individual may have, and in order to access a broad range information in order to best understand an individual's risk and needs. It follows that any approach to managing NIEV risk must be multi-agency in nature, and involve at a minimum policing, health, social care and education specialists, as well as the local authority, justice services, and wider services or individual expertise where relevant.

402. It is important to emphasise that participation in any multi-agency risk management model cannot absolve any agency from their statutory duties. Rather, the multi-agency construct enables participants to take collective responsibility for assessing and managing risk presented by complex cases. Futher still, a shared understanding of the risk assessment and management plan in a given case also enables each individual agency to deliver their respective support and intervention in a co-ordinated way, thus achieving greatest effect. In this context, ownership of risk is both specific to each agency in line with their statutory duties and shared in respect of a commitment to understand the full risk picture and to deliver an agreed and co-ordinated set of interventions to manage it. Taking the example of a Channel Panel responsibility for agreeing a support plan is shared, whilst responsibility for the delivery of each individual element of that plan is owned by the relevant agency. Risk therefore sits both with the Channel Panel as a whole and with each individual agency for their respective remit. Thus, recommending a referral to a mental health team as part of a support plan does not equate to transferring risk ownership or accountability solely to that agency.

403. In the case of a Channel Panel the functions of the Panel, its membership, the duties of each partner and its chairing by the Local Authority are all provided for in statute.[33] The Home Office view is that the placing of this multi-agency panel on a statutory footing in this way, and the clear identification of the Local Authority as the chair, has been essential to the effective delivery of Channel, including the development of a culture of shared risk ownership rather than risk transfer.

404. Self evidently, where the risk of extreme violence is imminent, or the risk around an individual is escalating and requires more active investigation and monitoring the responsibility falls to policing, as the ultimate body responsible for public safety and the prevention of crime. Given the nature of the NIEV threat, that often there is a significant online element, and that detection and investigation of escalating NIEV risk may at times require specialist expertise or capabilities, we must consider carefully how policing as a whole will approach this issue, and what the respective roles are of frontline policing, the NCA and CTP. This must be considered in the context of longer term police reform.

Case management

405. Case management systems across public protection and safeguarding will vary significantly, but as I have already noted, fundamentally the objective of a case management system is to enable the exchange of information between relevant parties so that appropriate actions and mitigations can be identified.

406. For many safeguarding and public protection or prevention arrangements, records are not held at a national level, with local areas adopting approaches best suited to their local arrangements and information and record keeping systems, working within existing information sharing legislation. The gold standard for recording and maintaining awareness and assessment of NIEV risk would be a national case management system, similar to that used by Prevent, or for management of CT Nominals. This would be a significant piece of infrastructure to design and build, with equally significant resourcing and cost implications.

407. It is unclear where ownership of such a case management system would sit – it would likely need to be owned by an agency or body with a national footprint, and which could provide funding, oversight, and assurance around performance. In addition to

[33] Counter-Terrorism and Security Act 2015 ss. 36-38

management of individual cases the benefits of a national system with uniform data points include consistency of approach and greater visibility of the operation and effectiveness of the system. This assists in identifying improvements to policy and operational practice when managing the NIEV risk, and ensuring learning from case reviews in the event of an incident or serious harm being perpetrated is disseminated to all practitioners. This expectation could partly fall on the Home Office given its role in overseeing public protection arrangements, and so access to the data for the purposes of oversight, assurance and policy development would be required. From experience, we know that it is extremely challenging to maintain the right level of access to data held by operational partners for these purposes, and so expectations placed on central government may not be met without clear, possibly statutory, provision for appropriate access to data.

408. It is likely that such a case management system would need to be underpinned by an appropriate statutory basis, to ensure that information is held on a lawful, necessary and proportionate basis.

Interventions

409. If a multi-agency structure is used to assess, determine a support plan, and manage the risk of NIEV around an individual, then this structure would be able to draw on the range of services and capabilities across health, education, social care, justice, policing and the local authority. This would see interventions primarily being delivered at a local level. Existing good practice includes options for interventions to be delivered by local civil society organisations, or for small amounts of funding to be made available to build protective factors around an individual.

410. Given the nature of the NIEV threat, additional specialist interventions may be required, which could include expert mentoring, psychological interventions, or online/cyber type specialist interventions. These could in many cases be provided at a local or regional level via multi-agency services or policing bodies with support from the relevant service or department to compile a toolkit of intervention or support options that could be easily drawn on by multi-agency partners when considering support plans for individuals at risk of NIEV. However some interventions capabilities may need to sit at the national level, where these are particularly specialist, or when dealing with particularly high levels of risk. This could include cases where specialist and up to date knowledge of the online

information environment is required, in order to provide credible intervention and inform ongoing risk assessment.

411. It is important to emphasise that any structure or multi-agency involvement will only be as effective as the availability and capacity of support services. An individual who poses a public protection risk is not automatically able to access the full range of interventions delivered by public services (mental health support, social work, education plans, housing etc.) as, no matter how dangerous that person is, they may not meet the statutory thresholds for that support, waiting lists may be significant or they may lose their eligibility through failure to engage (e.g. missed health appointments can lead to a person being put back on a waiting list). Thus even with a multi-agency risk management structure in place, for some individuals it will still be very hard to ensure they can actually access the support that might mitigate the risk they pose. Thus our consideration of provision of interventions and support needs to include consideration of prioritisation by public services where there is an identified public protection risk.

Legislative options

412. We are conscious when considering legislative options around NIEV that legislation can take significant periods of time to deliver. Detailed consideration of economic impact, implications for existing policy and delivery, and potential for unintended consequences is required. As is set out earlier in this statement, it is our intention, via the work of the Taskforce, Prevent and other routes, to make sure that we can provide suitable interim guidance, updated training, and to learn from emerging local approaches and pilot activity so that we can manage NIEV risk in the more immediate term. We will however seek to explore longer-term options for legislation.

Expanding the remit of existing multi-agency structures

Prevent

413. We have previously explored options for making changes to Prevent legislation, specifically s.36 of the CTSA 2015. This would be with the aim of clarifying beyond doubt to Prevent practitioners that the presence of ideology is not required in order to be vulnerable to being drawn into terrorism. This is because anecdotally, we have in the past been made aware of practitioners who will place more emphasis on the definition of 'terrorism' rather than considering the broader risk that someone may be vulnerable to being radicalised and drawn into terrorism, when making assessments using s.36. The

intended effect would be to support more consistent decision-making by practitioners, in cases where there is no ideology, but other factors such as fascination with violence, or engagement with concerning material online, may indicate a broader vulnerability to terrorism. Further consideration is needed on what impact this would have on referral numbers, Channel case numbers, and the resource and capabilities required to support this, but in theory, the impact on Channel case numbers should be minimal as we would not be substantively changing the scope of Channel.

414. Under the work of the Taskforce we must carefully consider, alongside a broad range of other options, whether to expand explicitly Prevent's remit so that it deals with all forms of extreme violence. This would require more substantial change to the Prevent and Channel Duty legislation, with more significant implications for resourcing and capacity within the system.

Prioritisation due to public protection risk

415. Given, as I have explained (paragraph 411 above), that some individuals when being considered for support under multi-agency structures may not meet the relevant statutory thresholds for support, or may not be prioritised for support given the relative needs of others, and the challenge this can pose for mitigation of public protection risk, cross government consideration has already been given to the need to prioritise those who pose a public protection risk in a range of support services and healthcare.

416. In order to secure priorisation of support services and healthcare on a consistent basis where individuals pose a NIEV risk, or indeed a wider risk to the public, it may be necessary to put in place additional statutory requirements. This is a largely unexplored and extremely challenging concept, with complex ethical and practical implications.

Consent and mandating engagement via civil orders

417. There is experience to be drawn from Prevent when considering whether consent should be sought from an individual - or the appropriate adult in the case of children - where intervention is proprosed to manage NIEV risk. Due to the specific statutory footing that Channel has been placed on, consent is a crucial compontent, with PLP being used to manage higher risk cases in the early intervention space if consent is not provided.

418. The question of consent must be considered when looking at options for expanding, adapting or creating new multi-agency structures, and how this might interact with the wider remit or responsibilities of a structure (for example, whether MAPPA would be suitable given some aspects, subject to licence conditions, may be mandatory).

419. We have heard from practitioners in Prevent and the wider CT system that being able to mandate attendance for an intervention is helpful, in particular for young people who pose significant terrorist risk. The introduction of Youth Diversion Orders is seen as a helpful step, making provision for mandatory attendance and wider measures to be placed around an individual, providing an alternative to criminal prosecution which can bring significant implications both for the individual, and for ongoing management by police, prisons and probation.

420. Work to consider civil orders for individuals at risk of NIEV has already started, and this will be progressed under the Taskforce. We will actively explore whether something comparable to the new Youth Diversion Order could be created to manage the NIEV risk. Such an order is likely to be an important tool to manage risk, however we cannot underestimate the complexity of delivery – including who would apply for a civil order to be put in place, what threshold for imposition of an order would be required, how and by whom compliance with orders would be managed, and what interventions or restrictions would be suitable and proportionate, including relating to online activity.

General public protection duty

421. We could consider placing a general duty on frontline professionals to be alert to and report concerns where somebody may pose a risk to public safety. This would be a significant step, but could provide statutory backing to supporting a cultural change towards public protection risk, and more systematic consideration of this. In practice, many frontline professionals and safeguarding practitioners will be alive to public protection risk and handle this in line with existing statutory requirements and guidance, and will be aware of how to report concerns to the police. An alternative approach will be to ensure that the need to be alert to public protection risk and consider of the harm someone may pose to others, is embedded in existing local, national and statutory and sector-specific training.

Duty to Warn

422. Phase 1 of the Inquiry indicated that options to make specified categories of people under a legal duty to warn about, or a duty to report, the criminality of another should be explored. As set out in the Government's response to recommendation 67 of Phase 1, the government is exploring the merits of this proposal with the Law Commission.

Online Information Environment

423. The Online Information Environment is a key feature of a wide range of public safety and national security threats, including extreme violence, whether ideologically driven or otherwise.

424. Earlier in my witness statement (in Section F) I describe measures already in hand and commitments made by the government to act in response to this challenge. In this section I set out the importance of a long-term strategic approach and some of the specific challenges which this might seek to address. The Inquiry will recognise that in so doing I am necessarily moving beyond the realm of settled government policy and providing my own professional views and my intent is to distinguish as clearly as possible where this is the case.

425. The impact of the online information environment on our society is one of the most significant factors in public policy. There are clearly huge benefits arising from the internet and the information and applications to which it enables access. There are also very significant risks which manifest and which both enable and exacerbate a wide range of public safety and national security threats. In some cases the role of the online information environment is now intrinsic to the manifestation of such threats. Terrorism is one such example. It is in my view likely that NIEV is another.

A Strategic Approach

426. The department recognises that there is significant merit in designing harm or threat specific interventions in the online information environment. I detail a number of these in respect of terrorism at paragraphs 230 to 258 and in respect of NIEV and / or CSEA at paragraphs 259 to 305. On the one hand such interventions, which range across operational activity, company engagement and narrowly focused legislation, can be targeted at the particular characteristics of a specific threat type. They require knowledge

of the particular threat type and of at least one aspect of its online manifestation. They can generally be put in place reasonably rapidly, although this may depend upon scale and scope. On the other hand such interventions are by design narrower in scope, they may target only specific services or types of service, they may be more prone to targeting only the visible characteristics of a particular threat, and, particularly when viewed as a whole, they may not be the most efficient means of delivering the desired outcome across a range of threats.

427. The department recognises that it is necessary to take a more strategic approach to understanding and addressing the characteristics of the services and ecosystems which make up the online information environment which are assessed to be the most significant drivers of threat and risk. The OSA represents a significant first step in addressing online harms and improving platform accountability. However, the scale and complexity of the online environment require a broader and more strategic approach across government, complementing the regulatory framework established by the OSA and addressing risks that extend beyond its scope. That work is led in the Home Office by the ETSSU. I set out below a selection of the characteristics currently considered to be most significant in this context and, where appropriate, discuss potential options for interventions which are or may in the future be under consideration by the department. I recognise that the scope of this content is broad but there is relevance in each issue to the NIEV threat as well as other public protection risks, and it is, in our assessment, critical that these issues are looked at holistically.

Specific Areas of Concern

428. Algorithmic promotion / recommender systems (see: role of online platforms and communities at paragraphs 209 to 215; pathways from online activity to real-world harm paragraphs 216 to 226). Algorithmic promotion and recommender systems are relevant to the longer-term work described in this section because they shape the content children are exposed to and the speed with which they may be directed towards more harmful material.

429. Further work should consider whether personalised recommender systems should be restricted, or in some cases prohibited, for children (as part of the policy development for the implementation of the social media ban for under-16s and restrictions on high risk features). That work should examine whether children's accounts should be limited to chronological, follower-based, or otherwise non-personalised feeds by default; whether

platforms should be prevented from using engagement-based optimisation to recommend content to children; and whether stronger duties are needed to ensure children are not algorithmically directed towards EVC, toxic communities or other harmful material relevant to NIEV risk.

430. Harmful but lawful content (see: paragraphs 278 to 284 above). The OSA already puts in place significant protections designed to limit children's exposure to certain categories of harmful but lawful content and to give adults more choice over the types of content they want to see. Notwithstanding that approach it remains the case that very significant quantities of harmful but lawful content remain online and are accessed at scale – including via algorithmic promotion as noted above. Measures currently in hand to make EVC illegal represent a shift in the legal definitions of acceptability.

431. As our understanding of the risks associated with significant consumption of harmful content currently considered to be legal develops it may be considered appropriate to bring more forms of content in scope of legal restrictions.

432. Advertising Transparency. Online services depend upon advertising revenue, and businesses depend upon online services to reach their customers. Research indicates that online advertising frequently appears in the context of both illegal and harmful but lawful content.

433. In the future it may be appropriate to consider whether companies and individuals purchasing such advertising should be able to choose whether or not to place their product or service alongside such content.

434. Anonymity. The expectation or assumption of anonymity can be a significant factor in influencing both individual and group behaviours online, contributing strongly to risky behaviours including interactions with harmful or illegal content and a willingness to express or interact with transgressive sentiments, which may in turn fuel escalatory dynamics.

435. In the future it may be appropriate for government to consider the extent to which anonymity is a desirable feature of specific online spaces or services and how that might effect the risk to users and in turn inform the nature of other features which may be desirable or otherwise as part of those services.

436. Risky, or Unlawful User Behaviour. A child making an explicitly extremist statement in an educational setting might reasonably expect that statement (depending upon context) to

inform the consideration of further action by the management of that establishment. At the present time, with the exception of CSEA, there is no requirement for online services or other appropriate online bystanders to report risky or unlawful user behaviour.

437. In the future it may be appropriate to consider the effectiveness of voluntary approaches and whether a mandatory safeguarding or reporting duty is desirable.

438. Social Media (see: proposals for a social media ban at paragraphs 293 to 299; and related device-level interventions at paragraphs 300 to 305). The wider challenge is that social media is not a single risk vector. It can expose young people to EVC, connect them with harmful communities, normalise violent ideation, enable stranger contact, and accelerate escalation through recommendation systems and other engagement features.

439. Future work should therefore consider not only age-based access controls, but also the design of services, the speed and effectiveness of content moderation, the visibility of harmful networks, the role of recommender systems, and how online behaviour can be identified and shared appropriately where it may indicate real-world risk.

440. Virtual Private Networks (see: age verification for VPNs at paragraphs 306 to 309). The key relevance here is that VPNs can undermine platform-level or network-level controls, including age assurance and access restrictions, by masking location or routing traffic around controls.

441. Any future policy response will therefore need to consider how VPN use affects the enforceability of age-based restrictions and other online safety measures, while recognising the legitimate privacy and security uses of VPNs.

442. Device-Level Age Assurance and Safety Features (see: device-level interventions at paragraphs 300 to 305). The relevance to NIEV risk is that device-level approaches may offer a more systemic route to reducing children's access to harmful online environments, rather than relying solely on individual platforms to verify age or apply controls separately.

443. Further work should consider whether the longer-term objective should be a child-safe digital environment, in which age assurance, parental or guardian controls, limits on harmful content, restrictions on inappropriate apps or services, and protections against circumvention are built into the device, operating-system or app-store layer by default. Further work would be needed to scope the feasibility, interoperability, privacy, proportionality, consumer choice, enforcement and respective responsibilities of device

manufacturers, operating-system providers, app stores, platforms, parents and government.

444. Privacy and End-to-End Encryption. (see: effect of online platforms and communities at paragraphs 209 to 215; pathways from online activity to real-world harm at paragraphs 216 to 222; challenges around sharing information about online behaviour at paragraphs 223 to 226).

445. Further work should consider how public safety risk is identified and managed where concerning activity moves from open platforms into private messaging services, including services protected by end-to-end encryption. This should include work with DCMS (formerly DSIT), Ofcom, law enforcement and industry to understand the limits of existing regulatory, safety-by-design and law enforcement levers; whether platform reporting, user reporting, metadata, risk signals or safety interventions can support lawful and proportionate action; and how public safety considerations can be balanced with privacy, cybersecurity and freedom of expression.

446. Toxic Communities (see: effect of online platforms and communities at paragraphs paragraphs 209 to 215, and pathways from online activity to real-world harm at paragraphs 216 to 222).

447. Further work should focus on improving government's understanding of how these communities form, how users move between mainstream and fringe platforms, and which design features, moderation gaps or enforcement limitations allow harmful spaces to persist. This should include work with DCMS (formerly DSIT), Ofcom, law enforcement and industry to consider whether existing online safety duties, voluntary industry engagement and law enforcement capabilities are sufficient to identify and disrupt online spaces that normalise or encourage extreme violence. It should also consider whether learning from counter-terrorism, child sexual abuse and VAWG online threat work can be applied to NIEV-related harms.

448. Escalatory Behaviours (see: pathways from online activity to real-world harm at paragraphs 216 to 222; sharing of information about online behaviour at paragraphs 223 to 226).

449. Further work should focus on whether clearer indicators can be developed to help frontline professionals, platforms and law enforcement distinguish isolated concerning online behaviour from patterns that may indicate escalating risk. This should include

developing common language, improving referral guidance, testing how online behaviours can be lawfully and proportionately shared between agencies, and considering whether pilot activity could help assess how such indicators operate in practice. The aim should be to support earlier identification without creating an overly broad or speculative monitoring regime.

450. Artificial Intelligence (AI). AI has the potential to excacerbate a range of harms online at a pace, scale, and complexity we haven't seen before.

451. Further work should assess how AI may affect both the generation of harmful content and the ability of platforms, law enforcement and government to detect and respond to it. This should include mapping which AI-related risks are already covered by existing online safety, national security and criminal justice work, and where there may be gaps in relation to NIEV. It should also consider how Home Office work on emerging technology, (now) CO-led AI policy and industry safety measures can be aligned so that NIEV-related risks are considered as AI capability develops.

452. AI Chatbots (see paragraphs 295 - 296). AI chatbots and companion bots pose a distinct potential radicalisation risk because they are interactive, personalised and persistent. Unlike search engines or social media feeds, they can simulate an ongoing relationship with the user, respond directly to their vulnerabilities or grievances, and provide repeated validation or reinforcement over time. In some cases, this may increase the risk that a vulnerable user becomes more isolated, more fixated on harmful ideas, or more willing to act on violent thoughts, particularly where the system fails to challenge, redirect or safely escalate concerning content.

453. Further work should consider whether existing platform and AI safety frameworks adequately address these risks. This should include engagement with developers, platforms and regulators on safety testing, redirection and crisis signposting, safeguards for children and vulnerable users, and the circumstances in which concerning interactions could be escalated lawfully and proportionately. Any approach would need to balance public safety, privacy, proportionality and freedom of expression.

454. Stranger Contact (see: effect of online platforms and communities at paragraphs 209 to 215; pathways from online activity to real-world harm at paragraphs 216 to 222).

455. Further work should consider how platforms identify and manage risks arising from unsolicited contact, particularly where children or vulnerable users are moved from open

spaces into private messaging environments. This should include assessing the adequacy of default safety settings, reporting mechanisms, friction in user-to-user contact, and escalation routes where contact appears linked to coercion, encouragement of violence or movement into harmful communities. It should also consider how this work aligns with existing child safety, grooming, VAWG and online harms activity.

456. Infinite scrolling / addictive design features (see: algorithmic promotion and recommender systems at paragraphs 211 to 215).

457. As trailed by then DSIT in their Fact Sheet 'New rules to protect children online' on 17 July 2026 **[JE/125 - HOM000524],** further work should consider whether infinite scrolling, autoplay and other engagement-maximising design features should be treated as part of the same risk environment as algorithmic recommendation. This should include considering whether children's accounts should have stronger default protections, including limits on infinite scroll, autoplay, push notifications, engagement-based recommendations and other features designed to maximise time spent on a service. The focus should be on whether the design of services, not only the content hosted on them, should be more directly regulated where it increases children's exposure to harmful online environments.

CONCLUSION

458. I end this statement by assuring the victims and their families that as we progress this work we will never lose sight of the terrible events of 29 July 2024, and the devastating impact they have had. As I hope will be evident from the summaries provided of the policy work that has been done since the attack in Cathryn Ellsmore's witness statements in Phase 1, our response to the Inquiry's Phase 1 recommendations and in this witness statement, we are committed to addressing the gaps that the attack has brought to the fore, and to supporting the Inquiry's invaluable work to help us do so.

STATEMENT OF TRUTH

I believe that the facts stated in this witness statement are true. I understand that proceedings may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

Signed **Signature**

Dated 31 July 2026