National Policing Requirement

2012

Contents

National Policing Requirement

Chapter 1

National Policing Requirement for the Strategic Policing Requirement

1.1 Strategic Policing Requirement

1.1.1 The Strategic Policing Requirement (SPR) supports chief constables and police and crime commissioners to ensure they fulfil forces' national responsibilities for tackling criminal or terrorist threats and harms, or other civil emergencies.

1.1.2 Threats have been assessed and selected from the National Security Risk Assessment on the basis that they either affect multiple police force areas or may require action from multiple forces, resulting in a national response. While treated separately, many of these threats overlap.

1.1.3 The identified threats are:

- public disorder
- civil emergencies
- organised crime
- terrorism
- large-scale cyber incidents.

1.2 National Policing Requirement

1.2.1 As part of the response to the SPR, a national document is needed which details the capacity and contribution, capability, consistency and connectivity required to counter the identified threats.

Planning Assumptions

1.2.2 Planning assumptions have been drawn from government and strategic documents to provide an appropriate policing response to the threats and prepare for the most serious threats. Planning assumptions are statements of the challenges the Police Service and other agencies believe they need to prepare for, based on intelligence and risk assessments. While these statements are not exhaustive, they do reflect current and ongoing concerns relating to threat, risk and harm.

1.2.3 The planning assumptions for some areas of policing, such as public order and civil contingencies, are formulated on the basis that these

events require a response which is predominantly reactive (regardless of whether the event is spontaneous or pre-planned). Planning is based on the threat of scenarios occurring, and this determines the appropriate policing response in terms of the number and type of resources required.

1.2.4 Planning assumptions for serious and organised crime and counter terrorism, on the other hand, are based on threats posed on a constant basis. This means there is a need for dedicated resources working proactively to mitigate the threats. Planning is based on the:

- volume of the demand
- need for a response
- likelihood and consequences of the threat posed
- number and type of resources required to manage it.

1.2.5 The planning assumptions are used to outline the capacity and contribution, capability, consistency and connectivity that forces require to counter each of the threats.

Capacity and Contribution

1.2.6 Police and crime commissioners and chief constables should have regard to the planning assumptions and ensure they are able to fulfil their force's contribution to the national capacity in response to threats, harms and other civil emergencies.

Capability

1.2.7 The Police Service should be capable of meeting the National Policing Requirement. Consideration should be given to the skills, training and equipment required, ensuring each force's contribution to the national requirement is effective.

Consistency

1.2.8 Specialist policing capabilities must be able to deliver an integrated response which is consistent across all police forces and partnership agencies.

Connectivity

1.2.9 Policing resources need to be connected effectively across force boundaries through national arrangements. Policing capabilities should also be able to connect effectively with key partners when planning for, and responding to, civil emergencies.

1.3 Summary

1.3.1 The purpose of this National Policing Requirement is to inform chief constables and police and crime commissioners of the facts required to plan effectively for challenges that go beyond their force boundaries.

1.3.2 They are advised to take into account the professional assessments outlined by the Police Service in this document when considering the appropriate policing response, and not depart from the requirements without good reason.

1.3.3 Police and crime commissioners and chief constables should have regard to the SPR and this document when issuing or varying their local Police and Crime Plans. This National Policing Requirement is a living document that will be subject to annual review.

Chapter 2

Supporting Elements for the National Policing Requirement

2.1 Overview

2.1.1 This chapter summarises a number of aspects and functions which support the National Policing Requirement. These are applicable across all of the threats outlined and are included to provide clarity and avoid duplication.

2.2 The College of Policing

2.2.1 The College of Policing operates independently of the government and has taken on the functions of the National Policing Improvement Agency (NPIA) relating to learning, development, specialist training and leadership.

2.2.2 In line with the National Policing Requirement, the College of Policing will:

- **provide** the Police Service with **consistency** by promoting standards of professionalism, education and professional development
- **strive** to improve **connectivity** by developing interoperability with partners and other sectors
- **continue** to develop and improve the **capabilities** required by the Police Service to deal with evolving threats to public safety.

2.2.3 Authorised Professional Practice (APP)[1] has consolidated policing guidance into a single, interactive, online format. It gives instant access to authorised knowledge and the ability to see how guidance links across areas of policing. APP significantly reduces the volume of national guidance in circulation, encourages the use of professional discretion and brings consistency to all authorised police practice.

2.2.4 APP describes areas of police practice which have cross-cutting themes and processes applicable across all policing disciplines. These are:

- investigation
- intelligence management
- information management

[1] For further information, email <APP.contact@college.pnn.police.uk>.

- operations
- engagement and communications
- prosecution and case management
- detention and custody
- decision making.

2.2.5 APP also addresses specific areas of practice that require additional national standards for reasons of high risk, interoperability and partnership working. Examples include:

- CBRN (chemical, biological, radiological and nuclear)
- civil contingencies
- covert surveillance
- armed policing
- mobilisation
- organised crime
- public order.

2.2.6 Capability frameworks have been created and are in the process of being developed in support of APP. These frameworks are owned and developed by the portfolio leads with the assistance of the College of Policing. They encourage forces to complete self assessments against criteria to ascertain their effectiveness in terms of business and operational delivery.

2.3 Local Policing

2.3.1 Localism forms the bedrock of policing, with local policing ensuring that communities have reassurance and confidence in the Police Service. Local policing is also an essential element in protecting the public from the national harms and threats outlined in the SPR.

2.3.2 Organised criminals, terrorists and civil emergencies are not confined to force boundaries. A significant component for tackling these cross-boundary issues is provided by:

- intelligence and information provided at a local level
- strong local partnerships and community relationships
- the early intervention and proactive action taken by local policing officers.

2.4 Coordination of Resources

2.4.1 National coordination of police resources is currently undertaken by the ACPO Police National Information and Coordination Centre (PNICC). PNICC coordinates the mobilisation of police officers and staff in times

of national and international demand, whether to support pre-planned or spontaneous events.

2.4.2 PNICC collects and holds force data about the location and number of specialist resources available to provide a national oversight of capability. When demand exceeds the capacity of a force or region, PNICC assist in coordinating support and further resources.

2.4.3 PNICC collates information about events of national significance and ensures that ACPO and central government have reporting mechanisms to ensure effective oversight and briefing.

2.4.4 Resource mobilisation is fundamental to delivering an effective response to the threats set out in the SPR. A recent review[2] of ACPO operational activity by Her Majesty's Inspectorate of Constabulary (HMIC) highlighted a number of recommendations to improve the function of PNICC. It is acknowledged that PNICC was designed for other circumstances. The report recommends a preferred option based on an adaptation of the strong mechanisms established for the Olympic Games, and suggests the development of a National Policing Coordination Centre (NPoCC). Further work is ongoing to outline the potential resource structure, core functions and governance of this new centre.

2.4.5 Some specific functions also exist in support of PNICC. During the early stages of a CBRN event, CBRN capability is coordinated through the Police National CBRN Centre, and national coordination for counter terrorism is delivered by the ACPO Counter Terrorism Coordination Centre (ACTCC). Where capacity exceeds the capability of the ACTCC, PNICC is required to support ACTCC functions. It does this by identifying and coordinating resources such as officers trained in counter terrorist searching and BDU (basic deployment unit) officers who can police cordons.

2.5 Overlapping Threats

2.5.1 The five threats listed in the SPR are inextricably linked, meaning they should not be considered in isolation. It is conceivable that a large-scale civil emergency results from a cyber incident instigated by a terrorist act. This would require a national, multi-agency response and call on many of the skills mentioned within the chapters of this document. For example, public order officers and partner agencies might be required to respond to the civil emergency to maintain order and aid a return to normality, while the specialist capabilities of cyber,

[2] Sir Denis O'Connor and Sir David Omand – 'Protecting the Public: Police coordination in the new landscape'.

counter terrorism and serious and organised crime officers might be required to investigate the incident fully and prevent a reoccurrence.

2.6 Multi-Skilled Officers

2.6.1 Due to the large degree of overlap between the threats set out in the SPR, police forces need to take into account the fact that there are officers who hold multiple skills. For example, officers trained in public order are often also trained to deal with CBRN incidents as well as being skilled in counter terrorist searching. Forces should, therefore, consider multi-skilled officers when calculating their capacity to contribute to the National Policing Requirement and their own local resilience to deal with the threats outlined. Forces are advised to train sufficient resources to achieve their contribution and allow for anticipated abstractions through annual leave, sickness, training and other commitments such as court attendance.

2.7 Her Majesty's Inspectorate of Constabulary (HMIC)

2.7.1 HMIC is independent of the government and the police. It assesses police forces across a wide range of aspects, from neighbourhood policing teams to serious crime and the fight against terrorism. The results of HMIC inspections are available to the public. This allows comparison of force performance against others and drives improvements in the quality of service delivered to the public. It is expected that HMIC will provide assurance that the preparation and delivery of the requirements set out in the SPR have been subjected to a proportionate and risk-based testing and inspection regime[3].

[3] See paragraph 1.15 of the Strategic Policing Requirement.

Chapter 3

National Requirements for Public Order

3.1 Overview

3.1.1 The primary objective in policing public order situations is to keep the Queen's peace and preserve order using the minimum force necessary. The Police Service supports peaceful protest and neighbourhood policing provides the bedrock for this. However, the Service has a duty to protect the public, prevent criminality and preserve life and property, taking appropriate action as disorder escalates, and proactive measures when required. This approach is supported by relevant legislation and guidance, such as APP[4] and the National Public Order Framework[5].

3.1.2 The Service provides policing with impartiality, transparency and empathy. Public confidence in the police's ability to maintain order is essential. The police must consider the legitimacy and proportionality of tactics when dealing with any threat posed.

3.1.3 The National Decision Model (NDM)[6] provides structure, clarity and rationale for decisions about deploying assets proportionately and effectively in response to any public order or public safety event.

3.1.4 Threats to public order come from a number of sources. These are identified primarily through the National Domestic Extremism Unit's[7] Strategic Threat Assessment and the National Public Order Strategic Threat and Risk Assessment[8]. Effective monitoring of community tension that may escalate into disorder is crucial to these assessments.

3.1.5 Mutual aid provision for public order policing has developed over the years and is based on practical experiences from many events including G20, English Defence League (EDL) protests and the national disorder of August 2011.

3.1.6 While many public order events are pre-planned, exceptional public order demands may emerge with little notice and the Police Service needs to retain the capacity and capability to respond to such spontaneous events.

---

[4] Authorised Professional Practice – for further information, email <APP.contact@college.pnn.police.uk>.
[5] To request access to the National Public Order Framework, email <acpopops@kent.pnn.police.uk>.
[6] See <http://www.acpo.police.uk/documents/president/201201PBANDM.pdf>.
[7] See <http://www.acpo.police.uk/NationalPolicing/NationalDomesticExtremismUnit>.
[8] To request access to the National Public Order Strategic Threat and Risk Assessment, contact ACC McCormick Cheshire.

3.2 Planning Assumptions

3.2.1 The Police Service should be prepared to deal with three separate seats of significant disorder simultaneously for a period of seven days within the UK. This planning assumption is based on information and experience of historical events (eg, G8, G20, EDL), and is reinforced by the disorders of August 2011, when significant disorder occurred across the major cities of London, Birmingham and Manchester. Historical experience is also supported by annual strategic threat and risk assessments, academic research and socio-economic assessments.

3.3 Capacity and Contribution

3.3.1 A national capacity of public order assets is required in order to meet the aforementioned planning assumption. This capacity is set at 297 police support units (PSUs)[9] available nationally for mutual aid deployments, with a specific contribution defined for each force and region. A PSU comprises 1 inspector, 3 sergeants and 21 police constables, trained to Tactical Level 2[10].

3.3.2 Each force's contribution to the national mutual aid capacity of 297 PSUs is defined by the Public Order Mobilisation Formula[11]. This formula was devised by the ACPO lead for Public Order and Public Safety and reviewed based on the disorders of August 2011 to enable a regional mobilisation plan to be developed. This plan sees forces initially requesting mutual aid from their regional colleagues before escalating to other neighbouring regions through PNICC[12] if the disorder develops beyond their own capabilities. The aggregate regional resource establishment (based on the 2015 forecast establishment figures from the Comprehensive Spending Review) is used to define the number of PSUs that each force has agreed to contribute (regional establishment of <15,000 = 6.5% of force establishment; regional establishment of >15,000 = 7.5% of force establishment).

3.4 Capability

3.4.1 In training sufficient resources, forces should consider the need for a local public order capability in addition to their contribution to the national mutual aid capacity.

---

[9] For further information, email <acpopops@kent.pnn.police.uk>.
[10] As defined in the National Public Order Training Curriculum.
[11] The Public Order Mobilisation Formula is currently in draft form awaiting consultation – for further information, email <acpopops@kent.pnn.police.uk>.
[12] Likely to become the National Policing Coordination Centre as outlined in the Independent Review of ACPO Operational Activity.

3.4.2 Forces are advised to complete annual public order threat and risk assessments. These contribute to regional threat assessments which, in turn, contribute to the national public order threat and risk assessment. Assessing local community tension should form part of this process. Forces need to have capabilities to gather, assess and disseminate public order intelligence effectively.

3.4.3 Forces need to have sufficient equipment to support the deployment of their national mutual aid PSUs. This includes a sufficient fleet of public order authorised carriers and other basic equipment (eg, shields, personal protective equipment and radios)[13].

3.4.4 Other specialist officers and assets are required to deliver the most proportionate policing response to the threats posed by pre-planned or spontaneous public disorder events. Forces should have a capability to provide these. Examples include:

- evidence gatherers
- medics
- AEP (attenuating energy projectile) trained officers
- dogs
- mounted police
- firearms officers
- tactical advisors[14].

3.4.5 Forces and regions need to be capable of mobilising their PSU resources spontaneously in line with the National Public Order Mobilisation plan[15]. The plan has three tiers of response:

- Tier 1 – local mobilisation
- Tier 2 – regional mobilisation
- Tier 3 – national mobilisation.

The plan also sets out timescales for deployments:

- 10% of national requirement within one hour
- 40% of national requirement within four hours
- 60% of national requirement within eight hours.

Close liaison with PNICC is fundamental to the plan. PNICC keeps track of the location of specialist policing assets nationally and is crucial to mobilising mutual aid resources for pre-planned operations.

[13] Defined in Module G3 of the National Public Order Training Curriculum.
[14] Outlined in the National Public Order Training Curriculum.
[15] To request access, email <acpopops@kent.pnn.police.uk>.

3.4.6 The capability of forces to mobilise PSU resources should be tested on a regular basis. ACPO and PNICC have developed a national mobilisation testing and exercising plan.

3.4.7 Forces need to have sufficient accredited public order commanders at gold, silver and bronze level to ensure public order operations are commanded only by these officers[16].

3.4.8 Forces should possess the capability to undertake effective briefing and debriefing for public order operations. Forces are advised to establish processes for engaging with communities and the media. Forces should also ensure that best practice and any lessons identified are shared externally.

3.4.9 Forces need to have sufficient capability to complete complex investigations following public order incidents and have effective criminal justice processes to ensure that offenders are brought to justice.

3.4.10 The portfolio lead, in conjunction with the NPIA, has developed a detailed force capability framework for public order[17]. Collaborative arrangements between forces or with external partners will provide the most effective and efficient means for establishing many of these force capabilities.

3.5 Consistency

3.5.1 The National Public Order Training Curriculum[18] outlines the national training requirements that forces need to meet to ensure consistency in tactics across force boundaries. The governance of this document will naturally fall within the new College of Policing. Forces need to ensure that all their PSU resources (including gold, silver and bronze commanders) are trained in accordance with this curriculum and the national standards outlined in it. The standards and quantity of public order equipment (eg, carriers and shields) are also defined in the document and forces need to ensure that their equipment is compliant.

3.5.2 Forces are assessed regularly to ensure that they are fully compliant with these national standards for public order. This assessment was previously undertaken by NPIA and it is envisaged that it will fall under the remit of the new College of Policing.

[16] In accordance with the APP module on command and control and the National Public Order Training Curriculum.
[17] To request access, email <acpopops@kent.pnn.police.uk>.
[18] To request access, email <acpopops@kent.pnn.police.uk>.

3.5.3 Forces should refer to APP for overall guidance on public order policing. APP identifies six core principles and command considerations for public order:

- policing style and tone
- communication
- use of the NDM
- command
- proportionate response
- capacity and capability.

The APP for public order also includes guidance on:

- the legal framework
- planning and deployment
- partnership working and communication (eg, crowd engagement)
- tactical options (eg, dogs and mounted tactics)
- variations for Northern Ireland and Scotland
- PSU commitments for mobilisation
- public safety policy
- football policing.

3.5.4 Effective joint working between the emergency services and other organisations during any emergency is important. The new Joint Emergency Services Interoperability Programme (JESIP)[19] has been established to ensure that the 'blue-light' services are trained and exercised to work together as effectively as possible in response to a major incident (including fast-moving terrorist scenarios) so that as many lives as possible can be saved. This two-year programme of work will develop joint training for commanders, joint operating principles, joint testing and exercising. Forces should engage and cooperate with JESIP to improve connectivity across the emergency services.

3.6 Connectivity

3.6.1 Forces need to be connected effectively to ensure that public order intelligence and community tension products are captured and shared regionally and nationally through tasking and co-ordination processes. In the future this should include information sharing with other emergency services to enable an effective joint response to major incidents of disorder[20].

[19] For further details, contact the ACPO lead for Interoperability.
[20] As outlined in JESIP.

3.6.2 Forces should cooperate with PNICC to guarantee effective cross-boundary mobilisation of public order resources for both pre-planned and spontaneous events.

3.6.3 Forces need to follow guidance on police interoperability[21] and cooperate with partners (eg, the Fire and Rescue and Ambulance Services)[22] to ensure connectivity during major public order incidents.

[21] As outlined by the ACPO UKOI Working Group.
[22] As outlined in JESIP.

Chapter 4

National Requirements for Civil Emergencies

4.1 Overview

4.1.1 The Civil Contingencies Act 2004[23] places a legal responsibility on the Police Service, as Category 1 responders[24], to provide an appropriate response to emergencies. An emergency is defined under the Act as a situation or series of events that threatens or causes serious damage to human welfare, the environment or security in the UK.

4.1.2 Within the National Security Strategy[25], civil emergencies are assessed as Tier 1, 2 and 3 risks. Tier 1 risks are judged to be the highest priorities for UK national security over the next five years, taking into account both their likelihood and impact.

4.1.3 In the context of civil emergencies, risks are broken down into threats (intentional) and hazards (naturally occurring). The threat and risk assessments for civil emergencies are based on a combination of responses from a range of government departments and are not police owned.

4.1.4 The National Security Risk Assessment (NSRA) builds on the classified National Risk Assessment (NRA). Priorities for emergency planning at the national level are determined by the NRA. This document identifies the main risks facing the UK and assesses their relative likelihood and potential impact using historical information, scientific data and professional judgements. The NRA is classified as SECRET and held by the police on behalf of the Local Resilience Forum (LRF). Together with local risk assessment guidance, the NRA guides LRF members in developing local risk assessments. The National Risk Register (NRR)[26] is a publically-available declassified version of the NRA. It is designed to encourage individuals, businesses, communities and organisations to think about their own preparedness.

4.1.5 Common consequences of the risks identified in the NRA are distilled in the National Resilience Planning Assumptions. These assist government contingency planning for civil emergencies by indicating the most extreme level of each consequence. They also provide

[23] See <http://www.opsi.gov.uk/acts/acts2004/ukpga_20040036_en_1>.
[24] The Civil Contingencies Act (2004) defines Category 1 responders as organisations at the core of the response to most emergencies (eg, emergency services, local authorities).
[25] See <http://www.direct.gov.uk/prod_consum_dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy>.
[26] See <https://update.cabinetoffice.gov.uk/sites/default/files/resources/CO_NationalRiskRegister_2012_acc.pdf>.

guidance to local planners on the types of common consequences they should consider.

4.1.6 Local responders are expected to be the building blocks of response for an emergency of any scale. Most arrangements for this are delivered through an LRF that shares boundaries with police forces. Successful functioning of the LRF is fundamental to achieving interoperability between emergency responders.

4.1.7 The UK Central Government Concept of Operations[27] identifies three stages in the management of any emergency:

- **preparation** – pre-planning
- **response** – containing the emergency and mitigating its impacts
- **recovery** – a longer-term activity of rebuilding, restoring and rehabilitating the community.

4.1.8 History has taught us to expect the unexpected. Events can and do take place that, by their nature, cannot be anticipated exactly. Response arrangements need to be flexible in order to be able to adapt to the circumstances at the time.

4.2 Planning Assumptions

4.2.1 At the national level, the Police Service should be prepared to deal with a major accident or natural hazard which requires a national response. Examples include severe coastal flooding affecting three or more regions of the UK, or an influenza pandemic. This planning assumption is based on those civil emergencies assessed as a Tier 1 risk in the NSRA.

4.3 Capacity and Contribution

4.3.1 A national capacity of skilled assets is required in order to meet the aforementioned planning assumption. Police forces should be in a position to contribute to the following:

- PSUs
- BDUs[28]
- CBRN response
- disaster victim identification (DVI)
- casualty bureau resources.

[27] See <http://www.cabinetoffice.gov.uk/sites/default/files/resources/conops-2010.pdf>.
[28] Basic deployment units – used at the 2012 Olympics and consisting of 1 inspector, 3 sergeants and 21 police constables who are non-PSU staff.

Forces should also be able to contribute to appropriate command structures at gold, silver and bronze levels.

4.3.2 The national PSU capacity is set at 297[29] and this is a valuable resource that can be used in support of civil emergencies. However, not all emergencies will require public order skilled officers and thus forces should also have the capacity to provide BDUs, where appropriate, and at the request of PNICC.

4.3.3 The current capacity for CBRN[30] is set at 8475 trained officers, which equates to 339 PSUs. A review by the Office of Security and Counter Terrorism is currently underway to re-examine the threat and risk of CBRN incidents and the appropriate policing response[31].

4.3.4 Regional arrangements ensure that there is national resilience to provide casualty bureau capacity. Forces contribute to these arrangements, whether based on lead force or collaboration agreements. Forces are also required to have a local casualty bureau capacity which can be maintained 24/7 for a period of up to one week[32].

4.3.5 Forces are requested to have the capacity to provide DVI officers with specialist skills to deal with non-contaminated fatalities on a proportionate basis. The ACPO DVI strategy 2008 to 2013 provides national capacities for each specialism. This is subject to a post-Olympics review.[33]

4.3.6 Forces are also requested to contribute to the national capacity of DVI officers with additional training to enable them to work in a CBRN environment involving contaminated fatalities. Currently this is defined as 96 trained officers across the UK, however, further modelling is required to ensure that this capacity is sufficient[34].

4.3.7 There is a requirement for forces to contribute to the PNICC rota for the potential deployment for DVI officers overseas. They should also have sufficient capacity for the crucial senior identification manager (SIM) role.

[29] For further details on PSU numbers, see chapter 3.
[30] For further details on CBRN capabilities, see chapter 6.
[31] For further details contact the ACPO lead for CBRN.
[32] For further details contact the ACPO lead for DVI.
[33] For further details contact the ACPO lead for DVI.
[34] For further details contact the ACPO lead for CBRN.

4.4 Capability

4.4.1 As Category 1 responders to civil emergencies, the Police Service is subject to the Regulations described in Part 1 of the Civil Contingencies Act 2004.

4.4.2 Through the LRF mechanism, forces will assess the risk of emergencies occurring and use this information to inform the community risk register and contingency planning as well as support multi-agency co-operation. Each LRF will have arrangements in place to deal with civil emergencies.

4.4.3 Through LRFs, forces should collectively exercise emergency plans and implement lessons learnt from exercises, emergencies, and emerging policy.

4.4.4 Forces should participate in strategic co-ordination groups and ensure that they have accredited gold commanders[35] available to act as chair when appropriate. Forces should also participate in regional co-ordination groups, if instigated.

4.4.5 Forces need to have local plans for preventing emergencies and reducing, controlling or mitigating the effects of emergencies, including contingency planning.

4.4.6 Arrangements should be in place within forces to make information available to the public about civil protection matters. Forces are also advised to have a strategy for communicating internally and externally, with partners, the community and the media during emergencies.

4.4.7 Forces should ensure business continuity management processes are in place so that, as far as reasonably practicable, all functions can continue in the event of a large-scale civil emergency.

4.4.8 Forces should have capabilities to gather, assess and disseminate information and intelligence related to civil emergency threats and hazards effectively. These should be shared with other forces and other local responders through LRFs.

4.4.9 Forces should have sufficiently accredited and trained staff in relation to PSU, CBRN, casualty bureau and DVI commitments. Casualty bureau staff should be trained to a common minimum national standard[36] and forces should ensure the required number of NMAT2 telephone lines are in place in preparation for any activation[37]. DVI

[35] See Authorised Professional Practice for further information on gold command.
[36] This is a work in progress – the 2012 DVI budget has funded the Casualty Bureau Steering Group to define this and develop a requirement on behalf of the DVI ACPO lead. This work is due in April 2013.
[37] For further details contact the ACPO lead for DVI.

staff should be trained to NPIA Foundation Level (mortuary and body recovery)[38] and this training is licensed to be delivered by lead forces. All SIMs should have completed the NPIA SIM training programme. There is an expectation that this training will migrate over to the College of Policing in due course.

4.4.10 To achieve their contribution, forces should ensure that they train sufficient resources to allow for anticipated abstractions through annual leave, sickness, training and other commitments. This includes ensuring sufficient commanders are accredited to undertake the critical incident command role at gold, silver and bronze level. Forces need to ensure that they have sufficient equipment to support the deployment of their mutual aid resources.

4.4.11 Forces should have a capability to provide effective scene preservation and provide assistance to Her Majesty's Coroner in the event of a civil emergency resulting in mass fatalities.

4.4.12 The national coordination of force assets is conducted through PNICC. Forces need to be capable of mobilising their resources promptly when requested. PNICC will assist with the coordination of mutual aid to forces nationally, but also with the deployment of staff internationally, should the circumstances require it. Forces should also produce their own mobilisation plans in the case of civil emergency. The capability of forces to mobilise should be tested on a regular basis.

4.4.13 Capability frameworks for civil emergencies have been developed by the portfolio leads and these reflect the national policing requirements. Many of these force capabilities will be realised through collaborative arrangements between forces or with other external partners.

4.5 Consistency

4.5.1 Forces should refer to APP[39] for overall guidance when dealing with civil emergencies. APP ensures a consistent approach to the way forces train and respond to civil emergencies, and provides specific guidance on:

- emergency procedures
- casualty bureau
- DVI
- police mobilisation
- CBRN response.

[38] Accreditation will move to the College of Policing.
[39] Authorised Professional Practice – for further information, email <APP.contact@college.pnn.police.uk>.

4.5.2 Effective joint working between the emergency services and other organisations during any emergency is important. The new Joint Emergency Services Interoperability Programme (JESIP)[40] has been established to ensure that the 'blue-light' services are trained and exercised to work together as effectively as possible in response to a major incident (including fast-moving terrorist scenarios) so that as many lives as possible can be saved. This two-year programme of work will develop joint training for commanders, joint operating principles, joint testing and exercising. Forces should engage and cooperate with JESIP to improve connectivity across the emergency services.

4.5.3 The LRF provides multi-agency strategic direction to civil protection planning at the local level to ensure local preparedness for emergencies. This includes shared risk assessment, joint planning and the testing and exercising of those plans.

4.5.4 The National Decision Model (NDM)[41] provides structure, clarity and rationale for decisions about deploying assets proportionately and effectively in response to any civil emergency. Applying the NDM will ensure that dynamic risk assessments are used in an appropriate and timely manner.

4.6 Connectivity

4.6.1 Forces should cooperate with PNICC in the event of a Tier 1 emergency, ensuring that police resources can be mobilised across force boundaries and internationally, if required.

4.6.2 To ensure connectivity, all blue-light services and partnership agencies should be able to communicate with each other at the scene of a civil emergency. It is vital that forces follow guidance on police interoperability and cooperate with partners to manage risk, reduce harm and save lives[42].

[40] For further details contact the ACPO lead for Interoperability.
[41] See <http://www.acpo.police.uk/documents/president/201201PBANDM.pdf>.
[42] As outlined in JESIP Appendix 2.

Chapter 5

National Requirements for Serious and Organised Crime

5.1 Overview

5.1.1 Serious and organised crime (SOC) includes a wide variety of activities, ranging from the illegal supply of commodities, to fraud and violence in multi-billion pound enterprises. These activities not only destroy lives, harm communities and damage businesses, but they also impact significantly on public finances.

5.1.2 In addition to the visible and direct impact, there are significant consequential impacts on other public services such as education, health and social services. In financial terms, the cost of SOC to the UK is estimated to be up to £40 billion per year.

5.1.3 This impact on the UK means that SOC is graded as a Tier 2 national security risk in the National Security Strategy and the Strategic Defence and Security Review[43].

5.1.4 The UK Threat Assessment[44] and the National Security Threat Assessment[45] describe the threat to the UK from SOC as significant. This is based on information and intelligence drawn from a wide range of sources both in the UK and abroad.

5.1.5 The current, key SOC threats identified in the UK Threat Assessment are:

- trafficking of controlled drugs
- organised immigration crime
- financial crime (fraud)
- organised acquisitive crime.

5.1.6 The organised crime strategy 'Local to Global'[46] sets out the government's comprehensive plan for combating organised crime from 2011 to 2015. Its publication fulfilled a commitment made in the Strategic Defence and Security Review and is of fundamental importance to the approach in fighting crime. The aim of the

[43]The National Security Strategy (NSS) <http://www.direct.gov.uk/en/Nl1/Newsroom/DG_191679> and the Strategic Defence and Security Review (SDSR) were published in October 2010 <http://www.direct.gov.uk/en/Nl1/Newsroom/DG_191706>.
[44] This assessment is published annually and is a RESTRICTED document for law enforcement agencies.
[45] See <http://www.official-documents.gov.uk/>.
[46] See <http://www.homeoffice.gov.uk/crime/organised-crime-strategy/>.

organised crime strategy is to reduce the risk to the UK and its interests from organised crime by suppressing the threat from organised criminals and reducing vulnerabilities and criminal opportunities. The organised crime strategy has three key objectives, to:

- **stem** the opportunities for organised crime to take root
- **strengthen** the law enforcement response
- **safeguard** communities, businesses and the state.

5.1.7 The strategy places emphasis on the prevention of organised crime and ensures that prosecution and disruption activity takes place against organised criminals, at a reduced cost.

5.1.8 All regions have now developed regional organised crime units (ROCUs) and, while these vary in their capacity, capability and strategic approach, they all provide an operational policing platform beyond the local level and in support of national agencies. Generally the teams provide a range of specialist operational, surveillance, covert and technical functions, all of which are required to attack the most problematic organised offenders successfully.

5.1.9 In 2013 the National Crime Agency (NCA) will be established to spearhead a national crime-fighting response to SOC. The NCA will consist of four commands which will cover:

- organised crime
- border crime
- fraud and cyber crime
- protection of children and young people.

The NCA will enable the work of law enforcement and intelligence agencies to become increasingly coordinated, effective and efficient.

5.2 Planning Assumptions

Four high-level planning assumptions have been defined:[47]

- ongoing drivers of organised crime
- the means by which organised crime is facilitated
- convergence of threats
- interdependencies/issues that affect our response.

[47] See paragraphs 34-46 of the 'Local to Global' strategy – <http://www.homeoffice.gov.uk/publications/crime/organised-crime-strategy>.

Ongoing Drivers of Organised Crime

5.2.1 Organised crime groups (OCGs) operate across traditional police and agency boundaries and criminal justice jurisdictions, both nationally and internationally and on a continuous basis without reprieve. They operate for financial gain and/or social recognition, dealing in illicit goods and services, and in the process harm businesses and the economy. People from deprived communities are at a greater risk of becoming involved in organised crime than those who are not and, as a result, OCGs direct their operations in areas of instability and conflict. OCGs use high levels of violence and continue trafficking immigrants.

The Means by which Organised Crime is Facilitated

5.2.2 OCGs will become more interconnected in carrying out their trade in goods, services and capital through the use of technology. They are able to collaborate effectively and adapt their operations, exploiting perceived opportunities and weaknesses. OCGs seek to create, exploit and influence links to law enforcement, legal professions and the private sector.

Convergence of Threats

5.2.3 There is potential convergence between the threats posed from organised crime and those posed from counter terrorism.

Interdependencies/Issues that Affect our Response

5.2.4 Organised crime is a global problem as well as a local one. It requires cooperation and engagement between national and international partners as well as those with a reach into local communities. A multi-agency response is needed to combat the threat posed by organised crime.

5.3 Capacity and Contribution

5.3.1 The capacity and contribution delivered by each force against the threat posed by SOC differs for each region, preferred partnership or multi-force collaboration. Their functionality should have a capacity and capability commensurate to the threat presented by SOC. This is a strategic issue which needs to be considered by chief constables and police and crime commissioners when looking at the tactical options available to tackle the threat.

5.3.2 The threat from organised crime is managed operationally through the Integrated Operating Model (IOM)[48]. The IOM enables UK law enforcement agencies to evaluate and tackle organised crime effectively as well as:

- increase their knowledge
- improve their understanding
- provide a coordinated response.

The IOM describes the capabilities, capacity, systems, processes and standards required by all policing, law enforcement agencies and partners to ensure that the total threat from SOC is identified, assessed, managed and coordinated effectively.

5.3.3 There are three parts to the IOM:

- **the structure or framework** on which it hangs, ie, national (NCA/SOCA), regional (ROCUs) and local (police forces)
- **the governance** provided by the organised crime strategy, SPR, police and crime commissioners and the Organised Crime Partnership Board
- **the four operational elements**, which are: organised crime group mapping (OCGM), tiered operational response (TOR), effective tasking and co-ordination processes and the management of OCGs using the 'Investigation and Disruption Manual'.

Organised Crime Group Mapping (OCGM)

5.3.4 OCGM[49], a component of the IOM, provides the Police Service and its partners with local, regional and national OCG data in terms of volume and demand. The OCGM process automatically places OCGs in bands based on answers to questions about criminal activities, intent and capability attributes. This means that OCGs are grouped statistically into bands that reflect the range of criminality and threat.

5.3.5 The assessment tool is, therefore, capable of ranking OCGs from across a wide range of criminality types. This ranking informs the final stage of the OCGM process, which is their prioritisation during the coordination and tasking process.

[48] See paragraph 60 of the 'Local to Global' strategy – <http://www.homeoffice.gov.uk/publications/crime/organised-crime-strategy>.
[49] See paragraph 129 of the 'Local to Global' strategy – <http://www.homeoffice.gov.uk/publications/crime/organised-crime-strategy>.

Tiered Operational Response (TOR)

5.3.6 TOR enables the large number of OCGs exposed by OCGM to be managed. Each OCG is allocated a tier of response through the tasking regime. After mapping an OCG and giving consideration to its banding, a decision is made to ensure there is an appropriate law enforcement response to it. To achieve this, TOR is applied to all mapped OCGs and ratified through the coordination and tasking process. During this process consideration is given to the assessment, organisational priorities, resources, opportunity to intervene and the imminence of the threat posed by an OCG to prioritise the response. The tiers are:

- **Tier 1** – comprehensive operational or investigative intervention
- **Tier 2** – limited plan or action that prevents or disrupts
- **Tier 3** – proactive intelligence development
- **Tier 4** – developing opportunities for action.

As an example, Tier 1 might require NCA intervention whereas Tier 4 might require intelligence gathering by neighbourhood policing teams.

5.3.7 Data accrued through OCGM is aggregated to provide a national picture. Currently there are 9,269 OCGs with 41,084 nominals across the UK[50]. This developing data enables the Police Service to continually identify the resources required to tackle SOC.

National

5.3.8 The Organised Crime Coordination Centre (OCCC)[51] enables police forces and other law enforcement partners to collate intelligence and information on OCGs. The OCCC identifies connections between OCGs, manages deconfliction and agrees the best approach for tackling them, leading to improved tasking and prioritisation.

Regional

5.3.9 ROCUs provide specialist, collaboratively-held functions, and support operations against OCGs whose complexity, sophistication and geographical reach is beyond the capability of local forces. There are currently nine ROCUs across the UK, mirroring the nine ACPO regions, with specific arrangements in the Metropolitan Police area. ROCUs have a number of specific functions and capabilities (see paragraph 5.4.2). The funding and functions of ROCUs are shared between the forces who contribute towards them, with the exception of two aspects – Regional Asset Recovery Units (RARTs) and Regional Intelligence

[50] See the 'Local to Global' strategy – <http://www.homeoffice.gov.uk/publications/crime/organised-crime-strategy>.
[51] See the Crime and Courts Bill – <http://www.homeoffice.gov.uk/publications/about-us/legislation/crime-courts-part1>.

Units (RIUs). These two functions are centrally funded by government, ensuring that there is a RART and RIU within each region. The majority of these are located within ROCUs.

Local

5.3.10 At the local level, forces need to identify and tackle OCGs appropriately. If an investigation escalates beyond a force's capacity, or particular specialist support is required, the investigation should be handed over to the regional and national units. This practice is in line with the National Intelligence Model and is completed through the local, force and regional tasking and co-ordination process.

5.4 Capability

National Specific Capabilities[8]

5.4.1 At the national level, the OCCC will manage the following activities on behalf of the Police Service:

- OCG flagging
- operational security (compromise)
- deconfliction (coordination).

Regional Specific Capabilities[52]

5.4.2 At the regional level, ROCUs engage with the Crown Prosecution Service to establish and agree joint policies for investigating and prosecuting organised crime. ROCUs are tasked through the multi-agency strategic and tactical tasking process, with appropriate representation from partner agencies and stakeholders including the Government Agencies Intelligence Network (GAIN)[53]. Regional tasking processes are assisted by a regional intelligence group with representatives from the RIU and force intelligence officers.

[52] See paragraphs 129-130 of the 'Local to Global' strategy – <http://www.homeoffice.gov.uk/publications/crime/organised-crime-strategy>.
[53] See paragraphs 117 and 119 of the 'Local to Global' strategy – <http://www.homeoffice.gov.uk/publications/crime/organised-crime-strategy>.

5.4.3 Local Assets

5.4.4 Forces should have, or have access to, assets to aid their response to the threat posed by organised crime. Forces need to demonstrate that they have a multi-agency intelligence capacity which feeds into the regional and national model perspective. Some asset capabilities are found only within ROCUs, such as:

- RARTs
- RIUs
- in some cases, shared confidential units exploiting the most sensitive intelligence sources
- cyber crime capability.

There are a number of other specific functions and capabilities that forces should have, or have access to, either through ROCUs or collaborations. These include:

- covert RIPA authorisations capability
- protected persons capability
- technical surveillance unit
- case support capability
- hi-tech capability
- covert surveillance capability
- equipment and facilities supporting interoperability
- dedicated source unit
- supporting operational assets (eg, firearms capability)
- search teams and an enforcement capability
- investigation assets
- financial investigation
- confiscation and asset recovery capability
- communications data capability
- fraud investigation.

Collaboration

5.4.5 There should be collaboration with other forces, other regions, agencies and partners in response to the threat of organised crime. A strategic process should be in place which articulates to collaborators and partners the current threat and risk assessment of organised crime. Collaboration with other forces, communities at the neighbourhood policing level and partners, in the form of Community Safety Partnerships[54], should be forged to prevent organised crime.

[54] See paragraph 129 of the 'Local to Global' strategy – <http://www.homeoffice.gov.uk/publications/crime/organised-crime-strategy>.

Fraud

5.4.6 Forces should have, or have access to, the capability to conduct investigations into fraud. This capability will range from investigating low-level fraud networks targeting specific individuals up to and including OCGs that commit large-scale fraud. Forces also need to have, or have access to, the capability to conduct investigations into persons and OCGs that use technology such as the internet to commit their offences.

Intelligence

5.4.6 It is important to gather and make use of intelligence. Forces should be able to demonstrate that they are able to use a range of sources to collect information, analyse intelligence products and manage information and intelligence. Once completed, these products need to be disseminated as appropriate.

Tasking and Co-ordination Processes

5.4.7 In order to combat OCGs effectively, forces need to demonstrate that they have a strategic and tactical tasking and co-ordination group which adopts a TOR.

Mapping OCGs, Individuals and Organised Crime Series

5.4.8 Forces need to identify, assess and manage OCGs so that OCGM data can be managed successfully.

Identifying, Assessing and Managing Organisational Risk

5.4.9 Forces need to identify, assess and manage their organisational risk. Once this process has been completed, forces need to have the capacity to test business continuity plans and identify and assess operational risks.

Communications

5.4.10 It is vital to have processes for communicating internally, externally and with partners and the community, including the media. Forces should be able to evidence communication through a briefing and debriefing process, capturing and disseminating good practice and lessons learnt. When dealing with SOC, forces need to have a communications, marketing and media strategy in place.

Governance and Command Structures

5.4.11 These need to be established so that forces are able to evidence financial and human resources management, and to provide clear governance and scrutiny. Forces should also have, or have access to, the capability and capacity to audit relevant systems and processes.

Knowledge Management

5.4.12 Forces need to provide staff with access to legislation and guidance which is relevant to their roles. Processes need to exist for staff to review and update their knowledge.

Security and Integrity

5.4.13 Forces need a designated lead who has ownership of security and integrity procedures protecting covert tactics, resources and sources. Staff need to be subject to the appropriate level of vetting, and forces should be able to evidence the risk-based involvement of professional standards in scrutinising personal and organisational integrity.

5.4.14 Detailed force and regional capability frameworks for SOC have been developed by the portfolio lead in conjunction with the NPIA[55].

5.5 Consistency

5.5.1 In support of tackling SOC, forces need to ensure they adopt a consistent approach in how they specify, procure, implement and operate with respect to:

- the police use of firearms (mobile armed surveillance teams)
- covert surveillance
- technical surveillance.

These aspects are covered by the ACPO UK Operational Interoperability Working Group.

Covert Learning Programme

5.5.2 SOC is supported by a covert learning programme which is delivered by the College of Policing. The covert learning programme ensures national consistency across the following areas:

- covert surveillance
- the management of covert human intelligence sources

[55] Developed by the NPIA for the ACPO OCPB (Organised Crime Portfolio Board).

- technical surveillance
- undercover operations
- kidnap and extortion incidents
- the use and management of covert techniques
- debriefing in prisons
- communications data
- the future confidential operating model.

There is an expectation that forces will ensure that persons operating in these disciplines have achieved the required standard.

Training for Investigation

5.5.3 National consistency with respect to investigation is assured through accredited training that includes Professionalising the Investigation Programme and Investigative Interviewing (PIP Levels 2 and 3). There is an expectation that forces will ensure that officers conducting investigations have received the required training.

5.5.4 The learning programmes are supported by APP[56]. The APP for SOC includes:

- a review of the National Crime Strategy, including a description of the NCA
- an explanation of ROCUs and their functions
- guidance on the local response to OCGs, including the roles of community safety partnerships
- a description of the IOM
- guidance on imposing Serious Crime Prevention Orders on both individuals and OCGs.

Fraud

5.5.5 Action Fraud is a service run by the National Fraud Authority which works in partnership with the National Fraud Intelligence Bureau (NFIB). The purpose of Action Fraud is to provide individuals and businesses with a consistent service when reporting and investigating fraud offences. This will lead to an enhanced, preventative national approach to fraud.

5.5.6 Tackling the top levels of fraud is a specialist policing role. Forces should ensure that investigators are suitably trained and accredited in respect of the National Fraud Course so that they can provide an appropriate and consistent response to victims.

[56] Authorised Professional Practice – for further information, email <APP.contact@college.pnn.police.uk>.

5.6 Connectivity

5.6.1 The newly established OCCC will function as a national hub collating, analysing and disseminating criminal intelligence related to organised crime. Local forces should cooperate with the national coordination and tasking arrangements led by the NCA to support this process.

5.6.2 The IOM provides a structure that ensures local, regional and national connectivity within SOC.

5.6.3 All crime reports and information relating to fraud are transferred to the NFIB at the City of London Police where they are analysed. Detailed analysis of all the available information ensures that, where there are good lines of enquiry, crimes are followed up. The NFIB do this by providing the relevant authorities with work packages. Where appropriate, these authorities will be expected to conduct the investigations.

Chapter 6

National Requirements for Counter Terrorism

6.1 Overview

6.1.1 Terrorism is rated among the highest risks within the National Security Risk Assessment[57] and it remains a serious and enduring threat to the UK.

6.1.2 Counter terrorism (CT) policing contributes to the management of threat and risk from terrorism across all four workstreams of the government's CT strategy (CONTEST)[58]. The key objectives for the police and partners relate to the four themes:

- **Pursue** – identifying and disrupting terrorist activity
- **Prevent** – working with communities, local authorities and other partners to identify and divert those involved in, or vulnerable to, radicalisation
- **Protect** – policing the UK border, critical national infrastructure, civil nuclear sites, transport systems and the public
- **Prepare** – leading the immediate response during or after a terrorist attack, including responding to CBRN incidents.

6.1.3 The Police Service's National Counter Terrorist Strategic Threat Risk Assessment[59] assesses the implications of the CT threat to make classified recommendations for policing priorities via the ACPO Counter Terrorism Coordination Centre (ACTCC).

6.1.4 The CT network is intrinsically linked to local policing. While not always the seat of operational activity, command and control is positioned within lead forces, whereas tasking and co-ordination is delivered nationally via the ACTCC. See paragraph 6.6.1.

6.1.5 The ability to flex and surge resources across policing domains is crucial, as is the 'local to global' golden thread of CT policing (from local communities within the UK through to a threat from overseas).

[57] See <http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf>.
[58] See <http://www.homeoffice.gov.uk/counter-terrorism/uk-counter-terrorism-strat/>.
[59] For further information contact the Senior National Coordinator for Counter Terrorism via the ACTCC.

6.2 Planning Assumptions

6.2.1 The CONTEST planning assumptions (2011 to 2015) reflect a shared understanding (between the government, the Police Service and other delivery agents) of future terrorist intent, technological trends and the political and economic environment. These assumptions cover:

- Al Qa'ida
- radicalisation
- technology and techniques
- mass-scale attacks
- Northern Ireland
- individual extremists
- foreign intelligence services.

Al Qa'ida

6.2.2 Al Qa'ida affiliates may continue to grow, taking advantage of state fragility and failure. They will aspire to attack western targets.

Radicalisation

6.2.3 It is likely that some individuals will continue to be radicalised. Extremist material on the internet will continue to motivate some people to engage in terrorism, but will rarely be a substitute for the social process of radicalisation.

Technology and Techniques

6.2.4 Terrorist groups will use a range of new and established attack techniques. Groups will continue to benefit from 'off-the-shelf' technology in planning and conducting attacks. The internet and virtual space will be strategically vital. See chapter 7.

Mass-Scale Attacks

6.2.5 Organisations will seek to conduct attacks which will cause mass casualties or otherwise have a visible mass-disruptive effect.

Northern Ireland

6.2.6 Northern Ireland-related terrorist groups will continue to conduct attacks in Northern Ireland in an attempt to reverse the peace process. Some groups will continue to aspire to conduct attacks in Great Britain.

Individual Extremists

6.2.7 Isolated individuals will continue to engage in terrorist activity in the name of extreme right or left-wing views or other ideologies.

Foreign Intelligence Services

6.2.8 The UK remains a high-priority target for a number of Foreign Intelligence Services (FIS). FIS conduct covert operations against UK interests, in the UK and overseas, to obtain both official and commercially-sensitive intelligence. FIS seek to collect intelligence on a broad range of subjects to inform and advantage their governments' political, military, technological and economic programmes. For this reason FIS target UK commercial and government-related organisations.

6.2.9 The trend of FIS mounting cyber attacks against UK interests is also likely to continue, and will potentially increase as FIS develop their technical capability.

6.2.10 The potential impact of successful state-sponsored espionage against the UK is both wide reaching and significant. It can cause damage to UK national security, economic well-being and resilience as well as defence and foreign policy strategies.

6.3 Capacity and Contribution

6.3.1 The Police Counter Terrorism Network provides a local, regional and national structure to ensure that the Police Service has the capacity to meet the aforementioned planning assumptions.

6.3.2 The development of this structure and resources has been predicated on the need to establish, alongside partners, adequate capacity and capability to deal with current and foreseeable threats in line with the Tier 1 risk (NSRA) status of CT.

6.3.3 There are a number of grants specific to the Police Counter Terrorism Network which provide the police with the capacity and capability to contend with the threats posed by terrorism. Forces make bids for allocation of funds under the CT revenue grant and allocation is based on a national assessment of threat and risk.

6.3.4 In the 2012/13 financial year the total CT revenue grant from the Home Office was £581m and the capital grant was £23m. In addition, there were separate funding steams for channel and domestic extremism. Significant capability is also provided from in-force funding, particularly but not exclusively non-ports officers within CT/Special Branches – see paragraph 6.3.11.

6.3.5 Police authorities (as are currently) sign up to Home Office grant terms and conditions on a yearly basis. They sign up at the beginning of the year and again at the grant statement year end return. Accepting the terms and conditions is to sign up to the funding and the deliverables for that funding. The CT national requirement does not cover capability provided by the royalty and diplomatic-specific grant.

National

6.3.6 National strategy and policy is delivered through the ACPO Business Area for Terrorism and Allied Matters (ACPO TAM), which also delivers a number of support functions including:

- facilitating national funding arrangements (excluding the MPS CT grant)
- delivering national projects
- performance overview.

Aside from NaCTSO and a small number of funded posts in the Joint Terrorism Analysis Centre and the Home Office Exercise Programme Team, all other national functions are distributed under a lead force model (see paragraph 6.3.8).

Regional

6.3.7 Historically, most terrorism investigations were managed and overseen by the Metropolitan Police Service (MPS). In 2006 a national policing CT network was established, providing a UK policing capability and strengthening the UK's response to terrorism. This new network needed specialist structures, systems, processes and expertise which linked in with policing at a regional, force and neighbourhood level.

6.3.8 The following dedicated CT policing resources were consequently introduced:

- counter terrorism command
- counter terrorism units (CTUs)
- counter terrorism intelligence units (CTIUs).

The units are nationally funded but regionally based and staffed and resourced by the police force in the area in which they are located

(known as the lead force). This regional network is supported by other, nationally-distributed functions including:

- the National Ports Assessment Centre
- the National Borders Targeting Centre
- the National Domestic Extremism Unit (NDEU)
- the Counter Terrorism Internet Referral Unit
- the ACTCC.

See also paragraph 6.6.1.

6.3.9 This multi-skilled network of regional CT intelligence and surveillance specialists, and in some areas investigative assets, assists forces and partners with the development of CT intelligence and their response to incidents and events. This includes staff posted abroad to train foreign police services to support the wider government security effort.

6.3.10 These regional units can also assist with delivering the wider CONTEST strategy and have the ability to act as a single responsive entity across the UK when required.

Local

6.3.11 CT policing cannot be delivered by dedicated units and specialists alone. During periods of both surge and normal demand, effective CT policing is intrinsically linked with, and dependent on, the core resources of local forces and other agencies. The capacity provided by local force assets falls outside ring-fenced CT grant funding but provides a necessary contribution to the overall CT effort. Most notably, these include force CT/Special Branches and neighbourhood policing.

6.3.12 Specifically, forces remain responsible for the acquisition, development, analysis and management of all force CT/DE intelligence and information, eg, local information-sharing arrangements and community and partnership efforts. This responsibility extends to identifying and managing local risks and vulnerabilities, with the support of national and regional tasking processes. This local responsibility is endorsed by Chief Constables' Council and solidified through respective memoranda of understanding, protocols and service level agreements.

6.3.13 In addition to the CT grant provision of Dedicated Security Posts (DSP) based at ports, protective capacity is also delivered via:

- counter terrorism security advisors (CTSAs), of which there are presently 227 nationally
- critical national infrastructure posts

- arrangements to address ground-based threats to aircraft, where relevant.

Chief constables are also required to agree appropriate security arrangements with airport operators, including funding arrangements for a police presence if necessary. The CT grant also supports:

- preparatory capability and planning
- channel delivery capability (intrinsically linked to local authority statutory safe-guarding responsibilities)
- prison intelligence
- DE response capability
- 'prevent' engagement officers working in priority areas.

6.3.14 Other force assets used to support CT investigations include:

- specialist protection
- armed support to surveillance (including CT specialist firearms officers)
- investigation teams
- regional support group assistance to partner agencies
- dedicated, protective support to the critical national infrastructure
- embedded 'prevent' delivery in forces without OSCT 'prevent' funding.

6.4 Capability

6.4.1 The ACTCC is responsible for the following functions (in consultation with the CT network and the Security Service):

- prioritising national CT assets
- providing support for operational activity
- facilitating the deployment of CT assets in times of crisis
- monitoring the overall operational resilience of the CT network.

The ACTCC is also the single point of contact for communicating CT activity and operational updates to the Home Office via OSCT.

6.4.2 Effective joint (police and partners) daily, weekly and six-weekly tasking cycles are important. They provide local forces and regional units with the capability to bid for conventional and specialist assets to meet their demands.

6.4.3 Forces need to ensure that they have a CBRN capability to respond to any terrorist-related CBRN incident. The current capacity is set at 8475 trained officers nationally (equating to 339 PSUs) predicated on the Home Office Model Response and Police Operational Response

Programme (but this is currently subject to review). The Home Office provides personal protective equipment and appropriate detection, identification and monitoring equipment to support these resources.

6.4.4 Forces need to ensure that their CBRN resources are accredited and equipped (across all command levels) to a nationally consistent standard. While existing equipment has been centrally provided, ongoing maintenance is to be provided by forces.

6.4.5 Forces need to ensure that they have an IT infrastructure and telephony capability which enables them to access the current CT intelligence system and the network which links local, regional and national CT messaging.

6.4.6 Forces need to ensure that they have sufficient capabilities of trained ACPO (TAM)-accredited CT search officers and security coordinators (SecCo) on a proportionate basis and according to local assessments. Presently there are approximately 300 SecCos and the governance is such that a National CT SecCo Board has been created with representatives from each of the ACPO regions. Each force needs to establish the number of events where deployment of a CT SecCo should be considered. From this, the number of qualified CT SecCos required to service the demand can be ascertained, balancing supply and demand. Regional resources can be 'shared'.

6.4.7 Forces need to maintain appropriate security clearance for personnel and they should fund and manage the vetting levels of their employees.

6.4.8 Work is ongoing in OSCT to review the national capability requirement in light of changes to the CT threat, the policing landscape and improvements in 'blue-light' doctrine and practice.

<u>Pursue – Intelligence Development and Understanding the Threat</u>

6.4.9 To stop terrorist attacks, forces need to have capabilities in place that gather and develop intelligence. They should be able to demonstrate that they have, or have access to, a source handling unit that links into local policing. Intelligence can then be developed and analysed, providing a product which can be disseminated.

6.4.10 Where appropriate, forces need to have ports officers, ports intelligence units, ports search teams and ports management which link in with other agencies conducting local and national operations. At the regional level, capabilities funded by CT grant may include:

- a special projects team
- covert internet investigation

- covert surveillance.

Pursue – Investigations

6.4.11 Where possible and subject to training, forces need to ensure that they have a strategic command centre capability to provide support to the regional cadre of CT commanders, deployable to a CT Hub, whom are accredited to the appropriate levels.

6.4.12 A centrally funded CT grant ensures there is a regional capability to undertake reactive and proactive CT investigations and other specialist investigations. Recognising that CT(I)Us have different capabilities to CTUs, regions need to provide specialist investigative assets such as forensics and exhibits officers and be able to deliver executive action in a safe and coordinated manner. They should coordinate all activity within the national network through efficient and effective tasking and coordination. Throughout a CT investigation, prosecutions need to be managed carefully through the criminal justice system, developing good working practices with the Crown Prosecution Service.

Prevent – Stopping People from Becoming Terrorists or Supporting Terrorism

6.4.13 The 'prevent' strategy is centrally funded through grants but delivered at the force level, augmenting the significant effort made by neighbourhood policing. Where there are risks of radicalisation, forces need to work with a wide range of sectors and institutions including education, faith, health and criminal justice.

6.4.14 Forces need to respond to the ideological challenge presented by terrorism and the threats posed by those who promote it. This should be done through local delivery, using:

- partner agencies
- community engagement
- briefings to partners
- information development
- disruption and intervention.

6.4.15 There are more than 200 'prevent' engagement officers who are centrally funded through Home Office grants. Their role includes:

- connecting CT policing, neighbourhood policing and communities
- disrupting people engaged in radicalisation
- supporting vulnerable people susceptible to radicalisation.

Protect – Strengthening Protection to Reduce Vulnerability Against a Terrorist Attack in the UK or Against our Interests Overseas

6.4.16 The 'protect' workstream of the CONTEST strategy is nationally funded but locally based with requirements to strengthen and protect:

- the UK border
- the transport network
- the critical national infrastructure
- crowded places.

Forces need to work with the National Coordinator Protect and Prepare to provide national strategic direction to 'protect' activity and protective security patrols at vulnerable locations in accordance with tasking and coordination. Forces need a dedicated security officer, physical security officer and audit and compliance officers.

Prepare – To work with Partners to Mitigate the Impact of a Terrorist Attack where that Attack cannot be Stopped and to Optimise Recovery from its Aftermath

6.4.17 Forces need to ensure that they develop capabilities in accordance with the NSRA and provide CT contingency planning guidance. Forces' capability to deal with CT incidents should be tested on a regular basis. Forces should work with the National Coordinator Protect and Prepare to develop regional preparedness according to national strategic direction.

6.4.18 A CT 'prepare' lead within each CT Branch has been proposed with a view to delivering contingency planning in collaboration with internal and external partner agencies. This role is not currently funded or required but it is deemed necessary to ensure a direct point of contact.

6.4.19 The aforementioned capabilities are based on those developed through CONTEST. Further work to define force capability frameworks for CT and DE is currently being undertaken by the College of Policing in consultation with portfolio leads[60].

6.5 Consistency

6.5.1 The National Coordinator Prevent, National Coordinator Protect and Prepare and Senior National Coordinator Pursue are responsible for the development of CT advice and guidance published in APP[61].

[60] Contact <PracticeImprovement.SupportOffice@college.pnn.police.uk>.
[61] Authorised Professional Practice – for further information, email <APP.contact@college.pnn.police.uk>.

6.5.2 Consistency is provided through nationally-accredited training for CT commanders, CT surveillance officers and other specialists. This is managed by the Counter Terrorism Organisational Development Unit based at West Midlands CTU.

6.5.3 The agreed model for a multi-agency response to a CBRN event is based on nine key tasks:

- command, control and coordination
- mobilisation
- arrival at scene
- scene assessment
- scene management
- deliberate reconnaissance
- decontamination
- rescue and triage
- survivor management.

These key tasks have been defined and agreed by the blue-light emergency services and incorporated in single and multi-agency doctrine since 2007. However, while it is not expected that these key tasks will be subject to substantial or, indeed, any changes, they will be included in a review of the UK CBRN capability.

6.5.4 The new Joint Emergency Services Interoperability Programme (JESIP)[62] has been established to ensure blue-light services work together as effectively as possible in response to a major incident.

6.5.5 All forces should operate in an environment where they can ensure access is restricted to preserve physical and IT security within the CT domain.

6.6 Connectivity

6.6.1 National coordination for CT is delivered by the ACTCC. The ACTCC works collaboratively with force CT/Special Branches, CTIUs, national coordinators' offices, the NDEU and a range of partner agencies. The ACTCC provides a national coordinating function by maintaining a national overview of CT assets, intelligence and operational activity. Where operational activity extends beyond the CT arena, the ACTCC will work collaboratively with PNICC as per agreed protocols to deliver a policing response.

[62] For further details contact the ACPO lead for Interoperability.

6.6.2 In the early stages of a CBRN event, CBRN capability is coordinated through the Police National CBRN Centre until PNICC is in a position to undertake this role[63].

6.6.3 Forces should cooperate with the Police National CBRN Centre, PNICC and the ACTCC where required to do so.

6.6.4 The ACTCC communicates with partners and the wider police family about current and emerging CT issues. It also briefs senior officers and informs the Senior National Coordinator for Counter Terrorism (SNCCT) and Assistant Commissioner Specialist Operations of operational police activity. The ACTCC coordinates advisory messages and disseminates protective security guidance to the CT network and local forces.

6.6.5 The ACTCC will provide the SNCCT with the UK CT threat and risk picture and a clear understanding of those assets deployed and assets available. It has been agreed by chief officers that the SNCCT will coordinate the response to national CT events.

6.6.6 Staff from partner agencies such as local authorities, the UK Border Agency, Fire Service, Probation Service, the Military and Civil Nuclear Constabulary are embedded within all regional CTUs.

6.6.7 Under the 'prevent' strand of CONTEST, work is undertaken with a range of sectors and institutions (eg, education, health, faith and criminal justice) where risks of radicalisation need to be addressed. These resources coordinate the safeguarding of people vulnerable to extremism and terrorism across regions, ensuring:

- partner and community engagement
- appropriate briefing of partner agencies
- deconfliction, where necessary.

[63] In accordance with the APP module on CBRN.

Chapter 7

National Requirements for Large-Scale Cyber Incidents

7.1 Overview

7.1.1 Cyber security is defined as one of four top priorities for UK national security[64]. The term 'cyber attack' covers anything from small-scale email scams to sophisticated large-scale attacks driven by diverse political and economic motives.

7.1.2 The National Security Risk Assessment[65] identifies a large-scale cyber incident and the risk of a hostile cyber attack by other states as Tier 1 risks. It is important to note that a cyber incident may not necessarily result from a criminal attack but could be caused by a technological issue or failure.

7.1.3 The UK Cyber Security Strategy[66] outlines these objectives for the UK:

- **tackle** cyber crime and be one of the most **secure** places in the world to do business
- be more **resilient** to cyber attacks and able to **protect** interests in cyberspace
- help **shape** an open, stable and vibrant cyberspace which the UK public can use safely
- have cross-cutting **knowledge and skills** to underpin the achievement of these objectives.

7.1.4 The crime threat at the national level may be a major incident, such as a criminal attack on a financial institution to gather data or money, or it may be an aggregated threat, where many people or businesses across the UK are targeted.

7.1.5 The UK's cyber economy is estimated to be worth £82 billion a year and is set to rise[67]. The scope and sophistication of persons engaged in this type of crime mean that investigations are technically complex and require access to specialist skills, often from the private sector. Criminals are organised and target the most vulnerable members of society. They are quick to spot potential vulnerabilities of new technologies and exploit them to commit offences or prevent detection. The National Security Cyber Crime Programme funding has enabled Action Fraud and the NFIB to deliver enhanced functions for fraud and

[64] See <http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf>.
[65] See <http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf>.
[66] See <http://www.cabinetoffice.gov.uk/news/protecting-and-promoting-uk-digital-world>.
[67] See <http://www.cabinetoffice.gov.uk/news/protecting-and-promoting-uk-digital-world>.

online financial crime. This will inevitably lead to an increase in the number of reported incidents referred to police forces for further action.

7.1.6 The structure of cyber crime organisations is very different from the traditional concept of organised crime groups. Often there is no obvious leadership, labour is divided according to individuals' technical specialisms, and most members only know each other online.

7.1.7 The internet allows criminals to commit offences across geographical and jurisdictional boundaries. This poses challenges for traditional law enforcement, especially as more of the nation's public and private assets are stored electronically rather than physically, and outside of the jurisdiction of the UK. There is a distinct lack of accurate information relating to the scale and scope of cyber crimes, which makes it difficult to identify the appropriate response.

7.2 Planning Assumptions

Cyber Crime

7.2.1 Cyberspace is being used to commit crimes such as fraud and identity theft on an industrial scale. The internet has provided opportunities for those seeking to exploit children and the vulnerable by committing crimes such as child sexual abuse and hate crime. The internet can also be used as a communications tool to facilitate crime and disorder.

State-Sponsored Attacks on the National Infrastructure

7.2.2 The internet has provided opportunity for states seeking to conduct espionage with the aim of compromising our government, military, industrial and economic assets. The internet can be used to spread disinformation, disrupt critical services or seek advantage during times of increased tension. Vulnerabilities in cyberspace could be exploited by an enemy in times of conflict to reduce our military's technological advantage or attack our critical infrastructure.

Use of the Internet for Radicalisation and Inciting Terrorism

7.2.3 As highlighted in the government's CONTEST strategy[68] (see chapter 6), cyberspace is already used by terrorists to spread propaganda, radicalise potential supporters, raise funds, communicate and plan. While terrorists can be expected to continue to favour high-profile physical attacks, the threat that they may also use cyberspace to facilitate or mount attacks against the UK is growing. This will increase

[68] See <http://www.homeoffice.gov.uk/counter-terrorism/uk-counter-terrorism-strat/>.

all the more if if terrorists believe that our national infrastructure may be vulnerable[69].

Hacking

7.2.4 The threat to the UK from politically motivated activist groups or those seeking to gain greater notoriety is recognised. Attacks by hackers on public and private sector websites and online services in the UK are becoming more common. Attacks are undertaken to cause disruption, reputational and financial damage, and to gain publicity.

7.3 Capacity and Contribution

7.3.1 The current capacity to enforce the law against cyber crime needs development as criminals still regard exploiting cyberspace as a profitable and low-risk option. To address this and the wider issue of cyber security, the government has set aside £650 million of public funding for a four-year National Cyber Security Programme (2011–2015) as a result of the Strategic Defence and Security Review 2010[70].

National

7.3.2 Nationally a number of specialist units have been bolstered by funding from the National Cyber Security Programme. Both the Police Central e-crime Unit (PCeU) and SOCA-Cyber have increased their capacity to tackle cyber crime and protect the public by developing expertise in these highly complex and specialist areas. The Cyber Security Operations Centre (CSOC), on the other hand, has a wider responsibility to assist in protecting the cyber security of the UK. The CSOC has been created to:

- monitor the health of cyber space and coordinate incident response
- enable better understanding of attacks against UK networks and users
- provide improved advice and information about the risks to business and the public.

7.3.3 The ACPO National e-Crime Programme[71] (NeCP) delivers the policing response to the National Cyber Security Programme. It assists forces in defining what is needed to provide a local, regional and national response, promotes standards for training for cyber crime and provides a centre for knowledge and best practice. The NeCP is currently funded by the government and the MPS.

[69] For further details see chapter 6.
[70] See <www.cabinetoffice.gov.uk/sites/default/files/resources/strategic-defence-security-review.pdf>.
[71] ACPO e-Crime Strategy 2009 which can be found on POLKA – <https://polka.pnn.police.uk/en/Communities/Documents/?clubId=153>.

7.3.4 The work of the PCeU was created as one of the strands of the NeCP. The unit has a national mandate to tackle:

- the most serious incidents of computer intrusion (unauthorised access to data)
- distribution of malicious code (viruses, worms and Trojan horses)
- denial of service attack (denying access to intended users and botnets where users are unaware their computers have been set up to forward transmissions of viruses)
- internet-enabled fraud.

7.3.5 The PCeU is jointly funded by the government and the MPS and currently has in excess of 100 staff members. It is a central unit for UK policing dealing with the response to cyber crime, promoting training standards for cyber crime and acting as a centre for knowledge and best practice.

7.3.6 The PCeU works jointly with UK foreign law enforcement, government agencies, industry and academia in the fight against cyber attacks. These partnerships provide improved enforcement opportunities as they help to:

- identify cyber threats
- improve intelligence
- prevent activity
- provide a joint incident response capability.

7.3.7 The PCeU will merge with SOCA-Cyber to form the National Cyber Crime Unit within the National Crime Agency (NCA)[72] in October 2013. The role, remit and responsibilities of the new unit are being developed.

Regional

7.3.8 The national and regional network of CT policing units have a range of capabilities to address terrorist use of the internet. The role of CT policing regarding cyber-related threats is developing and has close links with the roles and capabilities of other national agencies.

7.3.9 The PCeU has established three regional hubs based in the North West, East Midlands, and Yorkshire and the Humber. The PCeU hubs are a national asset but regionally based. Their primary role is to deal with national cyber incidents but, where capacity allows, they will also deal with regional issues.

[72] The NCA will replace SOCA in 2013.

7.3.10 Each regional unit comprises a small number of officers with a developing expertise in the cyber crime area, both of which, are funded by central government. These regional officers work alongside the London PCeU and provide further national capacity for operations. They also have the ability to support regional and local operational activity. The PCeU hubs will remain within the regions when the PCeU migrates into the NCA.

Local

7.3.11 Local forces need to have their own capacity for managing cyber crimes reported to them locally. In the event of a large-scale cyber incident, whether motivated by crime, terrorism or caused by a natural disaster, local forces may be asked to contribute the following assets to assist the PCeU:

- digital forensic capability – staff and equipment trained to a similar standard and operating to recognised working practices on suitable equipment which is interoperable with the PCeU
- arrest teams
- search teams
- local intelligence and investigative staff
- local senior investigating officers (SIOs)
- interpreter/language capabilities
- custody facilities
- scenes of crime officers.

7.4 Capability

7.4.1 A capability framework is currently under development by the portfolio lead in conjunction with the College of Policing. This sets out the arrangements a force needs to have, or have access to, in order to provide a local response to cyber crime. These include arrangements for governance, response, knowledge, security and collaboration.

Commitment to Cyber Crime Response

7.4.2 Forces should be able to evidence a commitment to their cyber crime response. As part of the national capability, all forces need to ensure that they have suitable equipment which enables interoperability. Forces need to demonstrate that they have, or have access to, the following capabilities:

- a confidential unit
- a cyber crime investigation facility
- a covert internet investigation capability.

As part of the national response, forces need to ensure they have, or have access to:

- a digital forensic capability
- a covert technical capability
- a lead SIO who is able to take on parts of an investigation involving a large-scale cyber incident.

Understanding and Responding to National Threats, Risks and Harms

7.4.3 Forces need to understand the national threats, risks and harms and contribute to the national response. They need to contribute to the national threat assessment by sharing intelligence on cyber crime through:

- organised crime group mapping
- the NFIB and the Action Fraud reporting tool
- SOCA
- the PCeU.

Forces should ensure that capability and capacity in relation to cyber crime is commensurate with local and regional assessments. These threats and risks need to be linked to the policing plan and forces need a business continuity plan relating to cyber incidents.

Collaboration with Others

7.4.4 Forces need to collaborate with other forces, regions, national agencies and partners on cyber crime. Arrangements need to be established for forces to collaborate regionally and nationally to maximise efficiency in use of staff and equipment. This collaborative approach should be extended to commercial companies and universities, thereby providing forces with access to specialist knowledge and equipment. Forces should enter into early engagement with the Crown Prosecution Service for prosecutions into cyber and organised crime incidents.

Structured Approach to Operational Deployment

7.4.5 Forces need to have a structured approach to operational deployment. To ensure a consistent approach to tackling cyber incidents, forces need to adhere to the NeCP and be aware of their partners' (eg, SOCA, NFIB, Government Communication Headquarters and the Security Service) acceptance criteria when deploying to these incidents.

Governance and Command Structures

7.4.6 Forces need to have governance and command structures for cyber crime investigations. They need to ensure that there are governance arrangements in place which link to regional and national structures. They should establish a command structure to deal with cyber-related incidents both within force and those requiring a cross-border response. Staff dealing with cyber crime need to be provided with appropriate training and continuous professional development. Suitable HR and financial management should exist to support work on cyber-related incidents.

Knowledge Management

7.4.7 Forces need to demonstrate knowledge management and that they are able to provide their staff with access to legislation and guidance relevant to their roles. This includes having processes for staff to review and update their knowledge.

Communications

7.4.8 Forces need to have processes for communicating internally and externally with partners, the community and the media. Forces need to establish a policy which allows appropriate partners and industry to attend briefing and debriefing processes, and also have a system for capturing and disseminating good practice. Press releases on cyber incidents need to be aligned to the national strategy by engaging with the ACPO press office.

Security and Integrity

7.4.9 Forces need to manage security and integrity. They should ensure that staff are vetted appropriately and have a review process for the systems access of their employees. Forces need to have a policy for controlling unlawful material (eg, child sexual images) and for personal/financial data. Forces should have, or have access to, a professional standards investigative capability and review their operational security arrangements regularly to ensure that cyber vulnerabilities are considered and mitigated. Forces should be able to evidence that staff are subject to the appropriate level of vetting.

Reviews and Evaluations

7.4.10 Forces need to review and evaluate their contribution to cyber crime investigations. In order to assess their contribution to cyber-related incidents, forces need to be able to conduct management reviews and allow periodic peer reviews. Once the reviews are conducted, forces

need to evaluate lessons learnt so that policies and procedures can be updated.

7.4.11 In 2009 a survey was completed by all forces in England and Wales to determine their capability with regards to cyber crime. Due to the speed at which technology has advanced, a new survey is being completed and these results should be available by the end of January 2013. This will provide an up-to-date understanding of capability levels within forces.

7.5 Consistency

7.5.1 The College of Policing develops and delivers cyber crime training to specialist cyber crime staff and to all frontline officers and staff. E-leaning packages such as those created by NCALT (the National Centre for Applied Learning Technologies) are used to provide frontline officers with the knowledge and skills needed to undertake their role where they are the first to respond to a cyber-related incident. A cyber thread is being woven throughout relevant mainstream training and standalone e-learning packages for delivery in 2013.

7.5.2 NeCP and PCeU officers are currently working with Skills for Justice to create a national competency framework for all PCeU officers working in intelligence and enforcement which can be used by forces and regions. POLKA (the Police OnLine Knowledge Area)[73] is used to share information and ideas and provide technology and legal updates with respect to cyber crime.

7.5.3 Improvements to forensic processes have been piloted in the East Midlands. This work has identified ways to prevent unnecessary submissions for analysis to highly trained hi-tech crime unit officers. If more widely implemented, this could provide consistency in how computer hardware is examined.

7.5.4 The NeCP have funded an interim National Hash Set Database based in Cheshire Constabulary to provide a consistent approach and governance to grading and examining indecent images of children. This database can be used by forces to reduce the time it takes to identify, forensically examine and grade child sexual images in accordance with the national standard.

[73] ACPO e-Crime Strategy 2009 which can be found on POLKA at – <https://polka.pnn.police.uk/en/Communities/Documents/?clubId=153>.

7.6 Connectivity

7.6.1 An agreed policy for managing a national cyber incident has been developed by CSOC and mandated by the Office of Cyber Security and Information Assurance within the Cabinet Office. The response is provided by partner agencies and coordinated by CSOC. There is no formal agreement with individual police forces as to what they might provide in response to a request for surge capacity under this agreement.

7.6.2 Cooperation is essential to tackling cyber crime effectively. Information should be shared between law enforcement agencies, commercial companies, government departments and universities to gain a detailed picture of the scale of a cyber incident. The Virtual Task Force brings together skills from the police, industry, academia and other law enforcement agencies to tackle specific cyber crime issues.

7.6.3 SOCA and the PCeU are actively involved with Europol and both are members of a group that is developing methods for Europol members to collaborate on e-crime.

7.6.4 SOCA and the PCeU are also members of the European Working Party Group on IT Crime. The PCeU acts as a national central reference point for the Police Service on global e-crime investigations coordinated through Interpol. In addition to Europol and Interpol, e-crime units cooperate with individual law enforcement agencies such as the Federal Bureau of Investigation.

Appendix

Abbreviations and Acronyms

ACPO	Association of Chief Police Officers
ACTCC	ACPO Counter Terrorism Coordination Centre
AEP	Attenuating Energy Projectile
APP	Authorised Professional Practice
BDU	Basic Deployment Unit
CBRN	Chemical, Biological, Radiological and Nuclear
CEOP	Child Exploitation Online Protection Agency
CSOC	Cyber Security Operations Centre
CT	Counter Terrorism
CTIU	Counter Terrorism Intelligence Unit
CTU	Counter Terrorism Unit
DE	Domestic Extremism
DVI	Disaster Victim Identification
EDL	English Defence League
FIS	Foreign Intelligence Services
G20	The Group of Twenty Finance Ministers and Central Bank Governors
G8	The Group of Eight
GAIN	Government Agencies Intelligence Network
HMIC	Her Majesty's Inspectorate of Constabulary
HR	Human Resources
IOM	Integrated Operating Model
IT	Information Technology
JESIP	Joint Emergency Services Interoperability Programme
LRF	Local Resilience Forum
MPS	Metropolitan Police Service
NaCTSO	National Counter Terrorism Security Office
NCA	National Crime Agency
NCALT	National Centre for Applied Learning Technologies
NDEU	National Domestic Extremism Unit
NDM	National Decision Model
NeCP	National e-Crime Programme
NFIB	National Fraud Intelligence Bureau
NMAT2	National Mutual Aid call taking Telephony service
NPIA	National Policing Improvement Agency
NRA	National Risk Assessment
NRR	National Risk Register
NSRA	National Security Risk Assessment
OCCC	Organised Crime Coordination Centre
OCG	Organised Crime Group
OCGM	Organised Crime Group Mapping

OCPB	Organised Crime Portfolio Board
OSCT	Office for Security and Counter Terrorism
PCeU	Police Central e-crime Unit
PIP	Professionalising the Investigation Programme
PNICC	Police National Information and Coordination Centre
POLKA	Police OnLine Knowledge Area
PSU	Police Support Unit
RART	Regional Asset Recovery Unit
RIPA	Regulation of Investigatory Powers Act 2000
RIU	Regional Intelligence Unit
ROCU	Regional Organised Crime Unit
SecCo	Security Coordinator
SIM	Senior Identification Manager
SIO	Senior Investigating Officer
SNCCT	Senior National Coordinator for Counter Terrorism
SOC	Serious and Organised Crime
SOCA	Serious Organised Crime Agency
SPoCC	Strategic Policing Coordination Centre
SPR	Strategic Policing Requirement
TAM	Terrorism and Allied Matters
TOR	Tiered Operational Response
UK	United Kingdom
UKOI	UK Operational Interoperability

National Policing Requirement

2012