REPORT TO: **STRATEGIC SCRUTINY MEETING**

DATE: **Monday 23 December 2013**

AGENDA ITEM: 5E STRATEGIC POLICING REQUIREMENT (SPR)

SUBJECT: SPR Update

Background

The Strategic Policing Requirement (SPR) outlines the responsibilities of forces in respect of their contribution to national policing:

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

The National Policing Requirement (NPR) has been developed to support delivery of the SPR, and outlines the capacity and contribution, capability, consistency and connectivity that forces should maintain to counter each of the threats. They are based on a number of planning assumptions that have been used to determine the appropriate national policing response.

This paper provides an overview of Lancashire Constabulary's position against those requirements.

1. Public Disorder

1.1 National Policing Requirement

Forces are expected to ensure that they have sufficient capability to provide the specialist officers, equipment and assets to respond to public disorder, both locally and in terms of regional and national mutual aid. This includes accredited public order commanders at Gold, Silver and Bronze levels. All assets, equipment, resources and training are expected to meet national standards.

The contribution required of each force towards the national capacity of public order assets (297 PSUs) is defined in the Public Order Mobilisation Formula. Mobilisation of these resources should be tested regularly.

Forces should ensure that public order intelligence and community tension products are captured and shared regionally and nationally, including with other emergency services, to enable an effective joint response to major incidents of disorder.

1.2 In Lancashire

To benchmark the Constabulary's position and progress in terms of the Strategic Policing Requirements for Public Order, H Division (Operational Support Services) has utilised the College of Policing's Capability Frameworks, which outline the detailed requirements in each SPR area.

In May 2013, representatives of the College of Policing attended the Constabulary to introduce the national self-assessment process through which forces can be judged on their compliance with the SPR (capacity and contribution, capability, consistency and connectivity).

The self-assessment consists of 10 'capability' areas (9 of which directly relate to the SPR), with each capability broken down in to a number of 'definitions'. There are 32 defined areas in total, with 27 relating directly to the SPR. Each of these capabilities and definitions are cross referenced with Authorised Professional Practice (APP).

The self-assessment process requires forces to objectively assess their own compliance in each definition area based upon advice supplied in the self-assessment document. Forces can rate themselves as Red, Amber or Green.

- Red - the force has not met the requirement, which should be reviewed frequently.
- Amber - the force has not met the requirement but a development plan has been agreed and activity is underway.
- Green - The force has met the requirement, which should be reviewed every six months to ensure continued compliance.

H Division has done work to benchmark their Public Order resources and have undertaken to review their self-assessment on a quarterly basis, to coincide with QPRs. At the most recent review undertaken on 24th October 2013 the assessment found that out the 32 definitions the results were:

- Red - 0
- Amber - 6 (4 directly related to SPR)
- Green - 26 (23 directly related to SPR)

Each of the Amber definitions has a development plan, an action owner and a completion date set. An updated is required prior to the next quarterly review, (i.e. 1st February 2014). The Amber findings relate in the main to organisational issues which will either be resolved or facilitated by the completion of the organisational reviews to be implemented in April 2014.

2. Civil Emergencies

2.1 National Policing Requirement

Police forces should be in a position to contribute to national assets in respect of:

- police support units (PSUs)
- basic deployment units (BDUs)
- chemical, biological, radiological and nuclear (CBRN) response
- disaster victim identification (DVI)
- casualty bureau resources.

Forces should have local plans for preventing and mitigating the effects of emergencies, including contingency planning and effective business continuity processes. This includes plans for mobilisation of resources and effective scene preservation in the event of a civil emergency resulting in mass fatalities; these plans should be regularly tested.

Forces are expected to work with partners, through the Lancashire Resilience Forum (LRF) and under the auspices of the Joint Emergency Services Interoperability Programme (JESIP), when formulating and developing their response to civil emergencies. This includes the gathering, assessment and dissemination of information and intelligence, as well as the exercising and deployment of emergency plans, implementation of lessons learned and development of effective internal and external communications strategies.

2.2 In Lancashire

Just as it has done with the SPR for Public Order, the Constabulary's H Division has utilised the College of Policing's Capability Frameworks to benchmark itself in terms of the SPR for Civil Emergencies.

In April 2013, representatives of the College of Policing attended the Constabulary to introduce the national self-assessment process by which forces can judge their compliance.

Once again, there are 10 'capability' areas (7 of which directly relate to the SPR), with each capability broken down in to a number of 'definitions'; in this case there are 33 defined areas in total, of which 23 relate directly to the SPR. Each of these capabilities and definitions are cross referenced with Authorised Professional Practice (APP).

Like the requirements for Public Order, H Division has done work to complete the self-assessment of Civil Emergencies and has undertaken to review that on a quarterly basis, to coincide with QPRs.

At the most recent review undertaken on 24th October 2013, out of a total of 33 definitions, of which 23 directly relate to the SPR, the assessment found that there were:

- Red - 0
- Amber - 3 (all directly related to SPR)
- Green - 30 (20 directly related to SPR)

Each of the Amber definitions has a development plan, an action owner and a completion date set. An update is required ahead of the next QPR, i.e. 1st February 2014.

The Amber findings relate to bedding in of some Business Continuity and Events Planning processes, the acquisition of a mobile command unit and the on-going work to create a force skills register.

3. Serious and Organised Crime (SOC)

3.1 National Policing Requirement

Each force and region is expected to have the capacity and capability commensurate with the specific threat presented by SOC. This includes a range of specific functions and capabilities that forces should either have or have access to, through force collaborations, Regional Organised Crime Units (ROCUs) and other partners and agencies.

Forces must have a strategic process which articulates the current threat and risk assessment, along with a multi-agency intelligence capacity which feeds into the regional and national model. Forces should be able to demonstrate that they use a range of sources to collect, analyse and manage information and intelligence.

Forces are expected to identify, assess and manage Organised Crime Groups (OCGs) in order that national mapping data can be managed successfully and there should be strategic and tactical tasking and co-ordination processes which adopt a tiered operational response.

A designated lead should have ownership of security and integrity procedures protecting covert tactics, resources and sources and staff should be vetted to an appropriate level. The force must be able to evidence the risk based involvement of professional standards in scrutinising personal and organisational integrity.

Forces also need to ensure that they take a consistent approach in the way that they specify, procure, implement and operate with respect to the police use of firearms (Mobile Armed Surveillance Teams), surveillance, and technical surveillance. A College of Policing (CoP) covert learning programme, ensures national consistency across a range of areas and there is an expectation for forces to ensure that staff have achieved the required standard.

Forces are expected to ensure that officers conducting investigations have received accredited training that includes Professionalising the Investigation Programme and Investigative Interviewing (PIP Levels 2 and 3). Forces should provide staff with access to legislation and guidance relevant to their roles and have processes in place for staff to review and update their knowledge.

3.2 In Lancashire

The Constabulary employs an efficient, joined up approach to delivering effective prosecution and disruption of OCGs, including organised crime group mapping (OCMG), tasking and co-ordination, investigation and disruption.

OCMG is supported by a rich intelligence scanning and gathering capability, capturing officer and community intelligence along with that of specialist units which pro-actively address specific intelligence requirements. Analysis provides a force level map of active OCGs which is processed through the national OCGM tracker to generate an accurate risk assessment.

The monthly level 2 tasking group considers force level threats, along with emerging divisional threats and high risk issues stemming from organised crime (OC), for allocation of appropriate resources. A pragmatic approach is adopted with impact on local communities and professional judgement playing a part in the decision making process. The meeting allocates the most appropriate specialist resources to effectively tackle identified problems, bring OC offenders to justice and disrupt / dismantle OCGs.

The force has a number of investigative options at its disposal in tackling SOC, including the Serious Organised Crime Unit (SOCU), the Force Surveillance Unit (FSU), Technical Surveillance Unit (TSU), BCU level Targeted Crime Units (TCUs) and the Fraud and Financial investigation teams. Lancashire's level two capability is sufficiently trained, practised and equipped to mobilise rapidly in response to local critical incidents, or those of regional or national importance.

In addition, the county has a well-established multi–agency group (Operation Genga) which aims to create a hostile environment for OC through relentless disruption. The emphasis is on diverse joint action, bringing varied and multiple powers and capabilities to bear on every facet of organised criminals' life. Contacts with regulatory authorities established through GENGA are used to curtail the activities of OCG members and hamper their attempts to legitimise criminal income

Lancashire is very proactive in publicising the issues and successes surrounding OC, with a public facing web-page which highlights key performance achievements and latest investigative successes. Convicted OCG members have recently been emblazoned on bus shelters and advertising hoardings in their local area, emphasising the consequences of getting involved with OC and demonstrating our determination to tackle the problem at all levels.

Effective use of various ancillary orders (Serious Crime Prevention Orders, Financial Recovery Orders FROs etc.) is a key aspect of Lancashire's management of convicted OC offenders. We have developed a close professional working relationship with the CPS serious case unit and honed the application process ensuring opportunities can be maximised within every investigation.

4. Counter Terrorism

4.1 National Policing Requirement

Forces should ensure that they have sufficient capacity and capability to provide the specialist officers, assets and equipment commensurate with the identified threat from terrorism. This includes appropriate resources in respect of all four CONTEST strands (Pursue, Prevent, Protect and Prepare). Forces should establish the likely number of events where deployment of a Counter Terrorism (CT) Security Co-ordinator (SecCo) is required in order to ascertain appropriate numbers of qualified personnel. Regional Resources can be 'shared'.

Forces are responsible for the acquisition, development, analysis and management of all force intelligence and information on CT and domestic extremism (DE), and there must be sufficient capability to gather and develop intelligence, including a source handling unit that links into local policing.

All forces should operate in an environment where they can ensure access is restricted to preserve physical and IT security within the CT domain and the IT infrastructure and telephony capability should be compatible with national systems.

Forces should respond to the ideological challenge presented by the threats of terrorism and radicalisation, working with communities and partners from a wide range of sectors and institutions such as education, faith, health and criminal justice.

Forces should work with national Protect and Prepare co-ordinators to develop regional preparedness and ensure security of vulnerable locations. The capability of Forces to deal with CT incidents should be tested on a regular basis.

4.2 In Lancashire

Whilst the Office for Security and Counter-Terrorism (OSCT) is responsible for activating and coordinating the national response to any terrorist incident, measures are in place locally to support deployment of regional resources. In the event of a terrorist incident, the local Counter Terrorism Branch (CTB) follows Home Office Counter Terrorism Contingency Planning Guidance.

Lancashire Constabulary works closely with national and regional partners, MI5 and the National Domestic Extremism and Disorder Intelligence Unit (NDEDIU), as well as the North West Counter Terrorism Unit, in managing the extremist threat.

National, regional and local CT structures are designed to address all elements of the Contest strategy with departmental leads for each strand. Lancashire’s CT resources are configured to manage the current and emerging threats from key areas, including International Terrorism, Northern Irish Related Terrorism and Domestic Extremism.

To promote consistency and interoperability, all CTBs and CTU’s adhere to the nationally agreed Intelligence Handling Model to assess and prioritise threat reporting, in conjunction with national partners.

Lancashire Constabulary works with communities to identify and address the issues that may directly or indirectly generate an extremist threat. The understanding of these threats allows police and partners to identify emerging issues. We also work with partners and communities to identify and offer support to those vulnerable to extremist messaging.

Lancashire Constabulary has dedicated Counter Terrorism Security Advisers (CTSAs), who are co-ordinated, trained and tasked by the National Counter Terrorism Security Office, a police unit co-located with the Centre for the Protection of the National Infrastructure (CPNI). Key responsibilities of the CTSA are the security of sites storing hazardous materials and crowded places as well as assisting CPNI in the protection of sites that form the national infrastructure.

Lancashire Constabulary also hosts Blackpool airport and Heysham sea port as well as monitoring activities at maritime and general aviation sites within the county.

With regard to PROTECT & PREPARE, the Lancashire CTB works with partners and key location managers to reduce their vulnerability to the extremist threat. The CTB also provide an update to the Lancashire Resilience Forum on current threats to ensure any inclusion in policy is current. Outside of investigating threats, the main local CTB contribution comes from the CTSA.

The PURSUE element of the Contest strategy sees joint management of investigations between police and partner agencies. In addition to those available in the national structures, Lancashire CTB has staff trained in various aspects of post event investigation. This includes the requirements around detaining persons for terrorism offences and scene management.

CTB contributes to the intelligence function around relevant events which could lead to public order issues; this includes instances of planned or spontaneous protest which could potentially attract extremist infiltration or targeting.

Within Lancashire, there are measures in place for managing a Chemical, Biological, Radiological, Nuclear or Explosive (CBRNE) incident via the Lancashire County Council Emergency Planning Service. Should a potential CBRN incident be identified within the force then the CTB, and out of office hours the on call officer, will make relevant checks to identify any relevant information that could assess the threat and support subsequent investigation.

Extensive partnership working in Lancashire ensures joint risk assessment and ownership in addressing the extremist threat. This naturally generates the most appropriate measures to identify and address identified risks and vulnerabilities.

5. Large Scale Cyber Incidents

5.1 National Policing Requirement

Forces should ensure that capability and capacity in relation to cyber-crime is commensurate with the local and regional assessments. There should be sufficient capability to provide the specialist officers, equipment and assets to respond to the threat, locally regionally and nationally as required.

This means that forces must have, or have access to resources including a confidential unit, cyber-crime investigation, covert internet investigation, digital forensic and covert technical capability. There should also be a lead SIO and force equipment should be suitable and enable interoperability.

The force should be able to demonstrate that it understands national threats, and can contribute to a national response. This includes sharing intelligence, collaborating with other forces, regions, agencies and partners and adhering to the national e-crime programme, to ensure a structured approach to operational deployment.

Staff dealing with cyber-crime should be appropriately trained, with opportunities for continuous professional development. Forces should ensure that staff are appropriately vetted and have a review process for systems access.

The force has processes for communicating internally and externally with partners, the community and the media, including access to briefing and debriefing processes, and that they have a system for capturing and disseminating good practice.

The force must have appropriate governance and command structures in place for cyber-crime investigations, which link to regional and national structures and should review and evaluate its contribution to cyber-crime investigations, through periodic management and peer reviews. Forces should evaluate lessons learnt from these reviews so that policies and procedures can be updated.

5.2 In Lancashire

Lancashire Constabulary has its own confidential unit and a covert internet investigation capability. Whilst the force does not currently have a dedicated force cyber-crime investigation facility, access is available on a regional basis, via the level two tasking process. As part of a national response, the Constabulary also has access to a digital forensic capability, a covert technical capability and a lead Senior Investigating Officer (SIO) who is able to take on parts of an investigation involving a large-scale cyber incident.

The Constabulary shares intelligence on cyber-crime through organised crime group mapping (OCGM), the National Fraud Intelligence Bureau (NFIB), the National Crime Agency (NCA) and the Police Central e-crime Unit (PCeU).

Lancashire Constabulary collaborates around cyber-crime both regionally and nationally, with other law enforcement agencies, with Lancaster University and has an effective working relationship with local Crown Prosecution Service (CPS).

Lancashire Constabulary has a comprehensive force and local intelligence capability, Confidential Unit, Covert Internet Investigation Unit, comprehensive open source research capability, appropriate high tech crime capability and a comprehensive tasking process to identify priority risks and threats and allocate appropriate SIO's and other resources. We have good relationships with regional forces, the North West Regional Organised Crime Unit and PCeU and have a robust Infosure capability protecting the Constabulary from being a victim of cyber-crime.

Due to their exceptional nature, we do not currently have large scale cyber-crime within our force risk assessment. Lancashire has not yet experienced a major cyber-incident but is acutely aware of the growing nature of this complex area of criminality and the Constabulary recognises need to improve its understanding of and readiness for such an event. This is work in progress.

There is currently an acknowledgement that we would benefit from increased training and understanding of cyber-crime at SIO level and a more comprehensive capability at investigator level, but resource allocation is under constant review and prioritised based on tangible risk and threat to the public of Lancashire.

The College of Policing Capabilities Framework sets out the arrangements forces should have, or have access to, to provide a local response to cyber-crime. These include arrangements for governance, response, knowledge, security and collaboration; Lancashire Constabulary has the required arrangements in place and is currently seeking to improve our knowledge and understanding of cyber-crime, through liaison and workshops with partners across the North West region.