Witness Name: Helen Rance

Exhibits: 22

Dated: 28th August 2026

THE SOUTHPORT INQUIRY

FIRST WITNESS STATEMENT OF HELEN RANCE

---

1. I, Helen Rance, am an officer of the National Crime Agency ('NCA'), Floors 12-14, 12 Endeavour Square, Westfield Avenue, Stratford, London, E20 1JN.

2. I am the Temporary Director of the Threat Leadership Command within the NCA and I have held this role since April 2026. My role within the NCA involves leading on the strategies deployed to fight against Serious and Organised Crime ('SOC') threats facing the UK. These identified threats are varied and complex and include Child Sexual Abuse ('CSA'), Modern Slavery and Human Trafficking ('MSHT'), cyber-crime, drugs, firearms, borders and Organised Immigration Crime ('OIC').

3. I joined the NCA in March 2025 as the Deputy Director of the CSA and MSHT Teams. Prior to joining the NCA, I served as a Police Officer in the Metropolitan Police Service ('MPS') for 23 years. Before leaving the MPS, I spent four years leading the MPS Cyber Crime Unit as a Detective Superintendent.

4. I know that Timothy Wright, Temporary Deputy Director for CSA and MSHT within the NCA, has provided evidence to the Inquiry by way of a witness statement dated 24th July 2026. This followed a request for evidence from the Southport Inquiry dated 25th June 2026 pursuant to Rule 9 of the Inquiry Rules 2006 ('the Rule 9 request'). I have read his statement and I am familiar with its contents and agree with the matters set out therein.

5. I am authorised to make this witness statement on behalf of the NCA to give further detail about the NCA's relevant activities. In preparing it, I have consulted relevant colleagues within the NCA and reviewed relevant documentation. Where matters are within my direct knowledge, they are true to the best of my knowledge, information and belief. Accordingly, this statement builds upon the evidence of Timothy Wright and provides further information regarding the role and functions of the NCA, including its strategic and operational approach to the management of SOC threats. It also sets out examples of approaches which have proven effective in other threat areas, identifies challenges encountered in responding to harms facilitated through the online environment, and outlines measures which the NCA considers may assist in reducing those harms. Finally, I address the NCA's views regarding the development of a whole-system response to the threat posed by Violence Fixated Individuals ('VFIs'). For ease of reference, these matters are addressed under the three topics identified in the Terms of Reference for Phase Two of the Inquiry.

6. The NCA does not have a primary role in identifying, assessing or managing VFIs as a distinct cohort and instead focusses on the wider threat posed by online Com networks. However, given the overlap between certain characteristics, behaviours and risk factors associated with VFIs and individuals involved in Com-related offending, the NCA's operational experience may assist the Inquiry's consideration of these issues.

Roles and Responsibilities of the National Crime Agency

7. The National Crime Agency was formed on 7th October 2013 pursuant to the Crime and Courts Act 2013 ('the Act') and superseded the Serious Organised Crime Agency.

8. The NCA's core remit is to lead the UK's fight to cut serious and organised crime. In doing so we aim to protect the public by targeting and pursuing criminals who pose the greatest risk to the UK's security and economic stability.

9. The NCA is an operationally independent non-ministerial department. This means that it operates as a government department in its own right but does not have its own dedicated minister. Instead, it is headed by the Director General ('DG') who is accountable to the Home Secretary as sponsoring minister, and through the Home Secretary to Parliament. The current Director General of the NCA is Graeme Biggar. The NCA 2015 Framework is a publicly available document which outlines the NCA's accountability, management, operational and financial arrangements and clarifies the relationship between the Home Secretary and the NCA. I exhibit this framework as HR/01 **NCA000006**.

10. While its principal accountability is to the Home Secretary, the NCA is also subject to external and independent scrutiny by Parliament, the Scottish Parliament and the Northern Ireland Assembly, the Northern Ireland Policing Board and other public bodies. The DG is expected to cooperate fully with these bodies. Some of the bodies which have a statutory role to inspect, scrutinise or regulate the functions or activities of the NCA include HM Inspectorate of Constabulary and Fire & Rescue Services, the National Audit Office and the Independent Office of Police Conduct.

11. The NCA has a statutory obligation under the Act, to ensure that it is transparent and that it publishes information about the exercise of its functions and other matters relating to them. However, for reasons of operational security, Parliament decided that the NCA should not be subject to the Freedom of Information Act 2002.

12. The operational independence of the NCA is codified under Section 4(1) of the Act. This gives the DG the power to decide which operations are mounted by the NCA and how such operations are to be conducted.

13. Each year, the DG determines the operational priorities of the NCA in line with the annual strategic priorities set by the Home Secretary. While the Home Office is the primary department with oversight of the NCA's work, it also engages with other government departments. The NCA may negotiate partnership agreements or Memoranda of Understanding with other government departments where appropriate and will keep the Home Office informed.

14. We work closely with partners. Examples of NCA partners are: police forces, HMRC, Border Force, the UK Intelligence Community, government departments and international organisations such as INTERPOL and EUROPOL. The NCA also works closely with organisations in the private, charity and regulatory sectors.

15. The Act provides the statutory basis to allow the NCA to co-operate with its criminal Justice partners. Section 2(5) states that the "NCA must consult with other law enforcement bodies in carrying out its functions".

16. The NCA has a wide range of specialist capabilities which allows the NCA to gather information to identify and target criminals involved in serious and organised crime.

17. Any information received by the NCA which points to serious and organised crime is assessed and developed by our intelligence teams. If the NCA has credible information, the NCA's Tasking team will determine whether the matter should progress to an NCA investigation.

18. The criteria for tasking a new NCA investigation includes assessing whether the operation supports the Home Secretary's strategic objectives and the NCA DG's operational objectives.

19. The NCA investigation team will gather the evidence and may submit a file to the independent Crown Prosecution Service ('CPS'), who will determine whether there is sufficient evidence to charge.

20. The NCA and CPS, although independent from each other, do work closely in complex cases. The CPS may provide early investigative advice which ensures the integrity of the investigation. Prosecutors will guide NCA investigators on the appropriate legal framework, reasonable investigative lines, disclosure obligations under the Criminal Procedure and Investigations Act 1996 and potential criminal charges and evidence. This early involvement of the CPS significantly improves criminal justice outcomes. The NCA Prisoner and Lifetime Management ('PALM') team collaborates with His Majesty's Prison and Probation Service ('HMPPS') to track and disrupt offenders post-conviction through safeguarding, offender management and disruption tactics. Further information is included at paragraphs 146-151 below.

21. The NCA also has a collaborative relationship with the College of Policing ('CoP'). The NCA feeds its expertise on SOC threats into the CoP to support the CoP developing best practice for SOC investigations and continual professional development for all law enforcement officers investigating SOC matters. NCA officers can access the standards and training provided by, and accredited by, the CoP.

Strategic Planning and Reporting

22. Part of the NCA's role in combatting SOC is to identify any significant trends and adapt its approach to tackle any emerging threats.

National Strategic Assessment

23. The annual National Strategic Assessment of Serious and Organised Crime ('NSA') provides a comprehensive insight into the SOC landscape by analysing and assessing information gathered over the preceding year by the NCA, the UK intelligence community, law enforcement and Non Governmental Organisation ('NGO') partners.

24. The NSA is disseminated to a broad range of stakeholders across the UK's security and law enforcement landscape such as the Home Office, intelligence agencies as well as domestic and international partners. The NSA is produced at OFFICIAL-SENSITIVE to

inform business planning across the SOC system and drive operational and policy decision making. There is also a PUBLIC version of the NSA released on the NCA website for a wider audience, inclusive of the media, academia, and general public. T1D/T1E

T1D/T1E

T1D/T1E. I exhibit T1D/T1E as HR/02-NCA000007.

National Control Strategy

25. The NCA National Control Strategy ('NCS') guides the UK's collective operational response to SOC threats described in the NSA. The NCS sets out the annual operational ambitions and the '4P' approach ('Pursue, Prevent, Prepare and Protect') to deliver the greatest impact against those ambitions. The NCS is produced at OFFICIAL-SENSITIVE and shared across select domestic and international partners involved in the fight against SOC.

26. T2D/T2E

T1.

NCA Business Plan

27. T2D/T2E/T2F

Statutory Role of the NCA in Relation to Children and Young People

28. The NCA has statutory child protection obligations in the UK under Section 11 (England) and Section 28 (Wales) of the Children Act 2004, the Children (Scotland) Act 1995, the Children and Young People (Scotland) Act 2014, and the Children (Northern Ireland) Order

1 T1D/T1E.
2 T2D/T2E.
3 T2D/T2E

1995. The framework mandates the NCA to safeguard and promote the welfare of children in the discharge of its functions. Children are defined as being aged below 18 years of age.

29. In relation to children, the NCA's focus is primarily around CSA, whether it occurs online (via an electronic device), offline or a combination of both. When the NCA was created, CSA was managed by the Child Exploitation and Online Protection ('CEOP') team. In 2018, as part of an agency-wide reorganisation, the constituent components of CEOP were relocated into three NCA operational Commands: They are:

    a. CSA Threat Leadership:
    This Command covers threat, education and partnerships and provides oversight on the NCA's response to Com networks via Project Rhyobasalt;
    b. CSA Intelligence:
    Some NCA officers from the CSA Intelligence team are deployed to the Project Rhyobasalt RICC. The Child Sexual Exploitation Referral Bureau ('CSERB')[4] sits within CSA Intelligence and receives referrals from the National Center for Missing and Exploited Children ('NCMEC') which may include individuals in Com networks; and
    c. CSA Investigations:
    This team receives referrals from Project Rhyobasalt and may conduct criminal investigations into members of Com networks. It is also responsible for child safeguarding.

    These three Commands, although distinct, work collaboratively with an extensive range of internal and external partners in order to identity the evolving threat of CSA.

30. The emerging threat posed by Com networks falls within the NCA's strategic and operational response to CSA because the majority of offenders and victims are children. Project Rhyobasalt, the joint NCA and Counter Terrorism Policing ('CTP') initiative to combat Com networks, sits within the NCA's CSA Threat Leadership team[5].

National Governance Arrangements for Serious and Organised Crime

31. As set out below, the NCA response to SOC is underpinned by internal and external governance arrangements. The NCA has formed strong relationships with the police,

[4] The statement of Timothy Wright dated 24th July 2026 provides further information on CSERB and NCMEC at paragraphs 47-49.
[5] Statement of Timothy Wright dated 24th July 2026, paragraphs 41-55.

government, third sector and the CoP. These relationships have developed over many years through established government boards. The boards are discussed below.

National Strategic Tasking and Coordination Group

32. At a high-level sits the multi-agency National Strategic Tasking and Coordination Group ('NSTCG'), which is chaired by the Director General of the NCA and attended by senior representatives from law enforcement, relevant government departments and regulators. The NSTCG meets bi-annually.

33. The NSTCG determines the strategic direction for law enforcement activity against SOC, ensuring effective tactical and operational service delivery by providing scrutiny, direction and support, in line with the NCS.

National Tactical Tasking and Coordination Group

34. Sitting below the NSTCG, is the multi-agency National Tactical Tasking and Coordination Group ('NTTCG'). The NTTCG provides the tactical leadership, governance, responsibility and accountability with regards to a national tasking and coordinating structure for tackling SOC across the United Kingdom.

35. The NTTCG meets every three months and is chaired by the NCA's Director General Threats. I provide updates on Project Rhyobasalt and requirements of the SOC community to support the national response to the Com to the NTTCG and NSTCG as required.

36. Strategic Governance Groups ('SGGs') are senior governance arrangements through which the NCS is used to set and track the progress of operational activity against identified threats. SGGs escalate threat and risks as required to the NTTCG and the NSTCG. They provide a mechanism for the NCA, working with relevant law enforcement and other partners, to oversee the collective response to those threats and ensure that activity is aligned with strategic priorities.

37. Each SGG has a Strategic Action Plan which sets out the activity to be undertaken by the NCA and its partners to mitigate an identified threat and associated risks. It provided a framework for coordinating and monitoring the collective response, with actions assigned to relevant organisations and progress reported through the governance arrangements.

National Assessment Centre

38. The National Assessment Centre ('NAC') also sits within the NCA and it produces a range of intelligence products to inform the governance groups about SOC threats. The NAC can self-task to produce a report but, more commonly, it is commissioned by the SOC community or external groups. The NAC engages with various partners to collect data and trends relating to online offences being committed against children and works closely with Threat Leadership in order to report on the evolving Com threat.

39. To understand the overarching Com threat, the NAC obtains open, closed and third sector reporting gathered via data sharing agreements from pre-existing partner relationships, attendance at relevant boards and working groups, intelligence collection and/or via online research. All material is collected and collated to enable analysis and assessment in line with the Professional Head of Intelligence Analysis standards and guidance.

40. Although some of the reporting is obtained from industry or open source, for instance the National Police Chiefs' Council ('NPCC') / Internet Watch Foundation ('IWF') reporting or NCMEC referrals; some is also obtained from detailed intelligence collection by policing and government partners which comes with the accompanying increased handling conditions and government protective marking. All material is assessed and used to understand the threat, identifying areas such as offender/victim demographics or vulnerabilities, online platforms used to network with like-minded individuals or which offer increased access to potential victims or statements around platform moderation. The NAC also includes research into key trends and patterns that describe and evidence Com offending and identify intelligence and investigative opportunities available to tackle the threat. The assessments are comprehensive overviews of offending and as such, there are strict policies in place to prevent their disclosure to those without the 'need to know' or appropriate vetting status.

41. Examples of partners feeding into the NAC include the NPCC, National Society for the Prevention of Cruelty to Children, Regional Organised Crime Units ('ROCUs'), CPS, T2D, IWF, Ministry of Justice/HMPPS, Lucy Faithful Foundation, CSA Centre for Expertise, The Children's Society, Department for Education, CoP, and the Department of Health and Social Care. The NCA also liaises with industry partners to identify their knowledge of CSA and Com activity on their platforms. This is collated and fed into the NSA.

Terms of Reference - Topic One

Law Enforcement Response to the Southport Atrocities

42. On 28th January 2025, shortly after the conviction of AR, the Director General of the NCA Graeme Biggar, the then National Lead for CTP Matt Jukes and the Chair of the NPCC Gavin Stephens, wrote a letter on behalf of UK law enforcement to the then Home Secretary The Right Honourable Yvette Cooper MP ('the policing letter') proposing measures to mitigate such atrocities occurring again. I exhibit this letter as HR/05– **HOM000254**.

43. The letter stated that the tragic events of 29th July 2024 'brought into stark relief and the public consciousness just what can happen when toxic online content is served up to a teenager with mental health issues, who had fallen out of mainstream education, and who was living in the isolation of his home and online life'[6]. The letter contained a joint assessment of the wider risks and harms posed to children by the toxic online environment. The letter contained policy proposals for the government to consider to enable a whole-system response to this threat, along with actions for law enforcement to support the response.

44. The NCA contributed to this letter to highlight the broader threat to children and the public at large posed by this toxic online environment and to urge the government not to focus on the threat posed by VFIs in silo, but to examine and address these wider online harms.

45. In March 2025, the Southport Diamond group was convened to bring together senior law enforcement leads, including the signatories to the policing letter, to oversee the delivery of the two law enforcement actions, which were:

    i. *We will consider whether there is value in better coordinating or consolidating our approaches to Prevent*[7] *in relation to online crimes, including terrorism, cybercrime, child sexual abuse and other serious crimes – which are currently at very different levels of maturity; and*

    ii. *We will explore establishing a multi-agency task force, supported by a fusion cell to bring together an all-source intelligence collection capability, including*

[6] Policing letter dated 28 January 2025, paragraph 1.

[7] Paragraph 5 of the Policing letter dated 28 January 2025. The reference to 'Prevent' in the first action is a reference to the Prevent strand of the 4P strategy to tackle SOC which is not limited to a pure criminal justice response (Prevent, Protect, Prepare, Pursue).

potentially with industry, against this range of increasingly overlapping online threats.

46. Both of these actions were taken forward by the Project Rhyobasalt Silver Joint Taskforce jointly chaired by the NCA and CTP. Action 'ii' has been successfully delivered by the establishment of the Project Rhyobasalt RICC. The work to deliver action 'ii' has been prioritised and work to deliver action 'i' is ongoing. There are further opportunities for this work to be taken forward by the Early Interventions Working Group within the Home Office Non-Ideological Extreme Violence ('NIEV') Taskforce[8].

47. In parallel, Project Rhyobasalt has developed a Prevent response focussing on Com networks, including options for the production of educational products, new policy and legislation, academic research, online messaging and further engagement with International and Industry partners.

Government Response to the Southport Atrocities

48. In March 2025, the Home Office established the Violence Fixated Individuals Unit ('VFIU') to coordinate government work and develop policy responses to the VFI risk. Various HMG entities and law enforcement representatives sat on the group. The NCA was invited to participate in the VFIU and attended meetings in order to contribute its operational experience, predominantly its experience tackling the threat posed by Com groups.

49. On 22 May 2025, the VFIU produced a draft paper 'Responding to non-ideological extreme violence: interim update. Strategic issues, action to date, further work required' ('the VFIU paper'). The VFIU paper recognised the importance of, and significant difficulties involved in, identifying, assessing and managing the threat posed by VFIs and orchestrating a whole system response. I exhibit this paper as HR/06-**HOM000345**.

50. The VFIU paper was sent to the NCA in draft for comment. The NCA's assessment is consistent with the challenges identified by the Home Office, and in June 2025, the NCA produced a response to this paper. I exhibit the NCA's response as HR/07-**NCA000012**. However, the NCA response stated that the NCA, alongside CTP and National Centre for Violence Against Women and Girls and Public Protection ('NCVPP') colleagues:

[8] See paragraph 90 which explains that the NIEV Taskforce may replace the Southport Diamond Group and the Project Rhyobasalt Silver Joint Taskforce.

'…are seeking to tackle a broader, but not significantly more numerous, phenomenon than non-ideological extreme violence. This policy analysis is therefore unhelpfully restricted to only one aspect of the online-enabled violence phenomenon we and other operational colleagues have been flagging [to] **T1D*** *the Diamond Group, the NCA-CTP announcement of the joint taskforce, and the actual work of the taskforce and the fusion cell. It is partly for this reason that the new maturing chapter of the National Control Strategy for SOC refers to this broader phenomenon as Online-Enabled Violence, which we think is a better descriptor than non-ideological extreme violence'*[9].

***cross government ministerial meeting**

The NCA has, to date, been consistent in its messaging that there is a broader issue of on-line enabled violence to be addressed.

51. The VFIU paper set out on-going work and deadlines, and at paragraph 32 stated:

i. Law enforcement with Home Office to develop options for strengthened ownership of non-ideological violence by mid-July. Options could include:

a. Creating an additional national portfolio holder within the NPCC for non-ideological extreme violence (distinct from sexual violence);

b. A single law enforcement agency is named to lead on non-ideological extreme violence [DN: realistically would have to be CTP or NCA]

52. Addressing this Drafting Note ('DN'), the NCA response stated:

'*On the question of an operational lead for this issue, NCA seniors will want to take a view on any suggestions/recommendations that the NCA should be the operational lead, given tough prioritisation decisions and the pressures on the Agency to focus on other high priority issues like Organised Immigration Crime…'*[10]

53. For completeness, I should clarify paragraph 19(iv) of the draft VFIU paper which erroneously referred to an 'existing NCA VFI cohort'; this is incorrect and, as set out in the previous witness statement of Timothy Wright, the NCA plays a very limited role in identifying individuals who pose a credible threat of real-world violence by disseminating those referrals to CTP[11]. This limited role aside, the NCA plays no role in assessing, nor managing VFIs; there is no 'existing NCA VFI cohort'.

[9] NCA response to the VFIU paper, paragraph 1.1.
[10] NCA response to the VFIU paper, paragraph 4.
[11] Statement of Timothy Wright dated 24th July 2026, paragraphs 13 and 17-23.

54. The NCA did not receive a response to its paper from the Home Office, nor a final version of the VFIU paper. The questions of whether, and if so to what extent, the NCA should play a role in tackling the threat posed by VFIs has not been raised with the NCA since the draft VFIU paper in May 2025. I am aware that the Inquiry is interested in the NCA's views on this issue and I have set out the NCA's position at paragraph 77 below.

NCA Position on the Future Identification and Management of Individuals Who Pose a Risk of Serious Violence and Harm

55. The NCA recognises the Inquiry's concern that the current system does not consistently identify, assess and manage individuals who present a risk of serious violence and harm, particularly where those individuals do not sit clearly within existing organisational or legislative frameworks. However, given the NCA's focus on Com offending, the NCA is not well placed to comment on the effectiveness of existing statutory and non-statutory frameworks, such as Multi Agency Safeguarding Hubs ('MASH') and Multi Agency Public Protection Arrangements ('MAPPA'), as it relates to enabling the identification and management of VFIs[12] or information sharing between agencies about individuals who pose a risk of real-world violence. The NCA does not have the operational experience in dealing with VFIs to be able to comment on the current effectiveness of leadership, coordination and accountability arrangements across government.

56. In my opinion, current safeguarding and criminal justice mechanisms were developed around established offline harm types and do not adequately address newer forms of online-enabled offending such as Com networks, online CSA and exploitation and cyber crime. Based on the NCA's significant engagement with partners in relation to Com network offending, I have particular concerns regarding effective early-intervention pathways for children identified in harmful online spaces, particularly where vulnerabilities are recognised before criminal offences have occurred and they enter the criminal justice system.

57. At present, some individuals who pose a risk of serious violence are identified by organisations with a statutory obligation[13] to refer those at risk of radicalisation into Prevent. Individuals with a non-ideological fascination with violence are not likely to meet

[12] The NCA Prisoner and Lifetime Management Team manage SOC offenders and have some interaction with MAPPA. See paragraph 146 for further information.
[13] Such professionals include social workers, health professionals, teachers and police officers.

the criteria for a Prevent response. Whilst the NCA does not sit on MASH panels, I understand that they focus on the safeguarding of victims and do not routinely receive referrals for offenders.

58. In my opinion, there therefore appears to be a gap in current arrangements concerning individuals who do not clearly fit existing safeguarding, criminal justice or counter-terrorism pathways. One option, as set out in Lord Anderson's report *Lessons for Prevent*, is to expand the remit of the counter-terrorism ('CT') Prevent programme to include non-ideological extreme violence. I understand that this model has also been adopted and implemented with success by Canadian counterparts via The Canada Centre for Community Engagement and Prevention of Violence programme[14].

59. A second option, which has been considered by the Home Office, is the establishment of a separate entity with overarching responsibility for the identification, assessment and management of VFIs.

60. However, the NCA's assessment is that this is not fundamentally a question of which single organisation should own a cohort known as 'Violence Fixated Individuals'. Rather, it is a question of whether the current system has adopted an overly narrow understanding of harm and risk, based upon 'ideological' and 'non-ideological' distinctions which are increasingly difficult to sustain in practice.

61. The NCA's experience across SOC, child sexual abuse and exploitation, online harms, cyber crime, emerging online communities and wider threat landscapes suggests that individuals frequently move between different forms of harmful behaviour, motivations and ideological positions over time. The factors that drive risk are often dynamic rather than static. Individuals may be motivated by grievance, notoriety, fascination with violence, extremist narratives, online group influence, personal vulnerabilities or a combination of factors that evolve throughout their offending trajectory.

62. As a result, the NCA assesses that there is a significant risk in designing future structures around a narrowly defined VFI category based upon motivation through an ideology or not. If systems are constructed around fixed definitions and organisational boundaries, there is

[14] https://publicsafety.gc.ca

a risk that individuals who present a genuine threat of serious harm will fall between existing pathways, or move between categories faster than agencies are able to respond.

63. The NCA therefore believes that the future debate should also focus on identifying and managing individuals who pose a risk of serious violence, regardless of whether that risk is considered ideological, non-ideological, criminal, extremist or otherwise or arises because the individual is fixated on violence for its own sake.

Challenges with the Current Definition of Violence Fixated Individuals

64. The NCA believes there are a number of challenges associated with the current system that differentiates between ideological threat and non-ideological threat. The term VFI implies a distinct and identifiable cohort, separate from those motivated by ideology or involved in Com offending. Whilst such a distinction may appear conceptually attractive, the NCA's operational experience tackling Com networks suggests that the reality is often considerably more complex; increasingly, investigations involve individuals whose motivations cannot be easily categorised. Individuals may consume terrorist material whilst engaging in wider online communities that promote violence, criminality or self-harm. Others move between extremist narratives, misogynistic content, grievance-based violence, fascination with mass casualty attacks and criminal conduct. In some cases, ideology appears central to their motivations; in others it appears incidental, opportunistic or transient. For many, motivation shifts over time[15].

65. The NCA would suggest that ideology is one way of categorising risk, but that risk can also manifest outside of the cohort with ideological beliefs. From a public protection perspective, the critical issue should not necessarily be what an individual believes, but whether their behaviours indicate an increasing risk of committing or inciting serious violence or inciting violence by others, including self-harm. The NCA therefore considers that a focus on ideological versus non-ideological classifications risks obscuring, rather than improving, understanding of the threat. Indicators of an increasing risk of serious violence can come from a wide range of sources, for example social workers, schools and parents, which is why the NCA considers that a whole system response to this threat is required.

[15] T1D/T1E/T1G

66. Law Enforcement engaged in the fight against SOC routinely risk assess by threat using the Management of Risk in Law Enforcement ('MoRiLE') risk assessment tool. Developed by and adopted by the NPCC in 2014, MoRiLE uses a standardised approach and common language to enable strategic and tactical issues to be assessed consistently across Law Enforcement. The tool assesses threat, risk and harm for organised crime and is limited to assessing threat solely from a Law Enforcement perspective; as a whole system response is required to address the threat of VFIs, I believe that a multi-agency risk assessment tool available to all government stakeholders would be required to objectively and consistently measure risk levels. One advantage of a single multi-agency risk assessment tool would be consistency in reporting across a complex system which includes multiple Local Authorities, and social and healthcare services. However, I do not underestimate the issues and complexities in developing such a tool, in particular the issue of sensitive information being shared across multiple departments, system accessibility and hosting.

67. As it relates to current multi-agency information sharing regarding individuals posing a risk of real-world violence, the NCA is not routinely sighted on arrangements so is not able to give a view on whether current frameworks are effective.

Why the NCA Does Not Consider It Appropriate for Responsibility for VFIs to Sit Solely with the NCA

68. Although the NCA agrees that improvements are required, it does not consider that assigning primary responsibility for the identification, assessment and management of VFIs to the NCA would represent the most effective solution.

69. The NCA is designed and legislated to lead the UK's response to SOC. Its operating model, authorities, capabilities and workforce are primarily configured to identify, understand, investigate and disrupt criminal threats at scale. The identification and management of individuals who have not necessarily crossed a criminal threshold is a significantly broader challenge. It requires ongoing risk assessment, safeguarding, behavioural monitoring, information sharing and intervention across multiple agencies. Assigning ownership to the NCA risks approaching the issue through a criminal intelligence lens, when the challenge of identifying individuals posing a risk extends well **before** criminal thresholds are met. The NCA is not structured as a preventative public protection organisation responsible for the management of individuals presenting behavioural risk within communities.

70. Many of the indicators associated with emerging risk first become visible through schools, healthcare providers, family members, social services, local communities and local policing. Effective management therefore relies heavily upon local knowledge, established safeguarding frameworks and multi-agency partnerships. The NCA does not maintain the operational footprint, safeguarding structures or statutory partnerships necessary to perform this function at scale. For example, the management of sex offenders in the community, including those identified or investigated by the NCA, is managed locally by forces in conjunction with local partners[16].

71. Even with significant investment, replicating these arrangements nationally would be challenging and would risk creating duplication with existing systems already operating within policing, safeguarding and counter-terrorism environments.

Current Structures

72. Significant national capability already exists to assess, triage and manage individuals whose behaviour raises concerns regarding future violence. CT Prevent provides an established framework through which vulnerability, radicalisation and behavioural indicators can be assessed and managed before criminal thresholds are reached. However, the NCA's view is that current arrangements create an artificial distinction between individuals with a discernible ideology and those without one.

73. NCA assessment of the Com threat suggests that individuals can acquire, abandon or modify ideological beliefs over time[17]. Others may draw influence from multiple sources simultaneously. Some individuals who initially present without a coherent ideology later adopt ideological narratives. Others appear to use ideology retrospectively to justify behaviour driven by entirely different motivations.

74. A system which depends heavily on proving the presence or absence of ideology, and does not consider harm other than narrowly defined violence, risks failing to keep pace with the reality of contemporary threat. The NCA would therefore support consideration of whether existing prevention and risk-management processes should evolve to better

[16] See paragraph 95.
[17] T1E

accommodate individuals presenting concerning behaviours, regardless of ideological categorisation.

Risks of Creating a Separate VFI Structure for Non-Ideologically Motivated Individuals

75. The NCA believes there are significant risks in establishing a separate VFI structure for non-ideologically motivated individuals or allocating sole ownership to any single organisation, and to do so presents the following risks:

    a. Creating a new silo around a threat that is inherently cross-cutting;
    b. Encouraging agencies to focus on definitions rather than behaviours;
    c. Creating gaps where responsibility becomes contested because an individual's motivations do not align neatly with existing categories;
    d. Duplicating capabilities that already exist elsewhere within government, policing and safeguarding structures; and
    e. Creating a system which continually requires individuals to be reclassified as their motivations, behaviours or expressions of ideology evolve.

76. In the NCA's view, the future system should be designed around the management of threat rather than the classification of motivation; in this context, the risk of real-world violence.

The NCA's Preferred Future Model

77. The NCA's strong recommendation is that the public would be better protected if a system is developed to address the broader threat. This would require an operational system involving NCA and local policing alongside CT Policing, as well as the other relevant public services such as education, healthcare and social services which may be in a position to identify other risk indicators.

78. If the focus remains solely on the narrow category of VFIs, then it would be best to expand the CT Prevent system to include VFIs. However, this would deal with the law enforcement role in tackling this threat, but the bigger gap relating other public services would still remain.

79. In my opinion, any preferred future model will need to be considered on both a short term and a long term basis, to take into consideration, in the short term, current law enforcement and government structures; and long term, the government's recent proposals for police reform. In the long term, a new National Police Service, which incorporates NCA, NPCC

and CTP functions[18], may provide opportunities to strengthen cross-system responses to emerging threats.

80. In the short term, the NCA believes that the current CT Prevent programme should be appropriately resourced and formally expanded so it can adopt cases where there is a risk of non-ideological extreme violence. This is on the basis that CT Prevent is an established multi-agency framework that is already receiving referrals for non-ideological extreme violence. We recognise that this is not straightforward, both in terms of capacity and resourcing, and also in terms of developing the different tools and responses needed to deal with non-ideologically driven behaviour.

81. I note that this appears to be the conclusion reached by Lord Anderson in his report *Lessons for Prevent*. Recommendation 2[19] of the report states:

> *Prevent should remain open to individuals falling within the existing category of "fascination with extreme violence or mass casualty attacks." Consistent efforts should be made to improve the quality of referrals and encourage those that are appropriate, including by providing clear and consistent messaging to potential referrers and to Prevent practitioners.*

82. This suggests that Lord Anderson thought CT Prevent, if properly resourced, was the right vehicle to tackle the threat posed by VFIs. The report goes on to consider the more ambitious proposal to place CT Prevent within a comprehensive safeguarding and violence prevention strategy (which he refers to as a 'big front door').

83. Whilst the NCA view is that CT Prevent could be expanded to include VFIs, it does not necessarily follow that responsibility for an expanded Prevent should remain with CTP. I am aware of CTP's opposition to expanding Prevent in its response to the May 2025 VFIU draft paper. The NCA does not consider it appropriate to express a view as to whether responsibility for an expanded CT Prevent programme should remain within CTP or sit elsewhere within government. This is ultimately a matter for the Home Office and CTP.

84. If an expanded Prevent were to remain with CTP, it would, in my opinion, need to be appropriately and adequately resourced. I am aware of resourcing constraints across law

[18] From Local to National: A New Model for Policing, Home Office White Paper, March 2026 page 10, paragraph 12.
[19] Lessons for Prevent, Lord Anderson of Ipswich KBE KC, July 2025, page 108.

enforcement and I do not underestimate, nor take lightly, the significant resourcing implications that the expansion of Prevent to formally include VFIs would pose for CTP.

85. If Prevent was to be expanded and not remain with CTP, the NCA view is that ideally a single entity with multi-agency capabilities should deliver that function. The NCA's view is that the Home Office NIEV Taskforce is suitably placed to identify a structure through which that remit might be delivered and work has begun to do so. The NIEV Taskforce will, in due course, be well placed to make recommendations on a suitable structure that would provide a coherent and streamlined multi-agency response.

86. In my opinion, such a model would require:

    a. A national referral and triage function;
    b. Joint assessment by policing, CTP, intelligence and safeguarding professionals;
    c. Access to shared intelligence and data sets;
    d. A common risk assessment methodology;
    e. Clear ownership and tasking arrangements;
    f. Robust links to local safeguarding and offender management structures; and
    g. The ability to manage individuals whose motivations cut across existing threat categories.

87. In my opinion, the NIEV Taskforce is well placed to design a process in which agencies are prepared to own and manage risk appropriately, rather than referring it onwards to others. Within multi-agency working there is generally an overarching issue with different departments willingness to own and manage risk appropriately, which is compounded by different risk appetites. I believe this would be an opportunity to design operating procedures setting out clear accountability structures, ownership, responsibilities, information sharing expectations and risk ownership provisions. Clear delineation between organisations in these terms would, I believe, result in a system in which agencies own and manage risk appropriately.

Current Home Office Initiatives to Tackle VFIs – NIEV Taskforce

88. After reflecting on the findings of Phase One of the Inquiry in the context of the policing letter, the then Security Minister, The Right Honourable Dan Jarvis MP, wrote to the DG of the NCA on 13th May 2026. I exhibit this letter as HR/08-**NCA000013**. The letter states that the remit of the NIEV Taskforce is to examine the end-to-end system for

identification, risk management and intervention across violent and high-harm threats that sit across, and in some cases outside, CT Prevent and the counter-terrorism system. The letter helpfully acknowledges the point set out at paragraphs 61-63 above, that the serious harms enabled by the online environment do not sit neatly within policy (or threat) areas but cut across them; and that as a result, a cross-cutting approach is needed, rather than fragmented interventions focused on individual harms in isolation. Whilst still in infancy, the NIEV Taskforce provides welcome governance strategies, accountability arrangements and guidance to address the interlinked issues cutting across safeguarding, serious violence and the online environment.

89. The letter also addressed steps to be taken by the Home Office to better understand online behaviour and escalation of risk, T2E

T2E

90. The VFIU, referred to at paragraph 48 above, was superseded by the NIEV Taskforce. The NIEV Taskforce is the overarching whole government response to the threat posed by VFIs[22]. The NIEV Taskforce is likely to replace the Southport Diamond Group and Project Rhyobasalt Joint Silver Taskforce (which was an initial vehicle to bring together senior partners from across HMG and policing), however this has not yet been formally agreed and documented.

91. Given the Home Office's cross-governmental responsibilities and convening authority, despite its infancy, the NIEV Taskforce has provided the mechanism for convening the

[20] Letter from then Security Minister, The Right Honourable Dan Jarvis MP, to the DG of the NCA dated 13th May 2026, page 2, paragraph 5.

[21] T2E.

[22] The governance structure of the NIEV Taskforce consists of the Governance Steering Board attended by senior officials at DG level and the NIEV Strategic Delivery Board chaired by the Counter Terrorism Director of the Homeland Security Group ('HSG') within the Home Office. Thereunder there are four working groups, three of which are chaired by the NIEV team within HSG: 1. The Southport Recommendations Working Group; 2. The Early Intervention Working Group; 3. The Operational Response Working Group; and 4. The Online Environments Working Group chaired by the HSG Emerging Technology Safety and Security Unit.

required partners together to ensure a whole system response.

92. The terms of reference for the NIEV Strategic Delivery Board ('NIEV SDB') names all contributors to the board, and it helpfully includes representatives from the key government departments with relevant responsibilities. As such it addresses, at official level, the first of the proposals from the Policing letter that a cross Governmental Ministerial group should be convened. I exhibit these terms of reference as HR/09 **NCA000014** . The NCA does not chair any part of the NIEV Taskforce. The NIEV SDB has been convened once to date, and the NCA's anticipates that the NCA contribution will largely be based upon its learning from Project Rhyobasalt and its engagement with the Violent Dangerous Online Communities ('VDOC') Working Group.

Home Office Initiative to tackle Violent Dangerous Online Communities - VDOC Working Group

93. In May 2026, the Home Office also established the VDOC Working Group, with a remit of tackling the threat posed by these online communities. This is a recent development which is likely to improve the coordination and leadership in tackling the threat posed by VDOCs and the NCA view is that it is a good model from which lessons could be learned for VFIs. Through its work on Project Rhyobasalt tackling the threat posed by Com networks, the NCA is a member of both the NIEV Taskforce and the VDOC working group. Whilst the NCA is a contributor to the NIEV Taskforce, it is the VDOC working group's wider focus on combatting dangerous online communities where the NCA can best add value through operational experience and expertise. Whilst the work remains at an early stage, the VDOC working group has progressed work on developing a joined up national approach to prevent movement into VDOCs, disrupting harmful networks and supporting sustainable disengagement and rehabilitation. This is based on evidence gathered through domestic law enforcement efforts to combat Com networks[23], experience from other jurisdictions and academic research into this threat.

94. **T1B**

[23] This evidence has been gathered from the circa 1500 referrals into the Project Rhyobasalt RICC, disruption data captured on the law enforcement Agency and Partner Management System database and international engagement via the Five Eyes Law Enforcement Group.

T1B

T1B

95. I have focussed on the NCA's remit tackling Com offenders within each phase and identified where, in the NCA's view, other departments and industry have a role:

a. **Early vulnerabilities**: Individuals identified at this stage of engagement will not generally have reached a criminal threshold, therefore law enforcement intervention with these individuals is not likely, nor appropriate. This phase is best managed in communities by social and healthcare services, the Department for Education, Department of Health and Social Care and Local Authorities which have the exposure, resources and skills to be able to address these early vulnerabilities.

b. **First Exposure to online spaces:** The NCA's role is limited to:

   i. Sharing operational insight and learning from Project Rhyobasalt with wider policing and industry; and

   ii. Supporting some police investigations with the delivery of safeguarding strategies through NCA Child Protection Advisors.

A whole system response delivered by all departments and industry is required to raise awareness of VDOC through the measures set out in the table.

c. **Involvement in VDOCs**

Law enforcement, including the NCA, lead on protecting the public and preventing crime by identifying those who have committed, or who are likely to commit, criminal offences through investigations, arrests, disruption, network mapping and intelligence development. However, these communities also include a large number of people for whom a law enforcement response is not proportionate and management of them remains in the education/social services/ mental health arena.

The NCA's role includes the delivery of the RICC to triage and coordinate Com network referrals internationally and domestically ensuring a coordinated law enforcement response.

However, the NCA and other law enforcement partners will not work in isolation in this phase and there needs to be a coordinated response across government to deliver interventions.

d. **Post Involvement:** There is a key role for local policing working with partners (such as teachers, social services and youth justice teams) in relation to public protection, building the existing Management of Sexual Offenders and Violent Offenders

('MOSOVO[24]') framework and MAPPA[25] to recognise and address this new type of online offending. This should be part of a wider post involvement coordinated response.

The NCA's view is that post involvement management, including monitoring compliance with ancillary orders, is often most appropriately delivered by local policing and/or local services operating in the same geographical area as the offender. An example that works well is post-conviction monitoring of convicted sex offenders by local MOSOVO policing teams.

96. I understand that similar work carried out by the Home Office in the VDOC working group is being, or will soon be, conducted by the NIEV Taskforce; in my opinion this will assist with identifying and defining the roles that each government department and industry must play to ensure a whole system response to tackle the threat posed by VFIs. Taken together, and along with the wider work on the under 16 use of social media restrictions and nudity filters[26], this provides a good, although inevitably not complete, response to the third proposal for government in our 28th January 2025 policing letter to the Home Secretary.

97. Cognisant of the wider online harms, the NCA has suggested to the Home Office that the NIEV Taskforce and the VDOC Working Group be merged to look at policy to address the broader threat picture.

Terms of Reference - Topic Two

98. The NCA is not a frontline crime reporting or response agency. Most referrals received by the Agency originate from police forces, international law enforcement partners, intelligence partners and industry. Responsibility for responding to individual incidents of real-world violence and identifying individuals who may pose a risk of violence predominantly sits with local policing and other frontline agencies. The NCA's perspective is therefore informed by the intelligence, referrals and investigations that fall within its operational remit.

99. An example of this is that when any referrals are received by the RICC relating to either individuals posing a risk of real-world violence, or Offline Com networks posing a risk of

[24] MOSOVO teams sit within every NPCC police force and manage sexual and violent offenders.
[25] MAPPA brings together the police, probation trusts, the Prison Service and the Youth Justice Board to manage sexual and violent offenders.
[26] See paragraph 115.

real-world violence, then they are referred to CTP[27]. In these circumstances, the NCA is acknowledging a credible threat of real-world violence, as opposed to identifying indicators of fixation with violence where ideology is, or is not, the primary driver. I am therefore unable to provide a view on how effective frontline agencies are at identifying these indicators. From a Com perspective, referrals into the NCA have increased year on year;

T1G

The causes of this increase are likely to be multifactorial and likely to include increased access to the online environment and harmful features and functionalities on social media platforms, such as algorithms directing young people to harmful content.

Project Rhyobasalt

100. The NCA's operational response to tackling the wider online harms identified in the policing letter was to take executive action by jointly setting up Project Rhyobasalt with CTP and policing to tackle the threat posed by Com networks. A high-level overview of Project Rhyobasalt was included in the statement of Timothy Wright[29] and I have set out further information about the project below.

101. The RICC is a small multi-agency capability compromising officers from the NCA, CTP and wider policing partners. It was established in response to the emerging threat posed by Com networks and remains at a relatively early stage of development. The team continues to refine its operating model and collaborative processes whilst responding to a threat that is increasing in both scale and complexity.

102. The RICC is not specifically funded; at present, the NCA involvement in the project is funded out of core NCA funding and we have reprioritised resources within the NCA to react to this new and growing threat.

103. The RICC is staffed by officers from the NCA, CTP and wider policing partners. Whilst it has demonstrated the value of collaborative working, it was established at pace and continues to operate across multiple organisations, systems and processes. There is no dedicated co-located capability, agencies cannot routinely access each other's systems, and differing organisational processes can create challenges in the

[27] Statement of Timothy Wright dated 24 July 2026, paragraph 53.

[28] T1G

T1G

[29] Statement of Timothy Wright dated 24 July 2026. Paragraph 19 defines Com networks and an overview of Project Ryhobasalt is set out in paragraphs 41-55.

development and management of intelligence. The current arrangements are reliant on strong partnership working and the commitment of those involved and would present challenges if required to operate at a greater scale. Any future expansion would require additional investment in staffing, technology, information-sharing arrangement and governance structures. The RICC is not designed or equipped to identify and management individuals who present a risk of violence. Rather, its purpose is to coordinate intelligence, support investigations and facilitate a joined up operational response to Com related offending.

Neurodiversity

104. Dr Adrian West, a Clinical Forensic Psychologist within the NCA Major Crimes Investigative Team[30] attended a NPCC roundtable meeting held on 6th March 2025 to identify the current HMG ability to identify VFIs. One of the conclusions reached at the meeting included:

> *While neuro-developmental disorders (NDs) and/or mental illness are prevalent in VFI and terrorism cases, it should not be assumed that the presence of either or both is causal. Proper risk assessment requires both evidence and nuance – to avoid false positives among the general population and associated (and unnecessary) stigma*[31].

I exhibit the minutes of this roundtable meeting as HR/11-**NCA000017**.

105. Ahead of this roundtable meeting, Dr West had prepared a brief paper dated 18th February 2025 for the NPCC Chief Scientific Advisor, Professor Paul Taylor, which set out his high level observations on neurodiversity in VFI offenders. I exhibit this paper as HR/12-**NCA000018**.

106. **T1D**

T1D

[30] The NCA Major Crimes Investigative Support Team may, if requested, provide **post arrest** support to police forces investigating major crimes, including those perpetrated by VFIs. Support may include post-arrest risk assessments and Clinical Forensic Psychologists advising on search and interview strategies and/or Behavioural Investigative Advisors advising on offenders from a behavioural science perspective. I am aware that the NCA has provided evidence in response to separate requests for evidence from the Inquiry regarding the Case Studies and I am aware that the Inquiry will be hearing expert evidence during the Case Studies, including from psychiatrists and psychologists on VFIs.

[31] Minutes from the NPCC roundtable meeting, paragraph 6.

T1D

107. T1D

T1D

108. As referred to in the statement of Timothy Wright[32], Project Rhyobasalt also commissioned a report from T1D produced in April 2026 identifying pathways to Com networks. I exhibit this report at HR/15-NCA000021. Page 20 of this report concludes that neurodivergence increases vulnerability to Com related activity and that links are an affinity, but not a causal driver.

109. More widely, the NCA has recognised neurodiversity as a characteristic of offenders in other crime types, for example, the National Cyber Crime Unit ('NCCU') within the NCA has observed neurodivergence as a feature of cyber dependent crime. A recent NCCU briefing stated:

> *Neurodivergence is frequently identified within Cyber Prevent referrals, but current research does not establish it as a cause or general risk factor for cyber-dependent offending. Internal Cyber Prevent research shows that individuals with recorded neurodivergence are also considerably more likely to have existing contact with statutory services, which may increase the opportunities for concerning cyber behaviour to be identified and referred. Cyber Choices responds to individual need through appropriate adjustments, needs-informed practitioners and multi-agency working. These adjustments do not require a formal diagnosis and are intended to improve understanding, engagement and longer-term outcomes, rather than treating neurodivergence as a marker of offending risk.*

I exhibit this briefing as HR/16-NCA000022 and I provide further information on the Cyber Choices programme at paragraph 138 below.

110. T1D

T1D

T1D. I exhibit this report as HR/17-NCA000023.

111. NCA officers have access to training and guidance regarding the approach to neurodiversity in the assessment of risk posed by offenders. This includes a comprehensive online e-learning module aimed at improving operational officers' understanding of neurodiversity that was recently developed by the NCCU.

[32] Statement of Timothy Wright dated 24 July 2026, paragraph 67.

Pathways from Online to Real World Violence

112. T1D

T1D

T1D, T1D, the NCA is aware of an increasing number of offline offending incidents directly linked to Com networks resulting in real world violence, such as animal cruelty and torture, graffiti, arson and violent assaults.

113. While there is a realistic possibility that Com-linked offending will evolve into more serious offline in-person offences, as it has in other countries notably the US. Offending such as stabbings are increasingly listed online as entry requirements to Com networks, these are often listed alongside less serious alternatives such as graffiti. The available evidence suggests that many discussions concerning serious violence may be indicative of bravado, fantasy or status-seeking behaviour rather than genuine intent, although it remains important to recognise that some individuals may progress towards real world offending.

114. No instances of terrorism or mass casualty events perpetrated by VFIs in the UK have been definitively linked to Com networks. There are only four instances of Com-linked offending under the Terrorism Act 2000, all of which relate to the possession and distribution of extremist or terrorist literature. Furthermore, the frequent collection by offenders and suspects of contradictory ideological material, such as both extreme right-wing and Islamist content, is almost certainly indicative of an interest in wider extremist rhetoric, rather than any specific ideological path.

Toxic Online Environment: Wider NCA Response

115. In response to the Government's 'Growing up in the online world' consultation in March 2026, the NCA publicly called for restrictions to be placed on children under 16 accessing online social media platforms. This was based on a joint 'NCA-NPCC Position Paper; Restricting Under 16s Access to Social Media' dated 12th May 2026, which I exhibit as HR/18 NCA000024, along with the NCA Press Release on the Under 16 ban which I exhibit as HR/19 NCA000025, the NCA Media Briefing containing the Director General's remarks at the press conference, which I exhibit at HR/20 NCA000033.

[33] T1D

116. Paragraph 2.1 of the NCA-NPCC Position paper includes the following summary:

The online environment as it currently exists enables online illegal harms and amplifies criminal opportunity, including online grooming, the production and distribution of self-generated indecent imagery (SGII), violence against women and girls, radicalisation, and offline serious violence.

117. The NCA Press Release identifies the features that the NCA considers the most harmful:

In our experience, the features that cause the most risk are commonly found across a range of well-known messaging, social media, gaming and AI platforms, and include:

***Mass discoverability of children** - where children can be easily found or suggested to large numbers of unknown users, allowing offenders to identify and target victims at scale.*

***Unrestricted contact from unknown adults** - where any adult can message a child directly, creating the entry point for grooming and exploitation.*

***Private or encrypted messaging** – used by offenders to move conversations away from the original service into private chats – often on messaging apps – where no one else can see what is happening, and abuse can escalate undetected.*

***Algorithmic recommendations that promote harmful content or contacts** - where systems suggest accounts, videos or communities that expose children to violent or sexual content or individuals seeking to harm them.*

***Nude image sharing** or streaming - where children can be coerced into producing or sharing sexual content, often in real time which can then be used for blackmail or further abuse.*

***Weak age assurance** - where children can easily access adult environments, and adults can misrepresent their age, undermining all other safeguards.*

118. The NCA Media Briefing states:

We have worked with the tech sector on these issues for a decade. This is a diverse sector with companies that have taken different approaches to child safety. Some have made important changes to their platforms to reduce some risk.

But the problem has been getting worse not better. And that is because, at the corporate level, the companies have chosen not to make safety a core design principle.

It is unrealistic to expect tech companies to prioritise safety over profit unless we legislate. When the market fails, the Government has to step in.

The Online Safety Act is a powerful piece of legislation, and we welcome the progress being made by Ofcom in implementing it. But the legislation took six years to pass, and has been three years in implementation. Tougher legislation is now required to create a level playing field where all services know what is required if their products are to be made available to children.

119. The NCA is supportive of the Government's recent announcements that this ban will be brought in, along with the requirement for nudity filtering on children's devices. In addition, the joint NCA-NPCC paper contains the additional recommendations:

***Scope the u16s restriction by function, not brand/platform**. Harm flows from platform functionalities, not brand names. Therefore, a function and risk-based scope (large scale discovery, recommender systems, DMs, at scale content sharing, ability to send nude images/videos) should be adopted with regularly updated coverage to capture new or re-branded services dynamically to reduce displacement. Focusing solely on platforms within the category of social media services could result in platforms and services that are designed with risky functionalities being out of scope. Therefore, we recommend that restrictions on functionality should extend beyond social media services to include, but not be limited to, gaming, secure messaging platforms and AI chatbots, if the evidence base identifies those platforms as high risk. Feasibility of differentiated minimum age limits based on platform risk should be considered when scoping the ban.*

***Pair with device-level nudity blocking**. Minimum age restrictions should be paired with operating system level nudity detection on devices used by under 18s to prevent the taking, sharing or viewing of nude imagery. Implementing both will significantly increase the barrier to CSA offending, reducing offenders' ability to groom, coerce and extort children and young people. Nudity filtering would also reduce non-consensual sharing of nude imagery between under 18s, minimising the risk of blackmail, bullying and isolation victims face when their images are circulated across educational settings.*

***Targeted enforcement of the Online Safety Act and improved Highly Effective Age Assurance (HEAA).** A restriction does not fix unsafe design and must not be a substitute for Online Safety Act enforcement and continued HEAA improvements*

(layered age-assurance methods, periodic re-validation) under Ofcom's Codes. However, children should not remain exposed to unsafe environments while long-term reforms are implemented. Early harm reduction and structural reform are not mutually exclusive.

***Anti-circumvention by design**. Require multi-factor geolocation, active VPN/proxy detection and blocking and re-verification for any change of country or age; treat such changes with temporary feature locks pending checks. Anti-circumvention measures should be strengthened by greater use of age assurance at app-store, operating system or device level.*

***Safeguarding first reporting**. Mitigate suppressed disclosure (reduced reporting by children to parents and professionals) through clear education and messaging that clarifies that any minimum age restriction is not designed to punish under 16s and they will not be blamed for any abuse experienced on age-restricted platforms.*

***Effective prevention online safety education.** Education must be delivered from an early age so children and young people have the skills and knowledge to deal with risks they may encounter when using platforms that are out of scope of a minimum age restriction, or accessing platforms at 16. Education professionals will need guidance on how to do this against the backdrop of minimum age restrictions. Continued delivery of education will likely reduce the impact of a 'cliff edge' that child safety organisations warn of.*

*These policy measures need to be complemented by increased targeted enforcement of the Online Safety Act particularly **Algorithmic recommendations that promote harmful content or contacts** and effective age assurance. There also needs to be further policy work around the risks associated with private or encrypted messaging – used by offenders where platforms cannot see and artificial intelligence*[34].

120. Virtual Private Networks ('VPNs') are commonly used to conceal a user's location and enable access to online services in a manner that may circumvent geographic or age-based restrictions. The NCA is aware of evidence indicating that VPNs have been used to bypass age assurance measures introduced under the Online Safety Act 2023 and Australian social media controls for children. While the scale of such circumvention is not yet fully understood, the NCA assesses that age-based access restrictions are likely to be more effective when combined with additional safeguards, including multi-factor

[34] NCA-NPCC Position Paper, paragraph 2.9.

geolocation checks, active VPN and proxy detection, and re-verification requirement where there are changes to a user's declared age or location.

NCA Recommendations for Industry Relating to Com Networks

121. The NCA has direct engagement with tech companies and in December 2025 issued an industry alert on Com networks to raise awareness, which I exhibit as HR/21- NCA000026 and NCA000027. The alert made recommendations on how platforms can better prevent and detect offending and safeguard users. In relation to Com offending, the NCA recommends that industry implements the following platform-level measures to improve online safety:

a.

b.

c.

d.

e.

T1D

f.

g.

h.

i.

Terms of Reference - Topic Three

122. The NCA's engagement with social media platforms and tech companies predates the emergence of the relatively new threat posed by the Com; for many years the NCA has engaged with industry to prevent and disrupt online CSA offending. The NCA directly engages with platforms such as Meta, Snapchat, Discord, Roblox, TikTok, and Telegram on a regular basis.

123. The threat posed by Com groups has been recognised internationally, and the NCA works closely with overseas partners to develop a coordinated approach. This includes engagement through the Five Eyes Law Enforcement Group ('FELEG'), which is currently chaired by the NCA. FELEG's response to the Com threat is delivered through **Project A**. In March 2026, **Project A** convened a public-private partnership event in New York, bringing together representatives from all FELEG member countries and 13 industry partners. The event facilitated the rapid exchange of intelligence and operational insights, resulting in a number of law enforcement investigations being progressed, while industry partners opened new investigations, identified previously unknown account users and supported urgent safeguarding interventions. All participating organisations indicated their willingness to support further collaborative activity.

124. Given the use of CSA material by Com networks, the NCA's established relationships with social media companies and tech platforms are also being used to raise awareness of this threat and prompt an appropriate response from industry.

125. The NCA does not possess regulatory powers to require online platforms to remove harmful content. The NCA works closely with Ofcom and provides operational insight into the services, platforms and technologies being exploited by offenders. Where illegal material, exploitation networks of serious criminal activity are identified, the NCA engages with technology companies through established partnerships and reporting mechanisms. This can result in the voluntary removal of content, accounts or services that breach platform policies. In the context of criminal investigations, the NCA may also request the preservation of relevant data. Formal content removal is typically facilitated through established industry processes or specialist organisations such as the IWF.

126. The NCA, along with other law enforcement partners, is currently supporting the Ministry of Justice and the Home Office on policy proposals to develop legislation prohibiting online extreme violent content. This work is in the policy development phase and the NCA does not underestimate the significant challenges and complexity of developing these proposals.

Analogous NCA Operational Areas

127. Whilst the NCA does not have responsibility for the identification, assessment or management of VFIs, it has relevant operational experience in a number of comparable threat areas. These include CSA investigations and prevention, the NCCU's Cyber Choices programme, and the management of SOC offenders through the PALM Team. The examples set out below identify the operational strengths, challenges and lessons learned which may assist the Inquiry in its consideration of future arrangement for managing VFIs.

(i) CSA Investigations and CSA Prevention

CSA Investigations

128. The NCA adopts CSA investigations where the threat, harm, complexity, sophistication or international dimension exceeds local and regional policing capability, or where specialist NCA capabilities or national coordination are required.

129. Com investigations may be adopted by the NCA where key administrators, organisers, moderators or other influential individuals are responsible for driving significant harm within online communities, and where effective disruption requires specialist capabilities, proactive tactics, covert methodologies or a coordinated national response.

130. The majority of online CSA investigations remain the responsibility of local police forces and ROCUs. The NCA may nevertheless provide specialist support where appropriate[35].

Operational Strengths Identified in CSA Investigations

131. Operational strengths identified by the NCA CSA Investigations team include:

a. Strong intelligence development, analytical capability, and proactive risk assessment of suspects and victims;

b. Effective international partnerships, particularly with overseas law enforcement agencies, supporting offender identification, victim safeguarding, intelligence sharing, and coordinated operational activity; and

[35] Paragraphs 49 and 51 of the witness statement of Timothy Wright dated 24 July 2026 set out the process for CSA referrals within the RICC.

c. The ability to deploy specialist Child Protection Advisers and victim-focused resources nationally to support arrests, safeguarding and coordinated victim engagement.

T1D

132. T1D:

a.

b.

c.

d.

e.

f.

T1D

Safeguarding Themes

133. The following safeguarding themes have been identified in CSA Com investigations:

a. Many suspects are children or young people, often presenting with neurodivergent conditions, creating additional safeguarding and welfare considerations; and

b. Victims are typically vulnerable children, often located internationally, who may not recognise themselves as victims and who can be reluctant to engage with law enforcement, due to intimidation and threats.

[36] 'Doxxing' is publishing online personal details of an individual who would otherwise wish to remain anonymous. 'Lorebooks' are manuals produced by Com members to share tradecraft and capture examples of harmful content in the quest for notoriety.

CSA Prevention

134. The NCA's CEOP Education programme seeks to reduce the vulnerability of children and young people to online sexual abuse by providing age-appropriate education, advice and support. The programme is delivered to three principal audiences: children and young people aged 4 to 18, professionals working with children and parents and carers.

135. The programme aims to:

a. Increase children's knowledge, skills and resilience online, helping them to recognise risks, stay safe and seek support when required;

b. Improve professionals' understanding of online CSA, enabling them to identify concerns and respond appropriately; and

c. Equip parents and carers with the knowledge and confidence to support their children online and access appropriate safeguarding resources where necessary.

136. Many of the harms addressed through the CEOP Education programme are also present within Com-related offending, including grooming, blackmail, coercion, image-based abuse and the exploitation of vulnerable children online. The programme therefore provides an established preventative framework which can be adapted to address emerging threats. Additional educational resources focused specifically on Com offending are currently being developed and are due to be released in Autumn 2026.

137. Through the CSA SGG[37], the NCA works with the Home Office, policing partners, the Lucy Faithful Foundation and other stakeholders to coordinate this preventative activity. This includes offender focused interventions, treatment programmes, deterrence initiatives and offender management approaches intended to reduce the risk of future offending

(ii) NCA NCCU – Cyber Prevent Framework and Cyber Choices Programme

138. Cyber Choices is a national programme coordinated by the NCA and delivered by Cyber Choices teams within ROCU and local police force cyber teams. It forms part of the National Cyber Prevent Framework 2022-2026, which is designed to reduce future cybercrime offending in the UK. I exhibit this framework as HR/22- **NCA000028** .

139. The programme seeks to educate and deter individuals, predominantly children and young people, from becoming involved in cyber crime by providing education, early intervention and diversion into legitimate opportunities. Cyber Choices has received

[37] See paragraph 33 for a definition and explanation of SGGs.

international recognition, with several overseas partner using it as a model when developing their own cyber prevention initiatives. The programme has also been presented at the White House Cyber Safety Review Board, where elements of its preventative approach have informed the development of cyber and prevention measures in the USA.

140. Cyber Choices is delivered through schools, policing and wider partnerships across the UK. It combines universal educational products aimed at large audiences with targeted interventions for individuals who may be at risk of engaging in cyber offending. The programme also utilises online communications, including social media and targeted advertising, to extend its reach and reinforce preventative messages.

141. The educational materials seek to increase awareness of:

a. The distinction between legal and illegal cyber activity;

b. The consequences of cyber offending for victims and offenders;

c. The real-world impact of online behavior;

d. Relevant legislation, including the Computer Misuse Act 1990; and

e. Legitimate pathways through which individuals can develop and apply cyber skills.

142. A key feature of the programme is its engagement with secondary audiences, including teachers, parents, carers and other professionals. By improving awareness of online risks and indicators of concerning behaviour, these audiences are better equipped to identify vulnerabilities, provide support and intervene and an early state. In the NCA's view, this preventative, partnership-based approach offers useful learning when considering how other forms of online enabled harm may be addressed.

<u>Operational strengths identified in Cyber Crime Investigations</u>

143. The NCCU's response to cyber crime combines specialist technical capabilities and strong partnerships across UK and international law enforcement, government, intelligence agencies and industry. These relationships support the exchange of intelligence, safeguarding information, victim reporting and operational data, enabling a more comprehensive understanding of the risk than would be available to any organisation acting alone. They also assist in identifying connections between individuals, online communities and online activity that may not otherwise be apparent.

Operational and Investigative Challenges in Cyber Crime Investigations

144. Cyber investigations continue to face significant challenges. T1D

T1D

T1D. Online communities present a particular challenge, as individuals with shared grievances, harmful interests or extremist beliefs can connect rapidly, operate anonymously and move between platforms and jurisdictions in response to moderation or enforcement activity. This can limit law enforcement visibility and make the assessment of intent, risk and escalation more difficult. As technology evolves, investigative methodologies and specialist capabilities must continually adapt in response.

145. The NCCU has also identified a gap where preventative interventions are unsuccessful. Unlike some other threat areas, there are currently limited civil measures available to manage individuals who present an ongoing cyber-related risk but have not yet entered the criminal justice system. As referred to in the statement of Timothy Wright[38], the NCA is engaging with the Home Office regarding the development of civil orders for cyber offending, drawing on approaches adopted in other crime types where such powers have assisted with the management of risk and the prevention of further offending.

(iii) NCA Prisoner and Lifetime Management Team

146. The NCA PALM Team acts as the primary interface between the NCA and HMPPS in relation to SOC offenders. Its functions include communicating risk information following remand or conviction, supporting prison-based risk management, providing operational assistance to investigations involving individuals in custody, quality assuring NCA applications for Serious Crime Prevention Orders ('SCPOs'), monitoring compliance with those orders following release, and contributing to MAPPA panels where appropriate.

147. PALM works closely with policing, probation and other partners to share intelligence and manage the risks posed by SOC offenders throughout their criminal justice journey. This includes monitoring compliance with court-imposed restrictions and identifying opportunities to disrupt further offending.

148. Responsibility for the management of registered sex offenders is with local police public protection and MOSOVO teams. This reflects the existence of established capabilities and governance arrangements, including MAPPA, through which the police,

[38] Statement of Timothy Wright dated 24 July 2026, paragraph 75.

probation and HMPPS jointly manage risk. The separation of responsibilities also helps avoid duplication and enables agencies to focus on their respective areas of expertise.

149. However, a number of cases (such as Owen Flowers, Thalha Jubair[39] and Matthew Falder[40]), have demonstrated an increasing overlap between SOC, cyber-enabled offending, online CSA and wider public protection concerns. In some instances, offenders may be subject to multiple forms of post-conviction management, requiring coordinated oversight between PALM, MOSOVO, HMPPS, Probation and Policing partners. These cases illustrate the importance of effective information sharing, clear ownership and collaborative risk management arrangements.

Challenges Identified by PALM

150. PALM's experience suggests that many of the principal challenges in offender management are organisational rather than technological. These include fragmented ownership of offenders across multiple agencies, differing organisational priorities, inconsistent operating procedures, the loss of intelligence through repeated handovers, and a lack of end-to-end management throughout the offender lifecycle. Collectively, these challenges can result in duplication of effort, gaps in accountability and uncertainty regarding ownership of risk.

Lessons and Recommendations

151. Drawing on its operational experience, PALM has identified a number of approaches which may strengthen multi-agency offender management:

a. Whole-life offender management through a model that maintains continuity of oversight and risk management throughout an offender's criminal justice journey;

b. Nationally agreed multi-agency operating procedures setting out clear responsibilities, ownership arrangements, intelligence sharing expectations and processes for managing offenders who are subject to multiple forms of supervision or court orders; and

c. A structured, pathfinder-style model incorporating continuous risk assessment, clear ownership, enhanced information sharing and coordinated management before, during and after custody.

[39] Two sentenced for hacking Transport for London in UK's biggest ever cyber crime case - National Crime Agency
[40] Dark web paedophile Matthew Falder's sentence reduced - BBC News

d. In the NCA's view, these lessons demonstrate the importance of clear accountability, effective information sharing and sustained multi-agency collaboration where responsibility for managing risk is shared across organisations.

Conclusion

152. The evidence set out in this statement reflects the NCA's experience of responding to the evolving threat posed by Com networks and other forms of online-enabled violence. Whilst the NCA does not have a primary role in the identification, assessment or management of VFIs, our operational experience demonstrates the increasing overlap between vulnerability, online communities, criminality and the risk of serious violence. It also highlights the importance of effective information sharing, early intervention, clear accountability and sustained multi-agency working when managing complex and emerging threats.

153. The NCA's assessment is that risks identified by the Inquiry are unlikely to be addressed through the creation of a narrowly defined VFI framework or by assigning responsibility to a single organisation. Rather, a whole-system approach is required, involving law enforcement, education, healthcare, social services, industry and wider government partners. Such an approach should focus on the identification and management of risk and harm, regardless of whether that risk is characterised as ideological, non-ideological, criminal or otherwise. The NCA will continue to support this work through its participation and contribution to the NIEV Taskforce by sharing its relevant operational activity, intelligence capabilities, experience of tackling Com networks and engagement with domestic and international partners.

Statement of Truth

I believe that the facts stated in this witness statement are true. I understand that proceedings may 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**

Helen Rance, Director Threat Leadership, NCA

Dated: 28th August 2026