Home Office

The Strategic Policing Requirement

February 2023

This publication is available at https://www.gov.uk/government/publications/strategic-policing-requirement

Any enquiries regarding this publication should be sent to us at: PSGHub@homeoffice.gov.uk (FAO: National Police Capabilities Unit)

Contents

Foreword from the Home Secretary

My mission as Home Secretary is clear: to deliver on the people's priorities, cut crime and provide the safer streets the public expect and deserve. The Strategic Policing Requirement (SPR) plays a crucial role in allowing me to set the direction against the biggest threats to public safety and ensuring the police have the capabilities to deliver an appropriately robust, national response ensuring common sense policing prevails.

The revised SPR provides, for the first time, strengthened detail around the action required from policing at the local and regional level to the critical national threats. It supports policing, both Chief Constables and PCCs, to plan, prepare and respond to these threats by clearly linking the local response to the national, highlighting the capabilities and partnerships that policing needs to ensure it can fulfil its national responsibilities.

Many of the threats will not be new to policing; we remain vigilant to the threat of international terrorism and dedicated in our commitment to disrupt criminals exploiting the vulnerable, including organised human traffic gangs that continue to facilitate the illegal routes via small boats and those exploiting vulnerable victims as part of county lines drug supply lines - there are an estimated 600 lines in operation across the country in any given month, associated with incidences of serious violence and knife crime.

I also want to ensure we deliver justice and high-quality outcomes for women and children who are victims of rape sexual offences and domestic abuse. I have therefore included VAWG as an additional national threat, as was recommended by HMICFRS in their 'Police response to Violence against Women and Girls (VAWG)' report (2021). The inclusion of VAWG will allow forces to maximise the capabilities required, including seizing the opportunities presented by Operation Soteria, to prevent and pursue VAWG offending. I have also substantially updated the 'Public Disorder' section as policing continues to prevent dangerous and highly disruptive tactics used by organised protesters that wreak havoc to the lives of the law-abiding majority and draw police officers away from their local communities. The Public Order Bill (published 11 May 2022) will allow our police officers to take pre-emptive measures to disruptive protests seen by the likes of Just Stop Oil. Furthermore, the new provision of specialist protest removal capabilities will help to prevent this nuisance.

New accountability and oversight arrangements mean that the public will now see a clear reference to the SPR in police and crime plans, including how it has shaped the strategic direction and objectives in forces and therefore how that force, contributes to tackling national priority threats.

I remain steadfast in my support of a ‘common sense policing’ approach and I am mindful that a lot of police work is not covered by the parameters of the SPR but remains vitally important. It is crucial that policing also continues to focus on neighbourhood crime and anti-social behaviour in their local communities, working closely with councils and other local partners who also have a role to play. I therefore fully support forces in their commitment to attend the scene of every residential burglary. A visible presence in local communities will help to retain the public’s confidence in policing, particularly whilst many are concerned about the rising cost of living.

Finally, I would like to thank those who have contributed to the revised SPR and all those on the frontline who respond to these threats on a daily basis to ensure public safety.

Introduction

1. The Strategic Policing Requirement (SPR) was last updated in 2015 in execution of the Home Secretary's statutory duty to set out what are, in her view, the national threats at the time the document is issued, and the appropriate national capabilities required to counter those threats.[1]

2. Whilst many threats can be tackled by individual police forces within their own force area, national threats can also require a coordinated or aggregated response in which resources need to be brought together from a number of police forces. Forces often need to work collaboratively, with other local partners and emergency services, within regional collaborations or with national agencies, to ensure the national threats are tackled efficiently and effectively.

3. This revised SPR contains seven national threats overall, reaffirming the validity of six national threats from the previous version, which are terrorism, serious and organised crime (SOC), a national cyber incident, child sexual abuse, public order and civil emergencies. It also includes Violence against Women and Girls, reflecting the threat it presents to public safety and confidence at the time of publication (see definition of a national threat below in paragraph 7).

SPR Review

4. Since the last review of the SPR in 2015, there have been important changes to the policing landscape. The National Policing Board (NPB) now has a role focussed on the strategic vision for policing and policing continues to face rapidly changing, often borderless threats. These changes presented an opportunity to review the SPR to ensure it remains current and fit for purpose and supports policing to tackle these threats. The Public Accounts Committee (PAC) came to a similar view in its report into serious and organised crime published in September 2019 when they recommended that the Home Office should review the SPR and consider the local needs and capabilities of forces.[2]

[1] This is in accordance with s37A Police Act 1996 as amended by s77 Police Reform and Social Responsibility Act 2011.

[2] https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/2049/2049.pdf

5. In reviewing the SPR, the Home Office consulted and obtained advice from policing partners and stakeholders to consider: the current national threats and whether they remained relevant; the required policing response and the necessary local and regional capabilities; and the appropriate governance arrangements that should be in place to ensure policing is held to account for its national contribution. This document reflects the consultation and work completed during that review.

6. The partners consulted included: Chief Constables; the National Police Chiefs Council (NPCC); the Association of Police and Crime Commissioners (APCC); Police and Crime Commissioners (PCCs) [3]; the College of Policing; National Police Coordination Centre (NPoCC); National Crime Agency (NCA); Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS); British Transport Police (BTP); as well as other government departments with an interest in the SPR such as the Cabinet Office and the Department for Levelling Up, Housing and Communities (DLUHC).

SPR Framework

7. A "national threat", as defined in s.37A of the Police Act 1996, is a threat (whether actual or prospective) which is:

   a. a threat to national security, public safety, public order or public confidence that is of such gravity as to be of national importance; or
   b. a threat which can be countered effectively or efficiently only by national policing capabilities to counter the threat.

8. In practice, this means that the SPR articulates the criminal and terrorist threats and other civil emergencies that require a cross-boundary policing response. This is either because the threat itself crosses force boundaries or because the response required to a local incident can exceed the capacity of a local force, and resources from other forces need to be deployed. It includes those that:

   a. align to the priority risks in the National Security Risk Assessment (NSRA);

[3] The term PCCs is used as shorthand to make reference to all Police and Crime Commissioners, all Combined Authority Mayors who exercise PCC functions, the Mayor's Office for Policing and Crime in relation to the Metropolitan Police district and the Common Council of the City of London in its capacity as police authority for the City of London Police area. Reference in this document to a Chief Constable is intended to apply to every Chief Constable in a Home Office force in England and Wales, the Commissioner of Police of the Metropolis, and the Commissioner of police for the City of London.

b. affect multiple or all police force areas and require local and/or regional resources from multiple police forces in order to counter the threat efficiently and effectively; and it includes those that;
c. may have seen a recent significant and widespread increase and/or impact on the public such that a cohesive and consistent local, regional and/or national response to counter it is required.

9. The 2020/21 consultation on the SPR concluded that the six threats – terrorism, SOC, a national cyber event, child sexual abuse, public disorder and civil emergencies – need to continue to be identified as national threats. However, as part of the review, some stakeholders cited drugs trafficking, specifically the county lines model, and fraud as threats that cross force boundaries that need to be addressed by policing. This iteration of the SPR includes the capabilities within the SOC threat response, required to tackle the harm to communities and individuals caused by drugs and fraud.

10. For each of the national threats, the SPR outlines what forces should be working towards, how the individual threats should be tackled by police forces, and who they should be working with. This detail is set out in the second part of this SPR. The SPR breaks down the response to each of the threats according to the following six pillars:

    a. **Outcomes**. This section outlines the strategic outcomes police forces should work towards when countering the national threats drawn, wherever possible, from publicly available government strategies such as the CONTEST strategy, the Tackling Child Sexual Abuse Strategy or the upcoming Fraud Strategy.

    b. **Capabilities.** This section identifies the capabilities (defined broadly as functions that the police deliver, formed from a combination of people, processes, IT, data, equipment and infrastructure) which should be in place, either within forces or as part of collaboration agreements, to counter each of the national threats and to drive outcomes. It specifies where capabilities are best located (e.g. at a regional or local tier) to avoid unnecessary and inefficient duplication of capabilities across the tiers of law enforcement. However, some of the capabilities required to respond to the national threats are not specific to one threat. The SPR also details specialist Cross-Cutting Capabilities (paragraph 144 onwards) that can be deployed to respond to at least three of the national threats.

c. **Capacity requirements**. This section outlines how capacity is assessed at force level to ensure there is the right level of resource available to meet demand and drive outcomes.

d. **Consistency and standards**. In some cases, there are specific requirements and standards to be met, or particular guidance that should be followed for specific capabilities and resources. Where national standards have been set, these are outlined here to ensure capabilities are delivered in a consistent way across England and Wales, facilitating interoperability between forces.

e. **Collaboration**. This section outlines how local forces should work with existing regional arrangements and national agencies to tackle the national threats that cross borders. These are not the only collaboration arrangements that can be formed within policing. Under the Police Reform and Social Responsibility Act 2011, chief officers and policing bodies have a duty to consider collaboration where it is in the interests of the efficiency and effectiveness of their own and other police force areas, and to keep these arrangements under review. Many forces already collaborate on services and the capabilities listed within the SPR. The Home Office encourages collaboration where that delivers the most efficient and effective outcomes for the public.

f. **Connectivity with partners**. This section outlines where police forces need to be well-connected with other local partners, for example with other blue-light emergency services or with the private sector, when responding to the national threats. It recognises that tackling these national threats requires a whole-system response and that police forces do not operate alone.

The Beating Crime Plan

11. The approach to exposing and ending hidden harms and building capability and capacity to deal with fraud and online crime are laid out in the Beating Crime Plan[4]. The Beating Crime Plan is the Government's strategy to cut crime, have fewer victims and protect the law abiding majority.

[4] Beating crime plan - GOV.UK (www.gov.uk)

12. As the Beating Crime Plan makes clear, evidence-based and targeted interventions such as the Safer Streets Fund, underpinned by common sense policing, lay at the heart of the Government's strategy to reduce crimes such as burglary and robbery. The Home Secretary has made clear to Chief Constables and PCCs they must get the basics right and improve forces' performance across the country, learning from best practice in tackling these invasive and unsettling crimes; further highlighted in the recent HMICFRS report[5] on the police response to burglary, robbery and other acquisitive crime. It is important Chief Constables and PCCs monitor emerging trends and have plans in place to deal with any new threats or increases in these crimes, especially given the move away from COVID-19 restrictions and lockdowns and the challenge of the current cost of living factors.

SPR Application

13. The SPR applies to Chief Constables and PCCs in Home Office forces in England and Wales and supports them to ensure their force fulfils its national responsibilities in tackling the national threats. The SPR:

    a. helps PCCs to plan effectively, in consultation with their Chief Constable, for policing challenges that go beyond their force boundaries;
    b. guides Chief Constables in the exercise of these functions; and
    c. enables and empowers PCCs to hold their Chief Constable to account for the delivery of these functions.

14. Whilst the SPR applies only to Home Office forces in England and Wales, many of the threats set out in the SPR affect all parts of the United Kingdom. Nothing in the SPR is intended to impact on the current arrangements for provision of mutual aid between police forces of the UK, including those outside of England and Wales.[6]

15. The SPR is available for adoption by non-Home Office police forces in England and Wales.[7] In order to meet interoperability challenges across the UK, other forces are

[5] Police response to burglary, robbery and theft must improve - HMICFRS (justiceinspectorates.gov.uk)

[6] As provided for in sections 24 and 98 of the Police Act 1996.

[7] The National Crime Agency (NCA), the British Transport Police (BTP), the Civil Nuclear Constabulary (CNC) and the MOD Police.

encouraged to have regard to the SPR's assessed threats insofar as they are applicable to their jurisdictions.

Assurance and Governance

16. The Home Secretary has a statutory duty to set out what are, in her view, the national threats at the time the document is issued, and the appropriate national policing capabilities required to counter those threats. This SPR also includes guidance relating to outcomes, capacity, national standards, collaboration and partnership working which will support policing to be more efficient and effective in their response to the national threats. The implementation of the SPR is the responsibility of Chief Constables and PCCs in England and Wales.

17. PCCs are required to have regard to this SPR when issuing or varying their police and crime plans. They must keep the police and crime plan under review in light of any changes made to the SPR by the Home Secretary. Chief Constables must have regard to both the police and crime plan and the SPR when exercising their functions. PCCs are responsible for holding them to account for doing so.[8]

18. It is not uncommon for legislation to require public bodies to "have regard to" guidance, codes of practice or other material. The expectation is that the PCC and Chief Constables should follow the SPR unless they are satisfied that, in the particular circumstances, there are good reasons not to.

Governance and Oversight

19. To ensure that the SPR has a meaningful place in the policing landscape and that it supports PCCs and Chief Constables to plan effectively for policing challenges that go beyond their force boundaries, it needs to be anchored in appropriate governance structures. Governance and oversight also ensures that the SPR is reviewed regularly by representatives from across the policing landscape, that it is embedded and followed by policing, and that the Home Office can identify changes that might be needed, for example to priority threats or capabilities, in future revisions of the SPR.

[8] The Common Council's statutory duty in relation to the SPR states they must have regard to the SPR when issuing their Policing Plan. The Common Council must also monitor the performance of the City of London Police in carrying out the Policing Plan.

20. The National Policing Board (NPB) governance ensures all parts of the policing system work together to deliver the best possible outcomes for the public.[9] The NPB, chaired by the Home Secretary, has two relevant sub boards, which are both chaired by the Policing Minister:

    a. the **Crime and Policing Performance Board** (CPPB) is the forum for scrutiny of performance against the National Crime and Policing Measures. It enables Ministers to set a framework for performance against which the relevant statutory bodies can collectively, and separately, hold the policing sector to account; and

    b. the **Strategic Change and Investment Board** (SCIB) provides oversight and scrutiny on a range of policing and law enforcement national investments that fund key capabilities, enabling the implementation of government priorities of crime prevention and reduction, and of public protection.

21. The Home Secretary has delegated annual consideration of the SPR to the SCIB whose membership is well-placed to discuss and assess the SPR. Annual SPR assurance reporting from PCCs (paragraph 24.1) will be sent to the Policing Minister as chair of the SCIB. This will inform annual discussion about the SPR and how it is being considered in setting the strategic direction and objectives for a force.

22. This assurance mechanism does not replace existing oversight processes for the threats and capabilities listed within the SPR. For example, Counter-Terrorism Policing continues to be co-ordinated and funded nationally through the Counter-Terrorism Policing Headquarters and is subject to separate ministerial oversight.

Assurance and accountability

23. Embedding the SPR within the policing landscape and ensuring it has a meaningful role in connecting the local to the national is an essential element of the SPR's assurance mechanisms. The review mechanisms that exist provide assurance that the SPR is being appropriately considered and that the "have regard to" duty is being complied with. These review mechanisms are set out below:

    23.1 HMICFRS independently inspects and reports on the efficiency, effectiveness and legitimacy of individual forces' performance through its PEEL programme and, on

[9] https://www.gov.uk/government/groups/national-policing-board

key aspects of policing through its programme of thematic inspections. Previously, HMICFRS has assessed how well forces have delivered against specific elements of the SPR in its PEEL inspections (most recently 2018/19). However, force compliance with the revised SPR will, in future, be looked at thematically. We will engage with HMICFRS on this as it develops its inspection programmes.

23.2 PCCs must hold Chief Constables to account for having, or having access to, the capabilities that have been identified in this document as critical to the planning of an effective and proportionate response to the national threats. PCCs are also required to have regard to the SPR themselves (paragraph 17) and there are now strengthened and clearer arrangements around how PCCs factor in the SPR when issuing or varying their police and crime plans.

23.3 PCCs have the legal power and duty to set the strategic direction and objectives of the force through their police and crime plan which must have regard to the SPR. PCCs also have the legal power and duty to decide the budget, allocating assets and funds to the Chief Constable. Guidance will be provided by the APCC, to support PCCs to detail how they have had regard to the SPR in their police and crime plan. In practice, this will cover:

a. the need to highlight the PCC's duty to have regard to the SPR in the police and crime plans;
b. an explanation of what the SPR is in the police and crime plans; and
c. an explanation within the police and crime plans of how the PCC has had regard to the SPR in setting the strategic direction and objectives for the force.

24. As the SPR is a document issued by the Home Secretary, an assurance mechanism is needed between the Home Office and PCCs. This will consist of two elements:

24.1 PCCs will provide an annual assurance statement within their annual reports on how they have had regard to the SPR and how it has influenced their setting strategic direction and objectives for their force. Guidance will be provided to support PCCs in the drafting of these statements.

24.2 The APCC will provide an annual summary of the assurance statements to the Policing Minister. This will inform an annual discussion at the SCIB.

25. Provisions in the Police Act 1996 require that the Home Secretary must, from “time-to-time”, issue a SPR and, in so doing, obtain the advice of such persons as appear to the Home Secretary to represent the views of chief officers of police and local policing bodies (paragraph 5). The SPR review concluded that the SPR needed to be reviewed and issued more frequently as those consulted felt the time elapsing from the last revision in 2015 had been too long. The Home Office has committed to revisiting the SPR again within two years of publication to ensure it remains in step with any key changes or shifting threats and priorities in the policing landscape. The SPR will also be reviewed at least every two years thereafter to ensure that it remains current.

The Policing Response

Violence Against Women and Girls

The term violence against women and girls refers to acts of violence or abuse that disproportionately affect women and girls. Crimes and behaviour covered by this term include rape and other sexual offences, domestic abuse, stalking, 'honour'-based abuse (including female genital mutilation, forced marriage, and 'honour' killings), as well as many others, including offences committed online. While the term 'violence against women and girls' is used this refers to all victims of any of these offences.[10]

Introduction

26. The Government published a Strategy to tackle Violence Against Women and Girls (VAWG) in July 2021, and a complementary Tackling Domestic Abuse Plan in March 2022[11]. The Strategy and Plan set out actions the Government is taking to make the safety of women and girls across the country a priority. They are themed around preventing these crimes, improving the experiences of victims and survivors, ensuring perpetrators are brought to justice, and improving the way different organisations, including statutory agencies, work together to tackle VAWG.

27. The HMICFRS inspection on the police response to VAWG stated there was a need for immediate cross-system action to respond with "greater pace and urgency to what HMICFRS consider to be an epidemic of offending against women and girls". The report outlined 15 recommendations to strengthen multi-agency working; ensure accountability; improve capability and understanding; and ensure better support for victims. The subsequent final report, published in September 2021, expanded on this and provides 20 recommendations across the following five overarching recommendations:

[10] Tackling violence against women and girls strategy (publishing.service.gov.uk), pg.8.

[11] Tackling Domestic Abuse Plan - GOV.UK (www.gov.uk)

- There should be an immediate and unequivocal commitment that the response to VAWG offences is an absolute priority for government, policing, the criminal justice system, and public sector partnerships.
- The relentless pursuit and disruption of adult perpetrators should be a national priority for the police, and their capability and capacity to do this should be enhanced.
- Structures and funding should be put in place to make sure victims receive tailored and consistent support.
- All chief constables should immediately review and ensure that there are consistently high standards in their forces' responses to violence against women and girls and should be supported in doing so by national standards and data.
- There should be an immediate review of use of outcomes 15 and 16 in violence against women and girls offences.

28. The Government, NPCC and College of Policing supported all the inspectorate's recommendations, including the recommendation for a new, full-time, National Policing Lead on VAWG and are funding this post.

29. In addition, a significant amount of work is being taken forward by the Government and policing following publication of the College of Policing and NPCC's "Policing violence against women and girls – National framework for delivery: Year 1[12]" and the "one year on" progress report published September 2022.[13]

Outcomes

30. The College of Policing and NPCC's framework for delivery outlines policing's ambition to bring about demonstrable and sustained difference in police attitudes and practice in responding to VAWG, through three overarching objectives:

    a. improving trust and confidence in policing;
    b. relentlessly pursuing perpetrators; and
    c. creating safer spaces.

[12] College of Policing and NPCC publication dated December 2021: Policing violence against women and girls - National framework for delivery: Year 1 (npcc.police.uk)

[13] College of Policing and NPCC publication dated September 2022: Policing violence against women and girls - one year on: Progress Report (npcc.police.uk)

31. The framework for delivery is for police forces to use and every police force is expected to have developed local action plans setting out their activity against the framework.

32. When responding to VAWG, all police forces are expected to follow the relevant Authorised Professional Practice (APP) set out by the College of Policing and can be found on the College of Policing website[14]. The capabilities section below provides a summary of the specialist capability particularly relevant to VAWG (and aligned to the APP). Whilst there is a huge amount of work underway to strengthen the VAWG response, the capabilities listed should be understood as the minimum requirement for police forces to have in place. The capabilities set out within the CSA section of this document (paragraph 106 onwards) are also relevant.

33. Recognising that the welfare of police officers and staff is important, in accordance with the duty of care placed on chief officers[15], all forces must have in place risk assessments, policies and procedures to ensure that the duty to consider the safety and welfare of staff is fulfilled as well as resilience built and the risk of desensitisation reduced. All police forces have access to and should utilise support and advice offered by the National Police Wellbeing Service (NPWS), Oscar Kilo[16], or have alternative wellbeing service provision as least as comprehensive.

Capabilities

Trained officers and staff

34. Forces should maintain the capability to respond to all VAWG criminal offences including by having appropriately trained officers and staff.[17] Alongside any other

[14] College of Policing APP

[15] Chief Constables hold a statutory responsibility in the Police (Health and Safety) Act 1997, to manage the welfare of their officers and staff, and it remains the role of elected Police and Crime Commissioners to ensure they are held to account.

[16] About Oscar Kilo - The National Police Wellbeing Service • Oscar Kilo

[17] Forces have discretion in how they allocate and deploy officers working on VAWG, and practice varies between forces. However, for domestic abuse forces should have, as a minimum, a body of specialist officers familiar with the dynamics of domestic abuse and with local knowledge of repeat victims and serial perpetrators, who can be called on to support first responders and other primary investigators. They should also have specialist supervisors who have an overview of domestic abuse within their force area. See: The role of domestic abuse specialists (college.police.uk)

appropriate action, and in the context of local priorities, officers and staff should be able to assess the extent to which they need to:

a. conduct complex and multi-faceted investigations to identify perpetrators, promptly collect all available evidence and take into consideration the wider pattern of behaviour, its context and when an individual incident forms part of a wider pattern of behaviour, and its cumulative impact;

b. access digital forensics specialists (see Cross-Cutting Capabilities, paragraphs 144 to 175) to obtain, analyse and use digital evidence in investigations or criminal proceedings;

c. make use of the existing legislative framework, including considering the use of preventative civil orders (including interim orders), to protect victims and intervene early[18] . This includes considering whether any of the following may be appropriate: protective orders such as sexual risk orders, sexual harm prevention orders, domestic violence protection notices, domestic violence protection orders, stalking protection orders, female genital mutilation protection orders, forced marriage protection orders, and whether and how the domestic violence disclosure scheme, also known as “Clare’s Law”, might be applied;

d. investigate breaches of civil orders, making full use of the range of tools available, to manage risk and to minimise harm;

e. monitor and manage registered sex offenders and other relevant offenders[19] for example by compiling intelligence reports about modus operandi, patterns of offending and other behaviour and associations of the offender, ensuring information is shared across agencies as appropriate, and investigating any breaches of notification requirements, using the appropriate multi-agency public protection arrangements (MAPPA) level and in line with the MAPPA guidance;[20]

[18] The suitability of a particular order depends on the nature of the risk posed by the individual offender and the circumstances involved. See: Court orders and notices (college.police.uk).

[19] Guidance on Part 2 of the Sexual Offences Act 2003 - GOV.UK (www.gov.uk); Managing sexual offenders and violent offenders (college.police.uk). The way forces configure and staff their functions relating to the management of sex offenders and violent offenders varies

[20] Multi-agency public protection arrangements (MAPPA): Guidance - GOV.UK (www.gov.uk)

f. gather, assess and record as much available evidence as possible on sexual offending in their force area, to build a detailed intelligence picture;

g. work with partners to identify the extent and nature of the practice of 'honour'-based abuse within their force area;

h. initiate safety planning and safeguarding arrangements in domestic abuse cases;

i. collaborate with neighbourhood policing teams, or the local equivalent, in managing VAWG and consider the use of police watch schemes to provide a visible police presence;

j. be aware of particularly vulnerable victims and higher risk perpetrators in their area (particularly relevant for local policing teams, including response and neighbourhood officers);

k. access and make use of materials relating to the investigation of rape and sexual offences available on the Knowledge Hub to ensure the force's approach is informed by best practice;

l. provide a single point of contact for victims, taking a sensitive approach, to keep them informed of decisions and of their rights, in line with the Code of Practice for Victims of Crime in England and Wales[21];

m. access and make use of the College of Policing resource[22] of supportive learning materials to help address vulnerability, violence and abuse and to manage the risk posed by perpetrators across the full range of VAWG offences.

Connectivity with partners

35. To ensure an effective, whole-system response to all types of VAWG, Chief Constables should ensure their force is working with all relevant partners to protect women and girls from harm. This includes having regard to relevant multi-agency guidance as appropriate, and joint working. For example, the VAWG National

[21] The Code of Practice for Victims of Crime in England and Wales and supporting public information materials - GOV.UK (www.gov.uk)

[22] Violence against women: Resources for policing | College of Policing

Statement of Expectations[23], the guidance for forced marriage[24] and the Police-CPS Joint National Rape and Serious Sexual Offences (RASSO) Action Plan 2021[25] which sets out how the police and the CPS will work together to improve the joint response to these crimes over the next three years. While policing is reserved in Wales, the Violence Against Women, Domestic Abuse and Sexual Violence (VAWDASV) Strategy[26], which sets the agenda for the Welsh Government and the agencies it directs and funds, may also be relevant. We have published domestic abuse statutory guidance to support organisations with understanding the legal definition of domestic abuse and inform the response to domestic abuse[27]. This collaboration will help to ensure that policing is contributing to building a stronger whole-system approach, which is needed to effectively tackle VAWG. Forces should:

a. collaborate effectively with the Crown Prosecution Service (CPS), including in seeking early advice, conducting evidence-led investigations and ensuring scrutiny of cases where 'no further action' decisions are taken;

b. share information and intelligence with agencies and other forces to detect and identify risk and individuals of concern. For example, forces should share information on the highest-risk domestic abuse cases with partners in multi-agency risk assessment conferences (MARAC)[28] to outline risk and identify options to support the development of a coordinated action plan to improve the safety of the victim;

c. collaborate with Independent Domestic Violence Advisers (IDVAs) to assess the level of risk and to develop safety plans to ensure the protection of victims of domestic abuse;

---

[23] Commissioning services to tackle violence against women and girls - GOV.UK (www.gov.uk)

[24] Multi-agency statutory guidance for dealing with forced marriage and multi-agency practice guidelines handling cases of forced marriage

[25] Police-CPS Joint National RASSO (Rape and Serious Sexual Offences) Action Plan 2021 | The Crown Prosecution Service

[26] https://www.gov.wales/violence-against-women-domestic-abuse-and-sexual-violence-strategy-2022-2026-html

[27] Domestic Abuse Statutory Guidance (publishing.service.gov.uk)

[28] A MARAC is a meeting where information on the highest-risk domestic abuse cases is shared between representatives of local police, probation services, health, child protection, housing practitioners, IDVAs and other specialists from the statutory and voluntary sectors. See: Toolkit for police officers on the MARAC process (savelives.org.uk)

d. collaborate with Independent Sexual Violence Advisers (ISVAs) in their work to ensure support and the safety of the victim is coordinated across all agencies and essential services. This should include collaboration on the creation of communications plans for engagement with victims of rape and sexual offences.

Terrorism

Terrorism is the use of, or threat of, action that inflicts serious violence against a person, serious damage to property, endangers a person's life (other than the person committing the action), creates a serious risk to the health or safety of the public, and/or is designed to seriously interfere with or disrupt an electronic system where that use of threat is designed to influence the government or an international governmental organisation, or to intimidate the public or a section of the public and is made for the purpose of advancing a political, ideological, racial or religious cause. This action could include, but is not limited to, activity carried out using explosives, firearms, vehicles as a weapon, low sophistication devices (such as bladed weapons), and chemical, biological, radiological and nuclear (CBRN) weapons by international and domestic groups or individuals.

Outcomes

36. Police forces have a substantial and critical role to play in the national counter-terrorism response. CONTEST is the framework that organises the work to counter all forms of terrorism.[29] It aims to reduce the risk from terrorism to the UK, its citizens and its interests overseas. CONTEST remains an ideologically agnostic strategy, agile enough to adapt to all forms of terrorism. Islamist terrorism remains the greatest volume of threat, accounting for three quarters of MI5 and CT Policing's casework. The threat from terrorism is enduring and evolving. Since the start of 2017, MI5 and the police together disrupted 37 late-stage attack plots.

37. Police forces should be able to demonstrate that they can respond to terrorist threats in accordance with CONTEST, working in support of Counter-Terrorism Policing and with partners to deliver that response within the following four workstreams:

- **Pursue:** to stop terrorist attacks happening in the UK and overseas. This means using a range of tools to disrupt those who wish to engage in terrorism-related activity and to counter the threat from people travelling for terrorism-related purposes.

[29] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf

- **Prevent:** to stop people becoming terrorists or supporting terrorism. Through Prevent, vulnerable individuals who are at risk of radicalisation can be safeguarded and supported, whilst also enabling those already engaged in terrorism to disengage and rehabilitate.

- **Protect**: to strengthen protection against a terrorist attack in the UK.

- **Prepare**: to mitigate the impact of a terrorist incident if it occurs. This includes working to bring a terrorist attack to an end and to increase resilience to recover from its aftermath.

38. While Counter Terrorism policy is non-devolved, much of it is delivered through devolved areas and functions, particularly in relation to local authorities and Community Safety Partnerships. Welsh CONTEST structures therefore reflect the role of Welsh Government who have devolved authority in Wales with strategic oversight via CONTEST Cymru jointly Chaired by Welsh Government and Welsh police.

Capabilities

39. Much of the police contribution to counter-terrorism takes place through the Counter-Terrorism Policing network. Police counter-terrorism work counters the full spectrum of types of terrorism, state threats and espionage, delivers counter-proliferation, investigates breaches of the Official Secrets Act and investigates War Crimes. The work of Counter-Terrorism Policing reflects a close collaboration with a wide range of partners, including the UK intelligence community, the private sector, local and international partners as well as the local community (see “Connectivity with partners” below, paragraph 51).

40. Counter-Terrorism Policing is the primary means for disrupting terrorist-related activity in the UK and it leads the police contribution to CONTEST across Prevent, Pursue, Protect, and Prepare. It consists of a network of operational units based regionally across the UK, delivering specialist counter-terrorism capabilities and threat-agnostic capabilities on behalf of forces. These capabilities include:

40.1. collecting and developing intelligence, working jointly with MI5 to run counter-terrorism investigations and disrupt terrorist activity through arrests and, in collaboration with the Crown Prosecution Service (CPS), prosecutions (Pursue);

40.2. making use of all tools and powers available to disrupt those engaged in terrorism-related activity and constrain their ability to carry out acts of terrorism, including the daily management of subjects subjected to measures under the Terrorism Prevention and Investigation Measures (TPIM) Act (Pursue);

40.3. working with local forces and partners to identify and safeguard individuals and communities vulnerable to radicalisation, supporting them in delivering their statutory duty under Prevent. This includes applying skills and powers to assess, manage and disrupt individuals who pose a risk of radicalisation and identifying online harms, working with social media companies to remove radicalising material from the internet. This includes disrupting those who seek to radicalise (Prevent);

40.4. delivering guidance, advice, training and security for the public, places, and protection for Royalty and VIPs. The National Counter-Terrorism Security Office (NaCTSO) is responsible for developing specific guidance, training products and communications, and supporting Counter Terrorism Security Advisers (CTSAs) who deliver security advice, guidance, training and other support to organisations, sectors, and sites in the private and public sector. Counter-Terrorism Borders Policing also identify individuals of interest as they travel, both inbound and outbound, through ports (Protect);

40.5. provision of Counter-Terrorist Specialist Firearms Officers (see Armed Policing in the Cross-Cutting Capabilities section, paragraphs 148 to 149) and guidance for all police responders to marauding terrorist attacks (MTAs) (Prepare);

40.6. provision of Chemical, Biological, Radiological and Nuclear (CBRN) guidance, advice, and equipment (Prepare); and

40.7. conducting and supporting counter-terrorism exercising across the network to drive operational development through embedded organisational learning. Counter-Terrorism Policing works with all forces to ensure their planning for local delivery of specific wider operations relevant to counter-terrorism are regularly reviewed and maintained. To embed and develop further organisational learning Counter-Terrorism Policing undertake an annual portfolio of counter-terrorism exercising, testing and training (Prepare).

41. Whilst Counter-Terrorism Policing is the primary means for disrupting terrorist threats, locally-maintained capabilities also have an important role to play in counter-terrorism. Chief Constables should be assured that their force:

41.1. maintains relevant Pursue capabilities including:

a. the ability to collect and analyse terrorist communications and their use of digital media in order to detect, prevent and investigate threats;

41.2. maintains Prevent capabilities including:

a. the ability to gather and assess all received Prevent referrals to determine if there is a counter-terrorism vulnerability, and then appropriately progressing cases to the correct support (e.g. Channel panel, Police-led partnerships etc.); and
b. Prevent lead to support the delivery of Channel, including inputting pertinent information into the Case Management Information System (CMIS) used to case manage and support individuals at risk of being drawn into terrorism

41.3. maintains relevant Protect capabilities including:

a. Security Co-ordinators (SecCOs) who are trained to provide advice on all aspects of operation security for any event, and for active planning, co-ordination and initiation of counter-measures to deliver it safely and effectively. SecCOs can also draw on specialist search teams and firearms support;
b. Designing Out Crime Officers (DOCO) who provide advice, guidance and assessments to local authorities and organisations on measures to reduce crime. They should promote general crime reduction measures which benefit counter-terrorism and work in close partnership with regional CTSAs to engage relevant businesses and organisations. They can also provide support in cases where new builds or refurbishments of private and public buildings would benefit from protective security advice;
c. Project SERVATOR officers, where trained and deployed, who are tasked to conduct highly-visible and unpredictable deployments. They use a range of tactics to disrupt criminal activity, including but not limited to terrorism, whilst providing a reassuring presence for the public;

d. access to Explosives Detection Dogs, either within force or via collaboration, to detect the terrorist and criminal misuse of explosives at iconic sites and local and national events;[30] and
e. routine patrol capabilities to provide intelligence, deterrence and detection capability for counter-terrorism purposes, and other threats or criminal activity.

41.4. maintains relevant Prepare capabilities including:

a. regularly exercised plans for counter-terrorism operations. Category 1 responders, under the Civil Contingencies Act 2004, have a duty to create and maintain appropriate response plans and exercise those plans (see Civil Emergencies section under “Outcomes” heading);
b. armed policing capabilities in the form of immediately deployable Armed Response Vehicles (ARVs) (see paragraphs 151 and 152), meeting national capability and resource standards; and
c. Chemical, Biological, Radiological, and Nuclear (CBRN) capability to respond to CBRN incidents, including major incident response and consequence management.

42. Force-level Special Branches are a critical part of the policing response to national security threats. In some regions, services previously provided by force-led Special Branch Teams had been fully integrated into regional Counter-Terrorism Policing operating structures. In other regions, Special Branch teams were being managed regionally or locally, working closely with the regional Counter-Terrorism Policing Unit. In April 2022, funding for Special Branch functions was transferred out of the Police Main Grant to the Counter-Terrorism Policing Grant. This will help to protect local counter-terrorism assets while providing forces with greater access to specialist expertise and resources when they need them, as well as driving efficiency, consistency and improved effectiveness.

43. Special Branches provide capabilities to:

a. manage intelligence and operations, including handling covert human intelligence sources (CHIS);

[30] Additional explosives capabilities, such as Explosives Ordnance Disposal (EOD), are delivered by military EODs in England and Wales, except in London where the capability is delivered by SO15 counter-terrorism command within the Metropolitan Police Service.

b. lead local-level investigations and provide support to regional-level and national-level investigations; and
c. deliver a safeguarding role to support local efforts to prevent individuals becoming involved in terrorism and extremism.

Capacity requirements

44. The threat to the UK from terrorism is assessed by the Joint Terrorism Analysis Centre (JTAC) who analyse and assess all intelligence relating to international terrorism, at home or overseas. Threats are also highlighted through the National Security Risk Assessment (NSRA) which is used to help inform prioritisation and preparedness for civil emergencies.

45. The consequences of emergencies and their maximum plausible scale, duration and magnitude are defined in National Resilience Planning Assumptions (NRPAs). These assumptions inform the work of the cross-government National Resilience Capabilities Programme which coordinates work to build and maintain capability to respond to the common consequences of emergencies.

46. Based on JTAC threat assessments, the NSRA and NRPAs, Chief Constables, together with the appropriate NPCC threat lead, are required to consider national, regional and local threats and risks in determining their local capability and capacity to mitigate those threats and risks. Chief Constables should also consider how their force, when required, will contribute capabilities in support of a national policing response.

Consistency and standards

47. The National Police Chiefs' Council Counter Terrorism Coordination Committee (CTCC) sets common standards to ensure that processes and equipment are fit for purpose and interoperable across the UK. Chief Constables should ensure that:

    a. their force follows College of Policing authorised professional practice (APP) in relation to operations, incident response, armed policing, crisis management, investigations, forensics, and prosecutions to ensure that they meet national standards in these areas;[31] and

[31] https://www.app.college.police.uk/

b. all frontline officers and staff have been trained and have access to resources which assist them to identify when a Prevent referral should be made to embed and drive consistency.

Collaboration

48. The CTCC provides strategic oversight of the operational delivery of national Counter-Terrorism Policing, including the Counter-Terrorism Policing Network. This comprises of regional Counter-Terrorism Units (CTU) and Counter-Terrorism Intelligence Units (CTIU) established across England and Wales. These units also work in collaboration with their counterparts in Scotland and Northern Ireland to:

a. ensure a consistent policing response in line with the current assessed threat and risk;
b. deliver command and control to counter-terrorism led investigations;
c. work in close partnership with the Security Service who lead counter-terrorism intelligence and assessment; and
d. deliver effective and efficient management of counter-terrorism assets and resources in all police force areas.

49. This collaboration facilitates join-up across the law enforcement counter-terrorism response and enables a flexible and efficient response to threats, ensuring that all who need them have access to specialist capabilities.

50. Chief Constables should be assured that their force is working effectively with:

50.1. their regional CTU or CTIU to share intelligence and access specialist capabilities for investigations and intelligence-gathering, including skilled detectives, analysts, forensic specialists, and high-tech investigators; and

50.2. the Senior National Coordinator for Pursue and Prevent and the Senior National Coordinator for Protect and Prepare to ensure the most efficient use of local, regional and national assets and resources in responding to terrorist activity.

Connectivity with partners

51. The CONTEST approach unites the public and private sectors, communities, citizens and overseas partners to counter all forms of terrorism. Police forces are key in facilitating this multi-agency response. Chief Constables should ensure that their force:

51.1. supports Pursue by:

a. working closely with partners to detect, investigate and disrupt terrorist activity, including the effective sharing of information to enrich the understanding of the terrorist threat at a local level;

51.2. supports Prevent activity by:

a. developing local partnerships with community organisations to deliver projects to protect individuals from radicalisation;
b. working closely with their local authority and other multi-agency partners to assess the risk of people being drawn into terrorism, providing, where appropriate, details of the police counter-terrorism local profile (CTLP);
c. supporting local authority Prevent coordinators in developing Prevent-related projects to help build community resilience; and
d. supporting opportunities to develop community challenges to extremists;

51.3. supports Protect and Prepare by:

a. disseminating information, advice and guidance on the terrorist threat, methodologies and mitigations to stakeholders who are responsible for publicly accessible locations to allow them to consider protective security and asset deployment;
b. following the Joint Emergency Services Interoperability Principles (JESIP) to enable effective joint working between police forces and with other emergency services (see Cross Cutting Capabilities section). Tactical and operational commanders should be trained and refreshed in working with the JESIP principles.
c. agreeing Ministry of Defence (MoD) support in extremis to some policing roles.

Serious and Organised Crime

Serious and organised crime (SOC) is defined as individuals planning, coordinating, and committing serious offences, whether individually or in groups and/ or as part of transnational networks. The main categories of SOC are: child sexual abuse, modern slavery and human trafficking and organised immigration crime **(vulnerabilities)**; illegal drugs (including supply methodologies such as county lines), illegal firearms; and organised acquisitive crime **(communities)**; and cybercrime, fraud, money laundering, bribery and corruption, and sanctions evasion **(economic).**[32]

Drugs

52. Drugs are a significant driver of crime, cause harm to our communities and contribute to approximately half of all homicides and acquisitive crime. Assessment by the National Crime Agency suggests that 48% of organised crime groups are believed to be involved in drugs criminality[33]. The critical role policing has in tackling drugs supply and county lines is outlined in the 10-year Drugs Strategy (*'From Harm to Hope'*)[34]. The Strategy sets out the requirement to target drug supply across every stage of the supply chain and at every tier of policing. Police forces are key to breaking the supply chain and delivering our commitment to reduce drug-related crime and homicide and have a valuable contribution to make in relation to all three priorities of the drugs strategy: reducing supply, reducing demand, and enhancing treatment and recovery. Chief Constables and PCCs should be aware of their role in supporting local delivery against the Combating Drugs Outcomes Framework and working in partnership in line with the Drugs Strategy Guidance for Local Delivery Partners[35] .

Fraud

53. Fraud is the most common crime type accounting for 41% of all criminal offences in England and Wales and this proportion is increasing. As banks have developed better automated systems to detect fraud, fraudsters have become increasingly adept at

[32] The main categories are taken from the NCA's, National Strategic Assessment 2021. file (nationalcrimeagency.gov.uk)

[33] NCA National Strategic Assessment of Serious and Organised Crime (NSA) (2022)

[34] From harm to hope: A 10-year drugs plan to cut crime and save lives - GOV.UK (www.gov.uk)

[35] Drugs strategy guidance for local delivery partners - GOV.UK (www.gov.uk)

manipulating or duping victims into transferring money to them. Fraud causes financial harm to the economy and the public, costing individuals £4.7b a year in 2015/16 (The Economic and Social Costs of Crime 2018) and causes emotional harm to the public with three-quarters of victims suffering from some form of emotional impact (Crime Survey of England and Wales YE March 2020). Fraud also undermines national security by impacting public confidence in the criminal justice system, the stability of businesses and the UK's financial reputation. Money obtained fraudulently often flows into organised crime, terrorism and human trafficking with two-thirds of organised crime groups focussed on frauds being involved in other criminal activities.

54. We are taking a broad approach to tackling fraud, working across government and partners in the multi-agency National Economic Crime Centre (NECC), including law enforcement, regulators, UK intelligence agencies, industry partners and charities. The new Fraud Strategy will shortly set out how we will work together, and highlight the priority given to tackling fraud by the government. It should further invigorate the work of the operational system, which is already stepping up its response by acting on the recommendations of the National Strategic Tasking Coordination Group (NSTCG) following the voluntary tasking of forces by the Director General of the NCA, first issued on 19 December 2019. The tasking originally asked partners to support work in key areas including improved visibility and coordination of operational activity. Policing has an important role to play, and we are investing in an improved response, including additional intelligence and investigative posts in the NCA, City of London Police (CoLP), and ROCUs, replacing the Action Fraud Reporting system for fraud and cybercrime and rolling out the National Economic Crime Victim Care Unit. This will enable a much greater focus on proactive, intelligence led disruptive activity at all levels to reduce the harm from fraud as early as possible, and by creating capacity at a national level to provide intelligence packages to ROCUs and forces in addition to supporting disseminations from the National Fraud Intelligence Bureau (NFIB). This is a deliberate shift from the primarily reactive stance in policing to date.

Organised Immigration Crime (OIC)

55. Organised immigration crime (OIC) is a visible and growing threat, with organised networks profiteering from undermining the UK's border security, often exploiting vulnerable people, and increasingly risking their lives in dangerous routes to the UK. The OIC threat continues to increase, with all modes of entry higher than in 2018 and

record numbers of small boat entries year-on-year. We cannot continue to make incremental change and expect this trend to reverse, but instead need law enforcement resources to be reprioritised to bring appropriate focus on OIC. All Forces should therefore implement the objectives of the 2021 (revised January 2023) Crime and Courts Act tasking issued by DG NCA. Alongside the NCA, Immigration Enforcement, Border Force and other partners, Policing will be a key contributor to our efforts to disrupt this pernicious crime and to raise wider awareness, making this type of crime more difficult.

Outcomes

56. The most visible elements of crime are often felt in local neighbourhoods: personal losses to fraud from friends and family, a stolen car, gang violence, or drug dealing. These crimes are driven by a complex web of global, organised criminal business whose primary motivation is profit. Tackling SOC is therefore crucial to delivering on the three key areas of the Beating Crime Plan:

- Cutting homicide, serious violence and neighbourhood crime
- Exposing and ending hidden harms and prosecuting perpetrators
- Building capability and capacity to deal with fraud and online crime

57. SOC also threatens our national security – it directly undermines the safety of UK citizens, the integrity of the state and confidence in our financial system. The Integrated Review of Security, Defence, Development and Foreign Policy[36] sets out the government's priority actions for tackling SOC and Economic Crime, including strengthening our local and regional policing response.

58. The NCA is responsible for leading the law enforcement system response to SOC. This includes coordination and tasking as well as gathering, analysing and disseminating a national intelligence picture. Police forces and Regional Organised Crime Units (ROCUs) – collaboration arrangements between forces that deliver specialist policing capabilities – work closely with the NCA and other law enforcement partners including Immigration Enforcement and Border Force, and play a vital role in

[36] https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

tackling SOC and reducing the threat. The ROCU network mission is to protect communities by disrupting organised crime groups, individual criminals and those who enable them. Working alongside partners the ROCU network is responsible for enabling an integrated policing response, coordinating key policing capabilities needed to achieve this. Police forces deal with the majority of SOC demand within the law enforcement system. They must also work effectively with partners including local authorities as well the voluntary and charity sector to take action to prevent the devastating and long-term harm SOC can cause to individuals and communities.

59. A new dedicated NPCC SOC policing lead, working in partnership with the Director General of the NCA, will provide national oversight of the policing response to SOC and support the continued development of force and ROCU capabilities.

60. PCCs and Chief Constables should ensure their force and ROCU contributes to tackling SOC. The '4P' delivery framework continues to provide a coherent approach for all partners. The four strands are:
    - **Pursue** offenders through prosecution and disruption;
    - **Prepare** for when serious and organised crime occurs and mitigate impact;
    - **Protect** individuals, organisations and systems from the effects of serious and organised crime;
    - **Prevent** people from engaging in serious and organised crime

61. In practice, this should be achieved by:
    a. making good use of all available intelligence to identify, understand and prioritise SOC and inform decision-making[37];
    b. having the right systems, processes, people and skills to tackle SOC and keep the public safe;
    c. ensuring disruptive activity reduces the threat from SOC;
    d. preventing people from engaging or re-engaging in SOC, including safeguarding individuals who are being criminally, economically, or sexually exploited; and
    e. ensuring individuals, communities and organisations are resistant and resilient to the impact from SOC.

[37] As determined by the SOC System Tasking's agreed prioritisation mechanism.

Capabilities

62. The nature and scale of the SOC threat that forces need to respond to will be different in each force area. However, each force should have core capability components to tackle SOC and keep the public safe. These are set out in paragraph 75 onwards.

63. The capabilities to respond to drugs supply, fraud and organised immigration crime have been explicitly highlighted as important in this section below. Drugs supply is one of the primary threats driving police force effort and given concerns about the potential impact of increased cost of living on both drug supply and demand, it is crucial that activity to tackle this threat continues. Fraud continues to rise, is often facilitated online and regularly has international links, it is expected to see further increases during a period of economic uncertainty and high cost of living. The capability for forces to be able to respond adequately to this threat is paramount to tackle the threat.

64. Following publication of this document, a fraud supplement will be produced providing greater detail on what is expected regarding the response to fraud. Finally, a focus on the cross-cutting threat emanating from Western Balkans Organised Crime Gangs requires specific local and regional intelligence collection that feeds into the national threat assessment, to support more targeted disruptions on key vulnerabilities.

Capabilities - Tackling Drugs Supply

65. At the local level - police forces need an agreed understanding of the local drugs threat and good working relationships with key partners. Forces should have an assessment of the local drugs threat (in many forces this is known as a ‘Drugs Market Profile’), which includes an assessment of commodities, supply, demand and market share. A local drugs threat assessment should be shared with ROCUs and NCA to support the National Strategic Assessment. As set out in the Drugs Strategy Guidance for Local Delivery Partners, these should also be used to support a joint needs assessment developed by the local Combating Drugs Partnership, through the review of local drug data and evidence, and agree a local drugs strategy and action plan, including developing data recording and sharing as outlined in the 10-year Drugs Strategy. Forces should work collectively with the members of the Combating Drugs

Partnership and the nominated local Senior Responsible Owner (SRO) to support the development and delivery of these joint products.

66. At a regional level - High Harm and Drugs Taskforces within regions seek to disrupt SOC, including a particular focus on tackling the middle-market drug supply. The operational teams comprise multi-disciplined officers and staff delivering a range of specialist capability including surveillance, financial analysis and enforcement, underpinned by a strong investigative response to high-harm offending. The teams operate in partnership with SOC system partners, including the NCA to identify opportunities to prevent and disrupt organised crime and to seize criminal assets and illegal drugs. Home Office Intelligence also plays a key role in International Drugs Supply and forces should share intelligence on the importation of drugs.

67. County Lines Coordinators are tasked by the National County Lines Coordination Centre (NCLCC) and provide advice and guidance on county lines to operational law enforcement partners. They should support forces across Pursue, Protect, Prevent and Prepare activity on county lines, collating and reporting to the NCLCC. They should contribute to National County Lines training and coordinate responses to County Lines Intensification Weeks.

Capabilities - Fraud

Local Capabilities (Pursue)

68. At the local level - police forces should have capabilities sufficient to respond to local ‘calls for service’, or disseminations from NFIB that are best placed in a local force, proactive intelligence packages disseminated from a national agency including the NCA, and other priorities as recommended by the NSTCG that need local support. This includes preparing for the replacement of Action Fraud with a new system in Spring 2024 which will improve the reporting tools for victims, subsequently increasing the number of reports, providing greater intelligence to policing for investigations, and allowing for greater disruption of fraudsters at scale and at all levels of the policing system.

69. This will be achieved by following best practice as recommended by CoLP in their role as National Lead Force for fraud including their “Fraud Investigation Model” and

upskilling officers through CoLP's Economic and Cyber Crime Academy. Forces must also have an increased regard to capabilities offered by the NCA to the law enforcement system or that can be brokered from partners by the NECC. These include support with the exploitation of intelligence held in Suspicious Activity Reports (SARs), the Joint Money Laundering Intelligence Taskforce gateway to private sector data, the expertise of the Proceeds of Crime Centre, and access to sensitive capabilities held by the NCA or by the UK intelligence community.

Local Capabilities (protect)

70. At the local level forces should have the capabilities to protect and support victims, preventing re-victimisation. Forces must ensure all victims in their local area receive a suitable level of support to protect them from further fraud separate to any investigation, such as that provided by the CoLP-run National Economic Crime Victim Care Unit. Forces should also be able to empower the public to better protect themselves from fraud, and force communication teams play an important role, alongside ROCUs and the nascent fraud Protect network, in providing protective advice to individuals and local communities and businesses. Forces should work with local as well as national groups such as Trading Standards, the National Cyber Security Centre and the NECC. It is vital that protective messaging is aligned with the nationally agreed and published Fraud Communications Toolkit produced by the NECC partnership, and that central coordination allows for de-confliction and enhancement of activity.

71. Forces should continue to deliver their safeguarding responsibilities by using data provided by Action Fraud to safeguard and provide bespoke prevention and protect advice to avoid re-victimisation.

Regional Capabilities

72. At a regional level – The Regional Economic Crime Units (RECU) and Proactive Economic Crime Teams (PECTs) provide a number of critical capabilities that support the national, regional and local responses to fraud, including the pursuit of high harm individuals and criminal groups, working in conjunction with the NECC and the CoLP. This includes investigative capabilities to undertake both reactive and, increasingly, proactive investigations and specialist disruption capabilities (see paragraph 76.10).

Regional Fraud Coordinators or Fraud Development Officers sit within RECUs and coordinate the force-level response to fraud across their region, providing connectivity between the CoLP and local policing.

73. This will be achieved by investing £100m in tackling fraud over the next three years to create over 300 new specialist posts across policing and the NCA including investigators, financial investigators, dedicated disclosure officers, digital media investigators, analysts and intel officers. Forces should also exploit the intelligence captured by the upgraded Action Fraud system once it is operational in 2024 - PECT's will both have capacity to receive nationally-generated proactive intelligence packages and proactively use NFIB intelligence to identify, disrupt and pursue more serious and organised fraudsters and fraud OCG's.

Capabilities - Organised Immigration Crime

74. At both local and regional levels - Police forces need an agreed understanding of the local immigration crime threat and should provide sufficient operational capability proportionate to the threat. Forces should also have good working relationships with key partners including NCA, Immigration Enforcement, Border Force and Home Office Intelligence, and clear processes in place for sharing information and intelligence. We will ensure police have appropriate powers, maximising their ability to take effective action to tackle OIC, without having to pull in law enforcement partners unnecessarily. OIC Coordinators are tasked by the NPCC lead, and should provide advice and guidance, and spread best practice on countering OIC, collating information and reporting to the NPCC lead. All Forces should engage with the MSOICU peer review program and demonstrate how they have implemented both specific recommendations, contained in Improvement Plans and the general good practice from the Program. At the local level forces should have the capabilities to protect and support victims, including through reporting into the National Referral Mechanism for modern slavery and human trafficking. Force communications teams should also play an important role in providing protective advice to local communities and businesses.

Serious Organised Crime - Core Capabilities

75. Chief Constables should be assured that locally their force has:

75.1. Intelligence and analytical capabilities sufficient to identify and understand the level of the threat, risk and harm posed by SOC within the force area and to provide a developed understanding of organised crime groups (OCGs) that are affecting communities, any priority individuals within these groups and considerations of operational threat, risk and harm;

75.2. a designated senior officer with responsibility for overseeing the force's response to tackling SOC, including chairing OCG management boards, force-level tasking boards, and holding Lead Responsible Officers (LROs) to account for delivery of 4P plans;

75.3. operational capability sufficient to respond to the SOC demand placed on the force that is not already owned by the ROCU, NCA or another partner agency. This should also include the operational capability to respond to local 'calls for service', disseminations from NFIB, and recommendations adopted under the fraud CCA voluntary tasking and via the NSTCG process;

75.4. disruption capability sufficient to respond to the SOC demand placed on the force that is not already owned by the ROCU, NCA or another partner agency in order to reduce the threat from SOC. This will be enhanced by having LROs assigned to mapped OCGs and criminal networks where possible, to relentlessly disrupt their business model, infrastructure and ability to cause harm. These roles occupy a pivotal position in connecting the SOC system through the design and coordination of an effective multi-agency response. They should be appropriately trained in how criminal networks operate, and be able to draw upon the full range of police and partner agency capabilities to reduce the SOC threat;

75.5. force cybercrime units (FCCUs) to investigate cybercrime incidents and pursue offenders. These units should deliver cybercrime Protect advice to businesses and the public that is consistent with National Cyber Security Centre (NCSC) advice, guidance and products to help organisations build resilience in response to cyber incidents and threats. They should also identify and refer vulnerable young people in their force area for Prevent intervention;

75.6. SOC prevention capability to identify, deter, and divert people from engaging or re-engaging in SOC. This should include working with partner agencies to safeguard

individuals who are being criminally or sexually exploited, for example by county lines OCGs[38]; and

75.7. operational performance capability to measure the force's impact against SOC threats across the 4Ps. This should include adherence to national performance frameworks such as those required to inform and support the national law enforcement response to drugs supply and county lines as set out in the 10-year Drugs Strategy.

76. To tackle SOC efficiently and effectively, the law enforcement response also needs to be regional, delivered by a ROCU. Contingent on funding (see paragraph 85) each ROCU will maintain core specialist capabilities used to reduce the SOC threat. These are accessible to forces through established tasking processes[39] and include:

Threat assessment and intelligence capabilities:

76.1. Regional Intelligence Departments (RID) collect, analyse and disseminate useful intelligence to either inform an understanding of the organised crime threat picture in the region, or in support of investigative efforts that require intelligence support. They will work with the NCA and partner organisations to support the national understanding of the threat, and with forces.[40] Within the RID are the following capabilities:

a. Regional Organised Crime Threat Assessment (ROCTA) team, as part of a ROCU intelligence department, provide a single, regional capability to identify and assess threats from OCGs, high priority individuals or other identified vulnerabilities in a standardised manner and facilitate SOC System Tasking (paragraph 81). A single picture of the SOC threat, collated by forces[41], the ROCUs and the NCA, ensures the best understanding of the UK-wide threats.

[38] The Home Office has published guidance to assist forces and partner agencies in working with individuals to prevent involvement in SOC. A Practitioner Toolkit – Working with young people to prevent involvement in Serious and Organised Crime (publishing.service.gov.uk)

[39] In many cases, the impact of these capabilities will be augmented by complementary assets within force or the NCA as part of a national capability delivery model.

[40] Forces will maintain a force intelligence bureau, responsible for managing and collating all intelligence within a force area, that will support intelligence gathering of local SOC-related activity

[41] Forces will undertake their own local assessments of threats, but this should be undertaken in a complementary way to the ROCTA assessment.

b. Regional Sensitive Intelligence Units (SIU) are secure environments that can receive, assess, analyse, disseminate and protect “all-source” intelligence and data relating to the SOC threat. They operate as part of a wider national network to acquire, add value and disseminate a wide range of intelligence and data to support the response to SOC.[42] SIUs provide a threat picture and one intelligence environment in which to access all information whilst ensuring all required safeguards are in place. They also provide a Gateway function for requests for ROCU support services.

c. Regional Prison Intelligence Units, in their current operating model, exploit intelligence that exists within the prison environment.[43] They have an effective relationship with His Majesty’s Prison and Probation Service (HMPPS), the prison estate and with other agencies involved in tackling SOC. These units also support the management of organised crime offenders in prison, supporting and informing the multi-agency response to managing and disrupting repeat offending.

76.2. Undercover policing, both foundation and advanced operatives, obtain evidence and intelligence. Foundation officers carry out low-level infiltration that does not require the ability to withstand intense scrutiny whilst advanced officers undertake higher-level and complex infiltrations and can withstand intense scrutiny;

76.3. Undercover Policing Online (UCOL) tackle online child sexual abuse and exploitation and dark-web enabled criminality. UCOLs are deployed to establish and maintain relationships with an individual, network or organisation through the use of the internet with the covert purpose of obtaining intelligence, information or evidence as part of an authorised operation;

76.4. Government Agency Intelligence Network (GAIN) co-ordinators in each ROCU provide forces and ROCU investigators with access to intelligence held by partner agencies. They coordinate the sharing of intelligence related to SOC with partners in compliance with legislative requirements;

[42] This network includes SIUs in the NCA, His Majesty’s Revenue and Customs (HMRC), Police Service Northern Ireland (PSNI), Police Scotland, Metropolitan Police Service, BTP, Ministry of Defence Crime Command, His Majesty’s Prison and Probation Service, Home Office Immigration Enforcement and Border Force.

[43] At time of publication, national prisons intelligence structures were under review and role and remit of the RPIU may be subject to change.

76.5. Technical Surveillance Units deliver technical surveillance capabilities such as equipment interference, intrusive surveillance, online covert activity, forensic computer analysis of devices, such as phones or laptops; and

76.6. Regional Targeted Equipment Interference (TEI) interfere with any type of device or equipment, such as smartphones, computers or vehicles, to obtain different types of data. Dedicated TEI Regional Managers sit in each region. They are responsible for ensuring each region operates at, and is able to, sustain a mandatory minimum level of capability and form the basis for networked capability delivery. They also form a national network, led by the NPCC Senior Technical Coordinator, who sits within a whole system TEI Co-Ordination Hub and leads on TEI capability development on behalf of policing.

Disruption capabilities:

76.7. Disruption Teams aim to disrupt organised criminals through a wide range of tactics, legislation and powers from across the partnership landscape, often focusing on non-traditional or non-criminal justice outcomes for disruption activity. Forces are also expected to undertake disruption activity against lower level SOC offending within their force area working with partner organisations as appropriate.

76.8. Multi-Agency Response to SOC (MARSOC) Hubs are based within ROCUs and within the Metropolitan Police Service. They bring together the police, HMPPS, the NCA and other partners to drive a whole-system response to the highest harm SOC "nominals".[44] These hubs select the highest harm offenders in the criminal justice system and coordinate the response from multiple agencies to disrupt their activity. The hubs report into a national team based in HMPPS.

Threat-specific capabilities:

76.9. Regional Cyber Crime Units (RCCUs) specialise in tackling more serious types of cyber crime, working in conjunction with the National Cyber Crime Unit (NCCU) and local FCCUs. RCCUs manage and coordinate the work of local cybercrime units to maximise the efficiency and effectiveness of local delivery (see National Cyber Event section, under the "Collaboration" heading, paragraphs 99 to 103).

---

[44] An individual who is believed, with some supporting evidence, to be part of an OCG

76.10. RECUs and PECTs provide a number of critical capabilities that support the national, regional and local responses to fraud and economic crime, including the pursuit of high harm individuals and criminal groups, working in conjunction with the NECC and the CoLP. This includes investigative capabilities to undertake both reactive and, increasingly, proactive investigations. RECUs also have specialist disruption capabilities including: intelligence-led asset recovery and confiscation teams to confiscate assets obtained through criminal means and enforce confiscation orders issued to convicted criminals by courts; Civil Order teams to use all available legislation and powers, such as Unexplained Wealth Orders[45] and Account Freezing Orders[46], to disrupt and prevent SOC offending; and Proactive Suspicious Activity Reports (PSAR) teams to also identify suspicious activities of individuals and groups of interest in order to use powers to seize money and assets where the relevant statutory tests are met.

76.11. The CoLP is the lead for coordinating efforts of police forces in tackling fraud across the country in their role as the National Lead Force for fraud, within the overall framework set by the NCA/NECC. This incorporates national reporting, victim care, dissemination of crimes, national level police investigations, training and best practice and intelligence development of fraud offending and offenders in the UK. It is responsible for the national fraud policing strategy and guidance, the national reporting system and cybercrime (Action Fraud), and the NFIB.

76.12. Individuals and organisations report fraud and cyber-crime incidents to Action Fraud. Reports are then analysed by the NFIB which creates intelligence packages for cases with a viable lead and send them to an appropriate local police force to investigate. A centralised system provides significant benefits in analysing and prioritising intelligence, supporting victims and reducing the burden on force control centres.

76.13. Capabilities to tackle drugs supply are listed at paragraphs 65 to 67 above.

77. In London many of the capabilities found in ROCUs are also present within the Metropolitan Police Service (MPS). Due to the unique threats affecting the City of London and the London metropolitan area, some ROCU functions, as well as other specialist capabilities, are provided by the London Partnership. Examples include

[45] Under Chapter 2 of Part 8 of the Proceeds of Crime Act 2002 (POCA).

[46] Under Chapter 3B of Part 5 of POCA

Modern Slavery Units in the MPS, and investigative capabilities of criminal assets, money laundering and complex cyber and fraud investigations that sit with the CoLP in the NFIB and the UK's national fraud and cybercrime reporting centre.

Capacity requirements

78. Chief Constables Council committed to grow the ROCU network by 725 officers between April 2021 and March 2023. This significant growth is enabled by a dedicated allocation from the Police Uplift Programme into ROCUs, the MPS and CoLP. We expect NPCC to further grow the capacity of the ROCU network in 2023/24, as well as to add 124 new dedicated fraud posts funded by the Spending Review that will be in place by March 2025.

79. The required capacity to tackle SOC will vary depending on the scale and nature of the threat in a given force area or region. ROCU resources should be operationally and geographically balanced. They should be aligned with the demand from the highest priority SOC threats for policing and remain attuned to the changing threat and evolve to deal with it.

80. Monthly tasking meetings at force and ROCU level consider the resources that a given level of SOC threat and demand within a force area or region requires and determines if local, regional or national capabilities, or a combination, should be allocated to tackle the threat.

Consistency and standards

81. SOC System Tasking supports the identification and management of capabilities across the law enforcement system. It enhances interoperability between partners and each tier of the law enforcement system, providing consistency in the way capabilities are accessed, tasked and coordinated. It operates as follows:

81.1. All law enforcement agencies should undertake an assessment and prioritisation of OCGs, individuals and tactical vulnerabilities through Management of Risk in Law

Enforcement (MoRiLE)[47] and the Prioritisation Mechanism[48] which ensures a consistent process for scoring threat, risk and harm prior to submission onto the national SOC Master List. This list provides a single view of demand across the system and should inform tasking decision-making at the local, regional and national level ensuring that ownership and risk sit with the organisation best placed to respond.

81.2. Tasking across the SOC system should be multi-directional. A Federated Tasking Team, with representatives from the NCA, ROCUs, forces and other agencies, sit at the heart of the SOC System Tasking model and can broker access to specialist capabilities, arbitrate over the transfer of risk, and provide operational review as required.

82. To ensure a consistent approach to SOC within force, Chief Constables should be assured that:

82.1. all officers and staff involved in the response to SOC within their force work closely with their Neighbourhood policing teams. This ensures that the signs, symptoms and vulnerabilities associated with SOC at a local community level are appropriately understood, and community intelligence supports the development of the SOC threat picture and 4P response activity; and

82.2. the Victim Code of Practice is consistently applied to all victims of SOC.[49] This should include support for children and vulnerable adults who have been criminally or sexually exploited by OCGs, such as those involved in drugs supply and county lines. In the case of fraud, victim data provided by Action Fraud should be used to safeguard those at risk from further harm and repeat victimisation.

82.3. The City of London Police as the National Lead Force for fraud also sets standards for police forces in tackling fraud which ensures a consistent approach, for example through their Fraud Investigation Model and their National Lead Force Plan published 2020. CoLP often represents policing in partnership working to better tackle fraud, including at tasking coordination meetings led by the NECC which aim

[47] The MoRiLE tool identifies harm and risk linked to crime type or community problem and assesses this against the force's capacity and capability to deal with the problem.

[48] Following completion of the MoRiLE assessment, the P-Mech then assigns a prioritisation banding (P-Banding) graded 4 (the lowest threat) to 1 (the highest threat).

[49] https://www.victimsupport.org.uk/help-and-support/your-rights/victims-code

to ensure the operational system collectively makes effective prioritisation decisions.

Collaboration

83. In order to tackle SOC efficiently and effectively, a coordinated law enforcement approach is essential. The NCA is responsible for coordinating the national law enforcement response. As the primary interface between the NCA and forces, ROCUs support the coordination of the collective effort against the SOC threat. They:
    a. offer forces specialist policing capabilities which sit exclusively at the regional tier of the SOC system. Capabilities considered highly sensitive will, in most cases, be delivered from the NCA through the ROCU network for the wider policing benefit;
    b. lead the regional operational response to SOC on behalf of forces within their regions. These include complex, high-harm investigations;
    c. assist a force's own response to SOC locally by acting as a centre of operational guidance and support;
    d. build an authoritative view of all SOC for their respective regions via their ROCTA, the team who develops the regional threat assessment. This, in turn, is submitted to the NCA to inform national and thematic threat assessments including the National Strategic Assessment; and
    e. provide a regular flow of intelligence into the NCA to ensure the National Assessment Centre (NAC) can draw on the latest regional insight to support year-round threat assessment and provide strategic intelligence products back to the ROCU.

84. ROCUs are expected to continue to develop better networked capability to bring further consistency, capacity and connectivity to the network. Transformation of the network will be supported by a National Strategic Business Plan[50] which sets out the priority activities and programmes of work that will bring increased Consistency, Coherence and Connectivity to the network in line with the 2030 ROCU Strategy.

85. In order to ensure the continuing success of ROCUs, Chief Constables and PCCs must continue to comply with their legally binding Section 22 collaboration agreements which require them to make an annual contribution to their ROCU of officers, staff and

[50] The National Strategic Business Plan is also applied by MPS who contribute to its objectives

funding. This contribution will vary in nature and quantity depending on their region and the size of their force. The Home Office will monitor compliance with these agreements.

86. In order to foster a whole-system, efficient and effective response to SOC, Chief Constables and PCCs should:
    a. access the specialist capabilities through their ROCU. Any new SOC capability should be considered first and foremost for development and delivery in ROCUs rather than duplicated locally within each force as this would generate inefficiency. Forces should be clear about what capabilities and capacity they possess locally which duplicates that available regionally and be prepared to explain the resourcing decisions they have made during HMICFRS inspection;
    b. share their force-level threat assessment with their ROCU to provide a single, authoritative view of the SOC threat across the region;
    c. share data and intelligence in a timely fashion to enable a coordinated and effective response to SOC threats that traverse police force boundaries. This is particularly important for drugs supply and county lines 'importer' and 'exporter' forces where forces should work together, as well as with their ROCU and the NCLCC to share intelligence, inform best practice and coordinate Pursue and Protect activity. This also includes sharing with Home Office Intelligence who play a key role in both border security and preventing illegal migration;
    d. For fraud, there is significant collaboration between CoLP who are the national police lead force responsible for fraud and the NECC who are the system lead responsible for leading operational work across law enforcement, regulators, the intelligence community and industry. Collaboration between forces is further facilitated through the role of CoLP as National Lead Force and the NFIB system. CoLP's NFIB system also collates data from industry reports and there is considerable joint working with industry through the NECC Public and Private Partnerships team which includes JMLIT, and via CoLP's funded units. These public private partnership teams include the Insurance Fraud Enforcement Department (IFED), Police Intellectual Property Crime Unit (PIPCU), the joint MPS and CoLP funded unit and the Dedicated Card and Payment Crime Unit (DCPCU).

Connectivity with partners

87. To ensure a whole-system approach to SOC, Chief Constables should ensure that their force works effectively with non-law enforcement partners through police-led multi-agency partnerships, such as a Community Safety Partnership. This must be led by the police but include PCCs, local authorities and other relevant partners such as those in education, health and social care, Immigration Enforcement, and third or private sector. Forces should:

87.1. share their SOC local profile which shows the signs and symptoms of SOC in addition to vulnerabilities within local communities. This should be informed by a wide range of public, private and voluntary sector intelligence and insight to develop a common understanding among local partners of the threats, vulnerabilities and risk from SOC in a local area. The SOC local profile should directly inform the police and crime plan.

88. These police-led partnerships should also:

a. share intelligence and exchange information, where appropriate and within legislative constraints, to inform the force-level SOC threat assessment;
b. develop 4P action plans for tackling SOC, with clear lines of accountability and ownership across the partner agencies. It should also strengthen multi-agency understanding and awareness of SOC, and drive reductions in SOC-related harm in communities;
c. share joint resources from these different agencies in support of 4P disruptions against SOC; and
d. understand and be able to demonstrate the collective impact 4P activity is having on the SOC threat.

National Cyber Event

A national cyber event covers cyber-attacks across the thirteen sectors of the Critical National Infrastructure (CNI) which include: chemicals, civil nuclear communications, defence, emergency services, energy, finance, food, government, health, space, transport and water. It covers those incidents identified as Category 1 (C1) or Category 2 (C2) as defined by the National Cyber Security Centre (NCSC). A C1 incident is a "national cyber emergency" which causes sustained disruption of UK essential services or affects UK national security, leading to severe economic or social consequences, or to a loss of life. A C2 incident is a "highly significant incident" which has a serious impact on central government, UK essential services, a large proportion of the UK population or the UK economy. Additionally, a C3 (High) incident may also be relevant. A C3 incident is "a cyber attack which has a serious impact on a large organisation or on wider / local government, or which poses a considerable risk to central government or UK essential services. A "High" flag is applied when there is a particular sensitivity, speed of response, or additional level of response resource required.

Outcomes

89. The National Cyber Strategy[51] sets out a vision that the UK will continue to be a leading responsible and democratic cyber power, able to protect and promote our interests in and through cyberspace in support of national goals. These goals include the aim to be a more secure and resilient nation, better prepared for evolving threats and risks and using our cyber capabilities to protect citizens against crime, fraud and state threats. Key strategic objectives for policing include:

Threat Pillar

89.1. Deter and disrupt state, criminal and other malicious cyber actors and activities against the UK, its interests, and its citizens (**Pursue**).

89.2. Prevent people from cyber offending, remove enablers and reduce incentives of cyber crime (**Prevent**).

[51] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

Resilience Pillar

89.3. Protect through building cyber security and resilience of UK and its economy, including safeguarding its citizens (**Protect**).

89.4. Strengthen capability to prepare for, respond to and recover from cyber attacks to minimise harm caused and support victims (**Prepare**).

89.5. The Home Office Outcome Delivery Plan[52] sets out in detail how we will deliver the department's priority outcomes, how we will measure our success, and how we will ensure we continuously improve. These outcomes include:

- Reduce cyber crime.
- Increase support for victims and potential victims of cyber crime.
- Reduce the wider fear of cyber crime and increase the public's satisfaction with cyber policing.

90. The Government Cyber Security Strategy[53] pursues a central aim - for government's critical functions to be significantly hardened to cyber attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030. This includes policing as part of the Emergency Services CNI sector.

91. Police forces should be able to demonstrate that they can effectively support these national efforts to respond to cyber incidents to ensure UK, including their own, networks, data and systems are protected and resilient by aligning their response to the outcomes detailed in the above strategic documents.

Capabilities

92. ROCUs provide police forces with access to a range of capabilities to help them tackle serious and organised crime including a dedicated cyber-dependent capability.

93. The National Cyber Security Centre (NCSC) directs the response to major cyber incidents (C1 and C2) whilst the NCA leads the law enforcement response. However,

[52] https://www.gov.uk/government/publications/home-office-outcome-delivery-plan

[53] https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030

in these incidents, it is highly likely that multiple CNI, government premises, businesses and/or supply chains will be affected. Local forces and regional units, led and coordinated by the National Cyber Crime Unit, have a key role to play in mitigating the impact of an incident, the investigation, and in victim care. In order to respond effectively to these incidents, Chief Constables should be assured that their force:

93.1. maintains a force cybercrime unit (FCCU) whose primary functions should be dedicated to:

a. support the NCA to identify and secure multiple crime scenes in order to gather digital evidence. FCCUs and Force Digital Forensic Units should have the necessary equipment, resources and training to retrieve, manage and examine data in compliance with all legal and regulatory requirements;
b. resource broader local investigative actions set by the lead investigating authority. Officers should have access to police research and analytical support in addition to digital forensics as part of these investigations; and
c. provide an effective response to victims, including businesses and the general public, who have been subject to a cyber-attack.

94. In addition to working with the NCSC and the NCA in response to C1 and C2 incidents, FCCUs should also be able to respond and investigate as lead agency to C5 or C6 incidents – those targeted at an individual or a small or medium-sized organisation – within their force area (see also SOC section, paragraph 75.5).

95. Chief Constables should also be assured that their force:

a. maintains the necessary public order capabilities (see Public Disorder section paragraph 117 onwards) in order to respond to any possible public order and public safety implications resulting from the incident;
b. has the necessary plans and contingency arrangements in place to carry out their duties as a Category 1 responder (paragraph 132); and
c. are more prepared to respond to and recover from cyber incidents that affect their force, including through better cyber incident planning and regular exercising.

Capacity Requirements

96. The NPCC Force Cybercrime Unit Minimum Capability Standard does not set minimum staffing levels, but forces should have sufficient capacity to deal with the increasing levels and complexity of cyber-dependent crime and to meet the outcome listed in the Standard: that the delivery of FCCUs will lead to substantially more and improved investigations, with increased numbers of arrests, convictions, and larger numbers of criminal networks disrupted and dismantled.

97. Forces will need to determine capacity levels based on levels of reporting and the level of liability in their force area. For the latter, they should consider the organisations and institutions in their force area that are potentially vulnerable to a cyber-attack and which, if attacked, would have a large impact on their force area.

Consistency and Standards

98. The Minimum Capability Standard also sets the minimum requirements and standards for FCCU capabilities. To support a coordinated response to cyber-dependent crime and attacks, Chief Constables should ensure officers and staff receive the appropriate training for conducting investigations, using digital forensics, and for Protect, Prepare and Prevent activity.

Collaboration

99. Under the previous National Cyber Security Strategy, the Home Office, NPCC, and the NCA have collaborated to establish an effective response to cyber-attacks in England and Wales. This operates as a single, nationally-networked resource at the national and regional level which means law enforcement can react in any situation.

100. Nationally, the NCSC is responsible for responding to cyber-attacks which threaten national security by providing advice, technical support and co-ordination to a cross-government response. The NCA leads the law enforcement response.

101. The NCA's National Cyber Crime Unit also responds to cyber incidents coordinated by OCGs or state actors. It works with the NCSC, ROCUs, forces and international law enforcement (Europol, Interpol and international partner's investigation units) to share intelligence and coordinate action. It is also responsible for developing

partnerships across the intelligence community and with private industry to share information and technical expertise.

102. The NPCC agreed that every force should have its own dedicated cyber-dependent crime capability and that this local capability should be “regionally managed and locally delivered”.

103. To ensure an efficient and effective response to cyber-attacks and to facilitate join-up, Chief Constables should be assured that their force is collaborating with national agencies to:

a. disseminate Protect advice coordinated and shared by the NCSC and from the National Protect Network, led by the City of London Police;
b. innovate and deliver Prevent advice and information shared by the National Prevent Network which is coordinated by the NCA;
c. exchange intelligence with the NCCU to ensure that the clearest possible intelligence picture is available nationally;
d. respond to tasked cyber actions in a timely manner. This national tasking process ensures that the response to cyber-attacks are disseminated to the most appropriate law enforcement authority dependent on the scale, location and complexity of the attack; and
e. support complex and high-harm investigations with local investigative work, victim care and Protect advice.

Connectivity with Partners

104. The response to the impact of national cyber security incidents may require multi-agency working with Local Resilience Forum (LRF) partners to mitigate the impact (paragraph 138).

105. Given the prevalence and widespread nature of cyber-dependent crime, partnerships between law enforcement agencies and other organisations are incredibly important. Chief Constables should ensure their FCCU is:

a. working with government premises, businesses, supply chains and the general public to ensure that they can protect themselves from the impact of a cyber-attack;
b. supporting the work of Regional Cyber Resilience Centres in each of the nine policing regions and London. These are collaborations between the police, public,

private sector and academic partners to provide subsidised or free products and cyber-security consultancy services to help SMEs and micro-businesses to protect themselves; and

c. supporting the work of the Cyber Prevent network in developing national, regional and local interventions and will draw on public, private and voluntary sector partners to deliver diversionary and dissuasive activities for young people.

Child Sexual Abuse

Child sexual abuse involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving a high level of violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example, rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing and touching outside of clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse. Sexual abuse can take place online, and technology can be used to facilitate offline abuse. Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children.

Outcomes

106. The Tackling Child Sexual Abuse Strategy outlines the Government's ambition to strengthen the response to all forms of child sexual abuse through three key objectives: tackling all forms of child sexual abuse and bringing offenders to justice; preventing offending and reoffending; protecting and safeguarding children and young people and supporting all victims and survivors.[54] The police have a key role in achieving this vision. Policing should support the measures outlined in the Strategy by:

a. adopting robust disruption strategies against offenders to lead to a reduction in the overall threat of child sexual abuse, working with relevant partner agencies;
b. robustly prioritising offenders to target those assessed as highest harm;
c. processing digital forensics without significant delays, to identify more victims and offenders;
d. working closely with prosecutors on efficient and effective case-building for effective trials for child sexual abuse to bring more offenders to justice;
e. maximising the effectiveness of civil orders including Sexual Harm Prevention Orders (SHPO) and Sexual Risk Orders (SRO) to manage risk;
f. becoming more adept at detecting offending and reoffending, including breaches of notification requirements and civil orders;

[54] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/955493/Tackling_Child_Sexual_Abuse_Strategy_2021.pdf

g. increasing the quality and availability of support for victims and survivors to support them to feel able to disclose abuse;
h. working with safeguarding partners and support services to provide wraparound support to victims and vulnerable witnesses throughout investigations; and
i. playing an active role in local child safeguarding as part of the local safeguarding partnership.

Capabilities

107. Forces should maintain child abuse investigation units and safeguarding teams.[55] These should be staffed by police officers and staff that have undertaken the relevant specialist training to respond to cases of sexual abuse. They should be able to:

107.1. gather and assess intelligence and data to understand the threats, including emerging ones, risks and harms to children and young people. This also supports forces to identify and target persistent offenders and make links with other investigations relating to child abuse;

107.2. detect the signs of vulnerability by drawing together all available information to understand the potential risks to a child and sharing this with other forces and partner organisations as necessary. When investigating cases of child sexual abuse in the family environment, forces should consider the risks to other children such as siblings or those in the neighbourhood, working with local partnership agencies to consider how to manage risk and safeguard children;

107.3. ensure effective strategies are in place to protect children and young people and prevent harm, developed and tested via local safeguarding partnership arrangements. Police forces should have internal systems and multi-agency protocols to ensure that concerns for children are prioritised and actioned appropriately by each agency and that partner agencies such as health care workers and social workers are involved in decision making and child protection plans;

[55] The term child abuse investigation unit refers here to a team or unit whose primary function is to investigate child abuse. Other terms for this grouping can include: child protection investigation unit; child protection team; child protection unit; and child abuse investigation team. It is likely that forces have a number of structures and terms for their child abuse investigation units and some may have units that deal with a wider scope of work than child abuse. Forces have the discretion to decide on the most suitable term for their unit. See: https://www.app.college.police.uk/app-content/major-investigation-and-public-protection/child-abuse/police-response/staffing/#definition.

107.4. conduct complex and multi-faceted investigations to identify perpetrators. Investigations should consider arrests, victims or witness approaches, research enquiries, and evidential searches, working with specialist agencies where necessary;

107.5. communicate with vulnerable victims, particularly children, and put their voice at the heart of decision-making, handling the diverse needs of victims effectively and with sensitivity to the trauma sustained. This includes appropriate interviewing techniques, the use of intermediaries and aligning with 'Achieving Best Evidence' practices;

107.6. monitor offenders and identify and manage re-offending, working with Neighbourhood Policing Teams where appropriate, and making use of the full range of tools available to them when managing risk, including the use of bail conditions and extension of bail (where applicable) to manage risk and protect children from harm;

107.7. follow best practice with regards to sexual harm prevention orders and sexual risk orders; and

107.8. access adequate digital forensics specialists to obtain, analyse and use digital evidence in investigations or criminal proceedings. They should have access to the latest technology[56] to match current and future demand, proving able to deal with increasing numbers of devices and increasing levels of anonymisation.

108. To counter online child sexual abuse, forces should have, or have access to, and use effectively:

a. risk assessment tools, such as the Kent Internal Risk Assessment Tool (KIRAT), and have officers well trained in how to use them. These tools should support the assessment of risk of individuals suspected of possessing, making, taking and distributing indecent images of children, prioritising the most dangerous offenders;

b. the Child Abuse Image Database (CAID), a secure database that brings together images, videos and hashes that the police and the NCA encounter to support law enforcement in the identification of victims and perpetrators. This includes contributing images and information to CAID. Forces should also consider the role of a Victim Identification Officer;

[56] The Transforming Forensics 'CSE Automate' project in 2021/22 delivered a package of materials to support all forces in adopting automation technology, consolidated workflows and testing procedures to streamline and improve productivity.

c. offender management skills and capability to uncover and investigate online offences from known offenders;

109. In some cases of child sexual abuse, due to scale, severity or complexity, forces will need to work with ROCUs for access to specific specialist capabilities.

Capacity Requirements

110. Forces should have adequate management information on child sexual abuse cases so they can understand risk and demand levels and force performance. Forces should also have sufficient capacity to deal with current levels and complexity of child sexual abuse cases, and plans to adjust capacity to deal with anticipated increases in the coming years. Each force should have a staffing model that is flexible enough to respond to this changing demand, with a swift feedback loop to understand and respond to emerging threats.

Consistency and Standards

111. In order to ensure a consistent approach to child sexual abuse across England and Wales, Chief Constables should ensure that:

a. officers are following the APP[57] on child sexual abuse and child sexual exploitation from the College of Policing;
b. their force is operating to the agreed definitions of child sexual abuse and child sexual exploitation as outlined in the APP;
c. intelligence gathering and data analysis is conducted in a consistent manner to strengthen the national ability to draw patterns and share information. Their force should also be responding to the Home Office's annual requirements on child sexual abuse, and liaising with child sexual abuse analysts in ROCUs on their commissions to ensure consistency of data collection at the national level; and
d. digital forensics, where possible, are accredited.

[57] https://www.app.college.police.uk/app-content/major-investigation-and-public-protection/child-abuse/

Collaboration

112. Organised forms of abuse and exploitation will cross police force boundaries and serious and serial offenders may abuse in multiple force areas. Victims of abuse may be vulnerable to trafficking across force boundaries or may go missing from one force area and be abused in another. It is important that forces have mechanisms in place for the effective sharing of intelligence with other forces, their ROCU and with the NCA, including through programmes such as the Tackling Organised Exploitation Programme, so that the scale and nature of the threat can be robustly understood and addressed, and victims appropriately supported.

113. To tackle many forms of child sexual abuse, forces will need to work with their ROCU and with the NCA. This is particularly the case with high harm and complex online cases with dark web or international elements. Forces should collaborate to share intelligence and access specialist capabilities, and they should also respond in a timely and effective manner to all packages sent to them from the NCA.

114. Forces should also engage appropriately with NCA-led strategic governance arrangements.

Connectivity with Partners

115. To ensure a whole-system response to child sexual abuse, Chief Constables should ensure their force is fully utilising their local multi-agency safeguarding arrangements. These arrangements should be with local authority and health partners, including prisons and probation, the voluntary sector – including community-based organisations – and schools, to set strategic direction and improve join-up of services. They should work with these partners to:

a. put in place preventative and early intervention approaches;
b. share information and intelligence to detect and identify risk to children, or specific locations or individuals of concern;
c. undertake joint risk assessments;
d. produce joint safeguarding plans for children deemed at risk, with clear roles for each partner and processes to hold each other to account for action taken;
e. put in place plans for managing risk around those who may pose a risk to children; and

f. put mechanisms in place to share lessons learned, including learning from local and national reviews of cases involving harm to children, and embed these into practice to respond to emerging trends, with the support of national programmes such as the Vulnerability Knowledge and Practice Programme.

116. Forces should also:

a. collaborate with the NCA to build constructive relationships with online platforms and industry to encourage them to share information about online offenders in a timely manner;

b. engage early with Crown Prosecutors to strengthen communication and joint-working and to ensure that a balance is struck between increasing the quality and quantity of cases taken forward to prosecution.

Public Disorder

Public disorder can take many forms and can include rioting, looting, vandalism, violence and arson. There are a number of trigger or flash points that could lead to localised disorder including controversial or fatal incidents involving the police and public; escalating inter-community tensions; and large-scale organised protest at risk of hijack by those intent on causing public disorder. Lawful protests are not considered a form of disorder and we support the right to protest peacefully, where such protests do not cause serious disruption to the lives of others.

Outcomes

117. Police forces should be able to demonstrate that they can appropriately mobilise in response to a variety of public order policing operations at a force, regional and national level in accordance with the National Mobilisation Plan.[58] These include the ability to respond to public disorder, protest and other significant events with a potential impact on public order by:

a. environment scanning, intelligence assessment and planning for spontaneous or pre-planned events through assessing capacity, planning, using the Strategic Risk Assessment (SRA) process, and then mobilising resources and capabilities[59];

b. assuming responsibility for responding to, and managing incidents or events that are within its capacity; and

c. activating regional or national mutual aid arrangements if there is not enough capacity or capability to respond locally.[60]

Capabilities

118. Forces are responsible for responding to and managing incidents or events which threaten public order in its force area. Chief Constables should ensure that they have a range of specific police public order capabilities as a force or across a region to meet the local requirements and their agreed contribution to regional and national requirements. These include:

[58] https://www.app.college.police.uk/app-content/mobilisation/

[59] The strategic risk assessment is a process by which forces analyse information about threats and risks against which they are required to commit resources.

[60] Mutual aid is the provision of policing assistance from one force to another for the purpose of meeting any special demand.

a. Operationally competent and nationally accredited Gold, Silver, and Bronze Commanders, and Public Order Safety Advisors (POPSA) to effectively plan and lead public order deployments in their force area and contribute to regional and national threats (in accordance with the SRA).
b. Local and National Strategic Intelligence, environmental scanning and coordination capability across all forces through to NPoCC;
c. Police Support Units (PSUs) with officers trained to “level 2” to respond to spontaneous or pre-planned public order and public safety events where specialist tactics are required. A force should maintain and test plans to mobilise PSUs to respond to outbreaks of disorder in their force area;
d. “level 3” public order trained officers who are deployed in Basic Deployment Units (BDUs) for spontaneous or pre-planned public order events where specialist tactics are not required;
e. Protester Removal Teams (PRT) trained to undertake the removal of persons:
    i. PRT (standard) trained to undertake removal of persons, including those who may have affixed themselves to structures or people;
    ii. PRT (complex) trained to undertake removal of persons, including those who may have affixed themselves to structures or other people at height;
    iii. Debonding officers trained in the removal of those persons who may have glued themselves to items, structures or other people as part of a protest;

f. Attenuated Energy Projectile (AEP) trained officers, as required by the region. AEPs provide officers with a differentiated use of force and firearms to dissuade or prevent a potentially violent person from their intended course of action to neutralise the threat in cases of serious public disorder;
g. Evidence Gatherers (EG) trained to produce evidential quality video footage for later prosecutions;
h. Police Liaison Team (PLT) officers to ensure the flow of information between police officers and crowd members, make assessments of individuals and groups and communicate emerging issues to the command team;

i. Forward Intelligence Team (FIT) who can gather information and intelligence on groups and individuals to identify areas of threat and risk, providing commanders with updates; and
j. Public Order Medics to undertake first aid treatment, inform casualty status.

119. There are other capabilities that can be deployed in public disorder scenarios, including police dogs and horses alongside specialist tactics and trained officers. These need to be available on a national basis but should be maintained by forces according to local needs.

Capacity Requirements

120. In order to respond to public disorder efficiently and effectively, police forces should ensure that their force capacity meets any requirements set by their region or as agreed by the NPCC. These requirements are determined by a national SRA that identifies the risks and required capacity to respond dependent on a consideration of information, intelligence, capabilities, and current capacity. This process ensures national availability – including in support of the Police Service of Northern Ireland and Police Scotland – of essential capabilities.

121. Capacity for nationally identified public order capabilities is determined through the National Public Order and Public Safety (NPOPS) governance structure. The requirements for deployment capability are currently:

a. PSUs totalling 297 across England and Wales, alongside 75 units for London;
b. Level 3 public order trained officers set at 234 BDUs; and
c. the ability for each region to deploy two full AEP teams, providing a total of 18 AEP teams if required[61].

122. There are currently no set capacity requirements for EGs, PLTs, PRTs, FITs, debonding officers, or public order medics. This will be updated according to the assessment of threats, harm and risk from the National SRA, and as agreed by the NPCC.

Consistency and Standards

123. Public order resources should be consistent across England and Wales and trained to agreed College of Policing standards. Any deployed equipment and vehicles should meet national requirements, agreed by the NPCC in collaboration with the College of Policing. Chief Constables should ensure their force's:

[61] Accurate at time of publication. Figures may change.

a. PSUs comply with the national definition of one inspector, three sergeants, and eighteen constables and are at least “level 2” trained along with three drivers and suitable transport;
b. BDUs consist of one inspector, three sergeants, and eighteen constables who are at least “level 3” trained including suitable transportation;
c. AEP team, if required by their region, consists of 6 officers, an operational AEP commander, one driver, and four officers; and
d. public order commanders undergo accredited training and continuous professional development in line with College of Policing standards.

Collaboration

124. Police forces should collaborate with each other through NPoCC. Mobilisation in response to events which threaten public order is based on a tiered mutual aid response. These tiers are national (tier 3), regional (tier 2), and local (tier 1). Each tier has its own key roles, structures and processes that facilitate effective mobilisation. The Police National Public Order Mobilisation Plan specifies the numbers and type of mutual aid resources that should be available.

125. In situations where an event or incident has the potential to exceed local capacity and capability, forces should activate appropriate command structures to take any immediate action to minimise the potential impact and assess the event to determine if mutual aid is required.

126. If it is decided that additional resources are required, the force should work through their regional structures and with NPoCC to ensure capability and capacity requirements for the incident are met regionally and then nationally if required.

127. At the national level (tier 3), NPoCC is responsible for mobilisation, capacity and capability assessments, testing capability and mobilisation of national assets, facilitating mutual aid, and ensuring effective reporting mechanisms to the Home Office. They also share good practice with forces and manage the Mercury System, a computer system that assists in managing the mutual aid deployment of police resources across force geographic boundaries. To ensure national mobilisation is efficient and effective, forces should:
a. participate in NPoCC’s quarterly assessments of capabilities and capacity;

b. participate in the testing of capability and mobilisation of national assets when required;
c. share local perspectives on current and future events, potential resource implications, and local resilience with NPoCC;
d. participate in a national debriefing and reporting process to share best practice, review training and tactics, as well as working towards consistency across the whole of policing.

128. **Regional mobilisation** (tier 2) is based on nine regions. Each region has its own Regional Information and Coordination Centre (RICC) which is responsible for communication and coordination across the region and deployment of mutual aid resources from within the region. To ensure effective and efficient mobilisation at this tier, forces should work with their RICC by:

a. Sharing local capacity and capability assessments;
b. sharing the force's mobilisation plan for quality assurance;
c. notifying the RICC of existing collaborative arrangements; and
d. liaising with the RICC when mobilised to identify and supply relevant resources.

129. In circumstances in which police forces have the capacity to respond to local incidents of public disorder (tier 1) and do not wish to rely on mutual aid, Chief Constables should be assured that they have access to specialist capabilities and tactics in force or through collaboration agreements with other forces.

Connectivity with partners

130. The police need to work closely with a number of bodies and groups to ensure public order is maintained at large-scale national and regional events as well as routine local community events, including music festivals, or other celebratory, cultural or sporting events. The police should:

a. ensure there is engagement locally with event organisers, local authorities and licensing bodies, and through the Safety Advisory Group processes.
b. participate in local Safety Advisory Groups overseen by local authorities;
c. engage with protest groups and those that represent them to discharge policing duties and responsibilities;

d. work with other Emergency Services in the planning and response to policing of public disorder, utilising the JESIP principles for joint working (see Cross-Cutting Capabilities section paragraphs 174 and 175); and

e. engage with communities, businesses and other stakeholders affected by public disorder or public order policing operations so that the impact can be mitigated, and forces can best discharge their policing duties.

Civil Emergencies

A civil emergency is an event or situation which threatens serious damage to human welfare in a place in the UK, the environment of a place in the UK, or war or terrorism which threatens serious damage to the security of the UK.[62] It covers, but is not limited to, events such as natural hazards, severe weather, flooding, human and animal disease, major industrial or transport accidents, and terrorist or cyber security incidents.

Outcomes

131. The Civil Contingencies Act sets out the legislative framework for preparing to respond to civil emergencies and divides local responders into two categories, imposing a different set of duties on each[63].

132. Those in Category 1, including the police, are at the core of the response to most emergencies. Category 1 responders are subject to the full set of civil protection duties. The police, as category 1 responders, are required to work with multi-agency partners to:

a. assess the risk of emergencies occurring and use this to inform contingency planning;
b. put in place emergency plans and business continuity management arrangements;
c. put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency;
d. share information with other local partners to enhance coordination and efficiency; and
e. co-operate with other local responders to enhance co-ordination and efficiency.

133. Category 2 organisations (such as the Health and Safety Executive, transport and utility companies) are 'co-operating bodies.' They have a lesser set of duties which cover co-operating and sharing relevant information with other Category 1 and 2 responders.

[62] Chapter-1-Introduction amends_16042012.pdf (publishing.service.gov.uk)

[63] https://www.legislation.gov.uk/ukpga/2004/36/contents

Capabilities

134. To effectively and efficiently respond to civil emergencies in their area, Chief Constables and PCCs should ensure their force:

134.1. has an operations unit that supports the contingency planning function within the force area and participates, with appropriate senior representation, in the Local Resilience Forum (LRF) to plan, prepare and exercise and, when required, respond to and recover from major incidents. This unit:

a. manages the strategic and tactical co-ordinating centres and the associated infrastructure required to enable them to operate effectively;

b. is responsible for planning for civil emergencies; and

c. supports Safety Advisory Groups to advise and discuss plans, in consideration of public safety at major events.

134.2. maintains appropriately qualified and trained commanders including:

a. multi-agency gold incident commanders (MAGIC) who assume and retain overall command for the operation or incident. They:

- have overall responsibility and authority for the police gold (strategic) strategy and any tactical parameters; and
- are responsible for ensuring that any tactics deployed are proportionate to the risks identified, meet the objectives of the strategy and are legally compliant;
- silver (tactical) commanders who can command and coordinate the overall tactical response in compliance with the strategy and manage the tactical command of the incident; and
- bronze (operational) commanders who are responsible for the command of a group of resources, and for carrying out functional or geographical responsibilities related to a tactical plan.

135. Forces should also have or have access to:

a. a regional casualty bureau to provide information on the investigation process relating to an incident, trace and identify people involved in an incident and reconcile missing persons reports;

b. Disaster Victim Identification (DVI) to recover and identify deceased people and human remains in multiple fatality incidents, bringing together antemortem and post-mortem information to make a positive identification by scientific means in a dignified manner; and

c. effective business continuity plans and resilient systems in order that it can continue to operate its core functions, including supporting major incident response when faced with disruptive challenges.

Capacity Requirements

136. Forces should plan and prepare with partners, through their LRF, for a series of reasonable worst case scenarios presented in the National Risk Register.[64] The risks, their impact on local communities and the actions that will need to be taken to mitigate the risk, respond and support recovery should be identified in the LRF's local community risk register. Capacity requirements for the police capabilities listed above should be determined as part of this risk assessment process.

Consistency and Standards

137. Responding to an emergency event locally requires interoperability with other non-law enforcement partners. To ensure the response is as efficient and effective as possible, please refer to "Connectivity with partners" below.

138. The National Resilience Standards also allow local responder organisations to self-assure their capabilities and overall level of readiness. The Standards principally define expectations of good and leading practice for LRFs.[65]

Collaboration

139. In situations in which additional law enforcement support is required, a Chief Constable should call for assistance using mutual aid. This provides overall resilience to the provision of effective policing of an incident and force area.

[64] https://www.gov.uk/government/publications/national-risk-register-2020

[65] National Resilience Standards (publishing.service.gov.uk)

Connectivity with Partners

140. To ensure the response to local emergencies is as efficient and effective as possible, a force should have well-developed partnerships with other Category 1 responders within their LRF. LRFs cover a police force area and are multi-agency partnerships between Category 1 and 2 responders. Where appropriate they will also work with the Voluntary and Community Sector (VCS) and the military to dispense their duties under the CCA. LRFs identify and plan for resilience risks. Chief Constables should ensure that their force:

a. is represented at an appropriately senior level on the LRF and participates in LRF business;

b. adopts the JESIP principles of joint-working with multi-agency partners, with the objective of normalising interoperability;

c. has a shared understanding of all risks, partner agencies' capabilities, limitations, priorities and working practice, in order to facilitate an efficient, effective and coordinated joint response to incidents of varying levels of severity and scale;

d. adopts commonly-agreed terminology, definitions, and graphic and map symbols to enable a joint understanding of risks, plans and working practices, and support the attainment of shared situational awareness and a joint understanding of risk in emergency response and recovery;

e. chairs, or is represented on, the Strategic Co-Ordinating Group (SCG) mobilised during the response stage of an incident. The SCG includes senior representatives from each of the key organisations and will: define multi-agency strategy; make informed decisions in good time; coordinate multi-agency activities; communicate and interoperate with other agencies at local and national levels; and monitor and change strategy, communications and activity as the situation evolves[66];

f. adopts the M/ETHANE model as the shared situational awareness reporting framework for responders and their control rooms (paragraph 175)

g. participates in multi-agency training and joint-exercising programmes; and

h. shares lessons after major incidents and exercises with the wider LRF community and other agencies.

[66] See CONOPs_incl_revised_chapter_24_Apr-13.pdf (publishing.service.gov.uk) (pg.48) and National Resilience Standards (publishing.service.gov.uk), pg. 30.

141. As part of the LRF, police forces should also work with Category 2 responders including, but not limited to, the Health and Safety Executive, transport and utility companies. They should also be able to facilitate relationships with community responders such as the British Red Cross and search and rescue organisations, and be able to call upon support and advice from specialist national agencies such as the Met Office, Environment Agency, Natural Resources Wales, UK Health Security Agency and Public Health Wales.

142. Forces should also work closely with DLUHC Resilience Advisers and Government Liaison Officers (GLO) and military Joint Regional Liaison Officers (JRLO). When required, they should be able to collaborate with both regional and national command structures, set up through DLUHC and the Cabinet Office, including Cabinet Office Briefing Room (COBR). They should share information with these government departments on emerging risks, live incidents and any changes in their ability to manage an incident locally.

143. The post-implementation review of the Civil Contingencies Act 2004, published on 1 April 2022, provides a technical assessment of the legislative framework to ensure that it remains appropriate and sufficient in order to maintain and improve the emergency preparedness landscape. The government will engage with stakeholders, including the policing sector, to deliver the recommendations set out in the report.

Cross-Cutting Capabilities

144. Whilst the SPR treats the national threats separately, many of the threats, and the capabilities required to respond, will overlap. The capabilities listed in the preceding sections should not be considered in isolation or as the only capabilities required to respond to the national threats.

145. There are other capabilities, not explicitly mentioned in the SPR, that are threat-agnostic and have a broader role in the protection of the public or the reduction of crime. These capabilities may also be used to tackle the national threats. These include but are not limited to: intelligence capabilities such as a Force Intelligence Bureau that leads on the management, coordination, collection and development of quality intelligence; investigative capabilities such as detectives to undertake investigations both locally and in response to major crimes or incidents; and contact management technologies to efficiently and effectively respond to all reported crime and incidents of the national threats.

146. For example, National Mutual Aid Telephony (NMAT) enables police forces to publicise freephone numbers when seeking public contact in relation to major or time-sensitive cases, such as terrorist incidents or child rescue alerts. It also facilitates mutual aid by supporting force call handlers to receive calls seamlessly from the same telephone number or queues to provide capacity management. It was successfully deployed for example, to assist with the London Bridge attack in June 2017.

147. There are also some specialist capabilities that are not exclusively deployed in response to a single threat but may be required to respond to at least three of the threats listed in the SPR. The SPR covers four capabilities in detail: armed policing; digital forensics; roads policing; and Joint Emergency Services Interoperability Principles (JESIP) trained police response staff. Many forces will already maintain or collaborate on these capabilities but Chief Constables and PCCs should understand the role that these capabilities can have in responding to the SPR threats.

Armed Policing

148. There is a long-standing tradition of policing by consent in this country which is vital for promoting good relations with the public. In keeping with this tradition, not all police officers are routinely armed with firearms. Police officers are routinely equipped with a range of protective equipment, such as irritant sprays and batons, while a proportion of these officers are selected, trained and equipped with less lethal equipment such as Conducted Energy Devices (CED).[67] Less lethal equipment is also available to all Authorised Firearms Officers (AFOs). There will be times, however, when the use of firearms is required. All armed officers are generically known as AFOs regardless of additional skills or training undertaken.

149. Armed policing capabilities are built upon ongoing assessments of operational threat and risk and are used in threat to life situations, such as terrorist attacks, incidences of serious and organised crime and serious violence. They can also be deployed in support of protective security operations. The police have a legal duty to only use as much force as is reasonable and proportionate in the circumstances, and less lethal weapons can be deployed as an alternative to firearms as appropriate. The use of firearms by the police should always be the last resort, considered only where there is a serious risk to public or responder safety.

Authorised Firearms Officers (AFOs)

150. AFOs are trained to analyse and determine an appropriate course of action as part of armed deployment. All Home Office forces[68] and the Civil Nuclear Constabulary (CNC) and Ministry of Defence Police (MDP) deploy AFOs trained to provide visible protective security and deterrence in their role to protect key sites such as airports, iconic locations, the CNI etc. AFOs also provide discreet personal protection to individuals where such protection is required. Not every force will have AFOs at this level and many may only maintain armed capabilities from Armed Response Vehicles (ARVs) upwards.

[67] CED are commonly referred by their brand name, Taser. TASER X26, X2 and T7 are the only devices currently authorised for use by police forces in England and Wales.

[68] A police force maintained under section 2 of the Police Act 1996, the Metropolitan Police Service, and the City of London Police

Armed Response Vehicles (ARVs)

151. The primary armed capability at local force level is delivered by armed response vehicles (ARVs) which provide an immediately deployable conventional firearms capability as well as less lethal options. They respond to no-notice incidents and can also provide visible protection to iconic locations, the CNI or other key locations, such as higher risk publicly-accessible locations, when required.

152. Every Home Office force maintains an ARV capability, either as a single force or as part of collaborative agreements. ARV capability also exists within the British Transport Police (BTP). ARV capacity is determined at force level through an Armed Policing Strategic Threat and Risk Assessment (APSTRA). This process also establishes operational requirements for armed support within a force and the weapons and equipment that armed officers carry.

Armed Support to Surveillance and Covert Operations

153. Armed officers can also provide support to covert operations. This includes armed surveillance officers whose primary function is surveillance and more specialist armed officers, referred to as Mobile Armed Support to Surveillance (MASTS), who support surveillance operations by providing greater tactical capability.

154. The vast majority of armed support to surveillance or covert operations is delivered by MASTS. MASTS officers are trained to operate in covert vehicles, on foot and in plain clothes. Not every force maintains this capability locally and many collaborate with neighbouring forces[69].

Counter-Terrorist Specialist Firearms Officers (CTSFOs)

155. CTSFOs are the UK's most highly trained and equipped AFOs. They maintain all of the skills of SFOs but also have certain enhanced tactical capabilities. They are strategically located at "hubs" across the UK, embedded in single force areas or within collaborations. They provide local forces with specialist firearms capability under the direction of the host force or collaboration Chief Constable(s).

[69] Some Home Office forces maintain Specialist Firearms Officers (SFOs) who are trained both in MASTS and Dynamic Search. Dynamic Search is the ability of a team to rapidly enter and search a building, train etc. in order to rescue hostages, carry out arrests, or secure readily disposable evidence.

156. They can also be tasked nationally to support counter-terrorism operations or, under an NPCC memorandum of understanding, to provide a non-CT dynamic search capability.

Less Lethal Weapons

157. Less lethal weapons offer specially trained police officers with a differentiated use of force from firearms. Only less lethal weaponry that has been authorised by the Home Secretary may be used by police forces in England and Wales.[70] There are currently only two forms of less lethal weapons authorised for use by police forces in England and Wales:

157.1. Attenuating Energy Projectile (AEP) are soft-nosed projectiles fired by officers to dissuade or prevent a potentially violent person from their intended course of action, thereby neutralising the threat. Although available as a tactical option in public order scenarios, AEPs have never been used in a public order scenario by police forces in England and Wales.[71]

157.2. CED (commonly referred to as Tasers) are designed to temporarily interfere with the body's neuromuscular system. They provide an important tactical option, allowing police officers to better protect themselves and the public from harm. They are not routinely used in incidences of public disorder. All AFOs are trained in CED. The deployment of CED is determined at force level through the Strategic Threat and Risk Assessment (STRA) that should establish the number of CED and trained officers required by the force against its operational requirements.

158. All officers will also have access to personal protective equipment, including batons and hand-held irritant sprays (PAVA or CS).[72] Canisters release a liquid in a spray form to defend the user against physical attack.

[70] There is an established process for the approval of less lethal weapons which will consider the relevant strategic, ethical, operational and societal issues, including an assessment of the medical implications identified by the Scientific Advisory Committee on the Medical Implications of Less Lethal Weapons. This is set out in the Code of Practice on armed policing and police use of less lethal weapons

[71] This differs from Police Service of Northern Ireland where the provide an important tactical option in public order scenarios.

[72] These items are not classed as less lethal weapons.

Digital Forensics

159. Digital forensics involves the identification, collection, examination and analysis of electronic data in accordance with the Forensic Science Regulator's Codes of Practice and Conduct, 2020. This should be done while preserving the information's integrity to make sure it is not tampered or interfered with. The Transforming Forensics programme estimates that 90% of all crime now has a digital element meaning digital forensics has a role to play in responding to multiple threats, in particular terrorism, SOC, national cyber events and child sexual abuse.

160. Digital forensics can range from investigating activity on social media to seizing and handling of body-worn video (BWV) and CCTV footage or mobile phone information. It also includes the:

a. extraction of data (recovery) by making a copy, downloading data from a digital device or recovering data from a remote system;
b. processing data to allow an examiner to work on them. This can include decrypting data and recovering files;
c. analysis and interpretation of data involving the synthesising of information from different sources. This may require significant expertise; and
d. presentation of findings to an investigation team as a written report and, eventually, in court.

161. Forces should have access to in-house digital forensics capability delivered through forensics departments, high-tech crime units, intelligence bureau or through Scientific Support Units. Forces may opt into wider commercial contracts to support their in-house capabilities through commercial providers, either procured individually or in collaboration with others.[73] In all cases, digital forensics capability must comply with all requirements set by the Forensic Science Regulator.

[73] There are a number of collaborative commercial contacts nationally with for example the MPS and NCA. The Forensic Capability Network has developed a Dynamic Procurement System (DPS) for a wide range of Digital Forensics and related quality services. The DPS includes standardised service packages underpinned by both technical and quality standards requirement. This is available to all forces.

162. These units will be staffed by specialist and trained technicians including Digital Forensics Investigators who conduct intelligence-led digital forensic investigations.[74] They provide evidence and expert interpretation of evidence. Some roles, such as Digital Media Investigators, may sit outside of the Digital Forensics Unit (DFU). Digital forensics experts and the Forensic Capability Network (FCN) are working with the College of Policing to identify all the roles where digital forensics science is being applied across policing that sits outside of the traditional DFU support.

163. Digital forensics units will use specialised software and hardware to capture, preserve, extract, process and analyse data from a broad range of digital devices, including mobile phones, wearables such as smartwatches, a growing range of household devices and other sources such as on-board computers in cars and data from mobile phone networks, particularly cell site analysis, which determines the approximate location of a digital device at a specific time.

164. Forensic technicians may either only extract data that would also be available to the user or use a range of advanced methodologies to extract additional data, which may have been deleted by the user. Data extraction will be done on the basis of established and validated processes and technicians will document all steps and processes to ensure that results are reproducible and can be independently verified when necessary.

165. Over recent years, forces have extended their digital capabilities through the use of configured technologies such as mobile phone kiosks at police stations and at crime scenes. These technologies are used to, for example, extract data from mobile devices or other peripheries, and obtain early evidence to support initial and emerging investigations. Many similar CCTV, social media and internet investigations form part of day-to-day police enquiries and volume crime investigations.

Roads Policing

166. Roads policing is responsible for the enforcement of traffic laws, detection, deterrence and the response to illegal or dangerous activity on the roads. The UK

[74] There is variation in the staffing structures of DF units with management posts in some units being held by warranted officers or police staff in others.

Road network is the primary transportation method for people carrying out a range of illegal and high-risk activities and is an enabler of the threats outlined in the SPR.

167. Roads policing capabilities play an essential role in tackling the use of the roads network by terrorist threats and serious and organised criminals involved in county lines drug transportation, modern slavery and human trafficking. They are also essential in managing incidents caused by public disorder or civil emergencies.

168. The NPCC has developed the National Roads Policing Strategy (2022/25)[75] which has four key pillars of activity, based around the key principle of 'Policing our roads together'. These are to; prevent harm and save lives, tackle criminality, drive innovation and technology and change minds. The strategy has been widely consulted upon prior to publication. There is a degree of national coordination of roads policing enforcement activity through the NPCC calendar of National Roads Policing Operations, such as tackling drink and drug driving, however most coordination is locally driven.

169. The road network is an element of CNI. Forces should have, or have access to, sufficient roads policing capabilities to protect against, or respond to, threats against this infrastructure. There is no singular model for roads policing units in police forces. Roads policing roles range from dual role officers to dedicated specialists, and there are varying roles within roads policing, such as commercial vehicle units.

170. Locally-maintained capabilities have an important role to play in effective roads policing and officers and staff should have the requisite procedural knowledge and training to meet these objectives including:

a. advanced driving capabilities including pursuit management, tactical pursuit and containment tactics (TPAC), and police motorcyclist capability;
b. management of incidents including large scale collisions, public disorder, and civil emergencies;

[75] https://www.police.uk/SysSiteAssets/media/downloads/central/advice/road-safety/npcc-roads-policing-strategy-2022-25.pdf

c. forensic collision investigative capabilities (accredited to Forensic Science Regulator standards) to provide valuable technical assistance to investigations. Examples include interpreting vehicle data and laser scanning crime scenes;
d. legislative knowledge relating to commercial vehicles, including HGVs and the transportation of dangerous goods. Increasingly forces are seeing a link between organised crime, including the transportation of drugs and human trafficking, and the use of commercial vehicles; and
e. roads enforcement skills such as the ability to understand tachograph data on driving time, speed and distance which can inform criminal investigations and identify significant locations of interest.

171. Forces should also have, or have access to, relevant technology, software, and equipment to execute roads policing capabilities including:
a. protective equipment, such as clothing, signage, and the appropriate vehicles for fast roads response and pursuits; and
b. Automatic Number Plate Recognition (ANPR) infrastructure through the National ANPR Service (NAS) to help detect, deter and disrupt criminality at a local, regional and national level. Enhanced data analysis using ANPR enables police to proactively target vehicles suspected of being used in criminality particularly when detecting and preventing cross-border criminality such as county lines activity.

172. Intelligence gathered from ANPR will be supplemented by a high level of routine operational activity, including through traffic stops which provide an opportunity to gather intelligence through overt activity.

173. Aggregating specialist enforcement skills, such as expertise in dangerous goods, within collaborations and collaborating with other agencies such as National Highways, the Driver and Vehicle Licensing Agency (DVLA) or the Driver and Vehicle Standards Agency (DVSA) has enabled some forces to effectively tackle organised crime and terrorism threats.

The Joint Emergency Services Interoperability Principles (JESIP)

174. The JESIP should form the foundation of all joint working between police forces and the other emergency services. Chief Constables, alongside the NPCC lead, should ensure JESIP, as set out in the Joint Doctrine, is embedded in all response policies, plans and procedures so it can be applied at every incident type. JESIP training should be provided for all levels of response staff, this should be continually refreshed and embedded into joint testing and exercising programmes with the other emergency services.

175. The JESIP Joint Doctrine: The Interoperability Framework[76], provides guidance on the actions that should be taken when responding to multi-agency incidents and contains the principles for joint working. These are:

a. **Co-locate** with commanders as soon as practicably possible at a single, safe and easily-identified location near to the scene.
b. **Communicate** clearly using plain English.
c. **Co-ordinate** by agreeing the lead service. Identify priorities, resources and capabilities for an effective response, including the timing of further meetings.
d. **Jointly understand risk** by sharing information about the likelihood and potential impact of threats and hazards to agree potential control measures.
   Shared Situational Awareness established by using M/ETHANE and the Joint-Decision Model[77]

[76] The Joint Doctrine: The Interoperability Framework – Edition 3 (published October 2021). https://www.jesip.org.uk/downloads/joint-doctrine-guide/

[77] The M/ETHANE model helps all agencies gather information about an incident in a consistent manner and is now the recognised model for passing incident information between services and their control rooms. The Joint-Decision Model is used by commanders to help bring together the available information, reconcile objectives and make effective decisions