HMICS

HM INSPECTORATE OF CONSTABULARY IN SCOTLAND

Strategic review of Police Scotland's response to online child sexual abuse

February 2020

Improving Policing Across Scotland

Produced and Published by Her Majesty's Inspectorate of Constabulary in Scotland

ISBN: 978-1-910165-56-0

Laid before the Scottish Parliament by Her Majesty's Inspector of Constabulary in Scotland under section 79(3) of the Police and Fire Reform (Scotland) Act 2012

HMICS/2020/01
www.hmics.scot

HM Inspectorate of Constabulary in Scotland

HM Inspectorate of Constabulary in Scotland (HMICS) is established under the Police and Fire Reform (Scotland) Act 2012 and has wide ranging powers to look into the ‘state, effectiveness and efficiency’ of both the Police Service of Scotland (Police Scotland) and the Scottish Police Authority (SPA).[1]

We have a statutory duty to inquire into the arrangements made by the Chief Constable and the SPA to meet their obligations in terms of best value and continuous improvement. If necessary, we can be directed by Scottish Ministers to look into anything relating to the SPA or Police Scotland as they consider appropriate. We also have an established role in providing professional advice and guidance on policing in Scotland.

- Our powers allow us to do anything we consider necessary or expedient for the purposes of, or in connection with, the carrying out of our functions

- The SPA and the Chief Constable must provide us with such assistance and co-operation as we may require to enable us to carry out our functions

- When we publish a report, the SPA and the Chief Constable must also consider what we have found and take such measures, if any, as they think fit

- Where our report identifies that the SPA or Police Scotland is not efficient or effective (or best value not secured), or will, unless remedial measures are taken, cease to be efficient or effective, Scottish Ministers may direct the SPA to take such measures as may be required. The SPA must comply with any direction given

- Where we make recommendations, we will follow them up and report publicly on progress

- We will identify good practice that can be applied across Scotland

- We work with other inspectorates and agencies across the public sector and co-ordinate our activities to reduce the burden of inspection and avoid unnecessary duplication

- We aim to add value and strengthen public confidence in Scottish policing and will do this through independent scrutiny and objective, evidence-led reporting about what we find

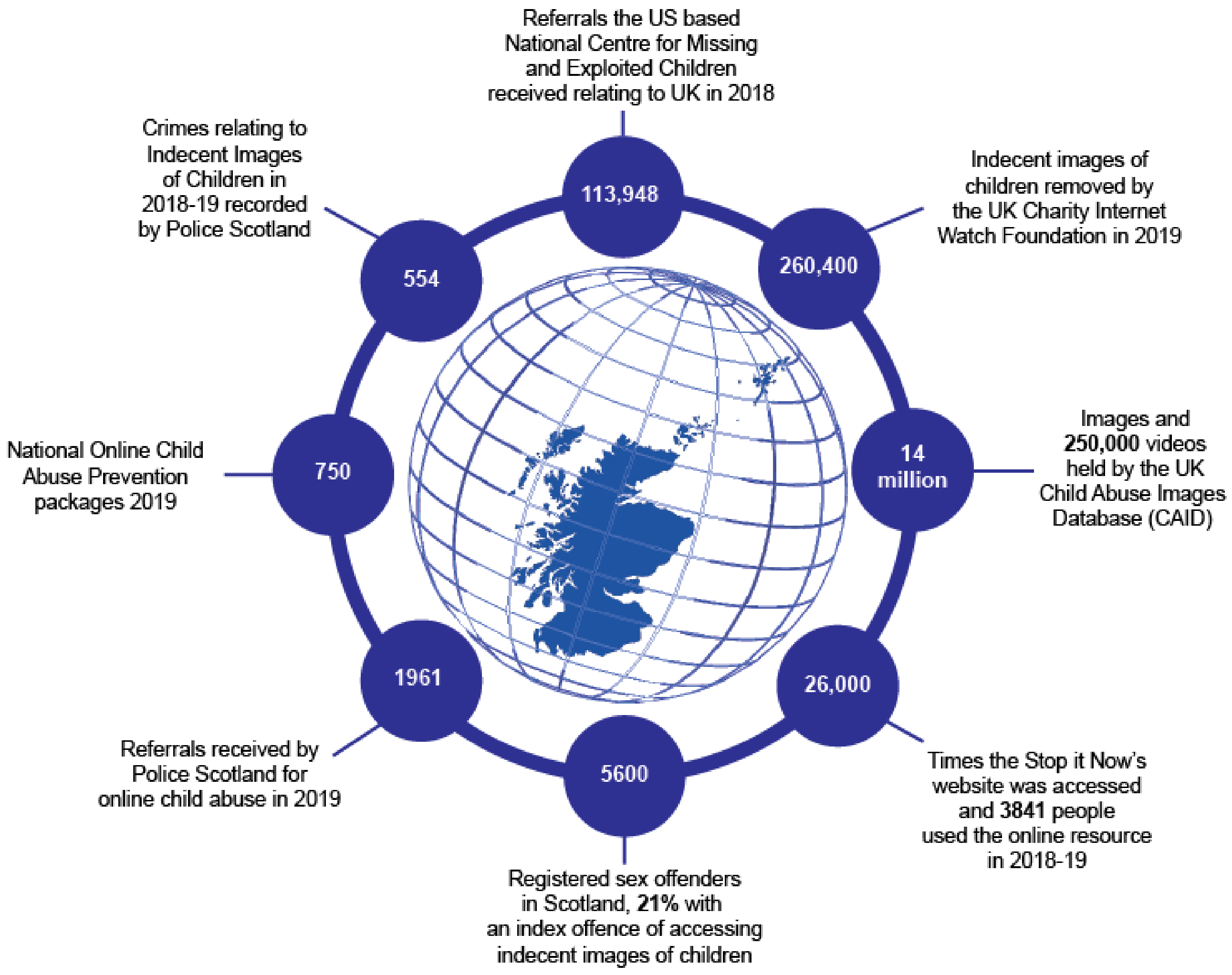
Our approach is to support Police Scotland and the SPA to deliver services that are high quality, continually improving, effective and responsive to local needs.[2]

This review was undertaken by HMICS in terms of Section 74(2)(a) of the Police and Fire Reform (Scotland) Act 2012 and is laid before the Scottish Parliament in terms of Section 79(3) of the Act.

[1] Chapter 11, Police and Fire Reform (Scotland) Act 2012.
[2] HMICS, *Corporate Strategy 2017-20* (2017).

Contents

Key facts



113,948

Referrals the US based National Centre for Missing and Exploited Children received relating to UK in 2018

260,400

Indecent images of children removed by the UK Charity Internet Watch Foundation in 2019

14 million

Images and **250,000** videos held by the UK Child Abuse Images Database (CAID)

26,000

Times the Stop it Now's website was accessed and **3841** people used the online resource in 2018-19

5600

Registered sex offenders in Scotland, **21%** with an index offence of accessing indecent images of children

1961

Referrals received by Police Scotland for online child abuse in 2019

750

National Online Child Abuse Prevention packages 2019

554

Crimes relating to Indecent Images of Children in 2018-19 recorded by Police Scotland

Our review

Online offending in the form of taking, distributing or viewing of indecent images of children, online grooming, inciting children to commit sexual acts online and live streaming of sexual abuse, is child sexual abuse.

This review relates to the Police Scotland response to online child sexual abuse, however the findings should contribute to a wider discussion about how society deals with those who view indecent images of children online. It has previously been suggested by the National Police Chiefs' Council that interventions involving rehabilitation and treatment should be considered for some offenders, allowing police resources to focus on those who present the greatest danger to children.[3]

There are real challenges to capturing the true nature and extent of online child sexual abuse, which are not unique to Police Scotland. The way in which reports of crime are recorded makes it difficult for police to understand the actual level of offending online.

The Police Scotland strategic direction is unclear. There is no evidence of an overarching strategic approach to a growing problem.

Responsibility for tackling different elements of online child sexual abuse sits across a variety of departments in Specialist Crime Division and local policing divisions. Public Protection is the correct professional function to lead the response, yet has the least resources.

Police Scotland devotes considerable time and effort to progressing National Online Child Abuse Prevention (NOCAP) packages, the vast majority of which are generated from intelligence provided by the National Crime Agency, which is the UK receiving agency for all intelligence submitted from global law enforcement organisations, specifically the US National Centre for Missing and Exploited Children.

The processing of NOCAP packages takes up almost all of the resources in the Internet Investigation Unit, and generates significant demand for the Communication Investigation Unit, and the teams tasked with executing the packages.

Whilst an accredited risk assessment tool is used by Police Scotland to prioritise the referrals from the NCA, which are then developed and researched to create NOCAP packages, there is no overall consideration of the impact the effort devoted to progressing these packages is actually making to the levels of offending.

There is no dedicated analytical capability nor centralised intelligence assessment capability directed at online child sexual abuse. The lack of qualitative analytical and intelligence assessment hampers the force's ability to identify future trends and developments, to formulate proactive responses, and to task specialist resources.

There is very little proactive work being carried out in this area of criminality. One of the main proactive tactics would be employing the services of undercover online specialist officers, however this rarely happens.

[3] NPPC, Police chief calls for paedophiles who view child abuse images to be spared prosecution as officers 'can't cope' with volume of reports, 28 February 2017.

Almost half of the online grooming cases emanate from the activities of online child abuse activist groups (vigilante groups), who are unregulated and untrained. A more robust proactive capability on the part of Police Scotland would reduce the opportunities for these groups to operate.

The value of interventions that seek to engage with offenders and those likely to become offenders, is underrated. The service available is inconsistent in terms of coverage across the country, and not part of an overarching national plan. Similarly, resources to support children, young people and their families affected by online child sexual abuse, are not easy to identify or access.

I would like to record my thanks to all those who contributed to this review including police officers and staff in Specialist Crime Division and Local Policing, the National Crime Agency, and a range of agencies providing services for children and young people and interventions for offenders.

Gillian Imery QPM
Her Majesty’s Chief Inspector of Constabulary
February 2020

Introduction

In the HMICS Scrutiny Plan 2019-20 we outlined our intention to conduct a strategic review of Police Scotland's response to cyber enabled, cyber dependent and internet facilitated sexual crime as it relates to children, collectively referred to hereafter as online child sexual abuse.

Cyber enabled criminality is the term commonly used to describe the commission or attempted commission of crimes using the internet, or by otherwise accessing a computer system, device or network.

The aims and objectives of this review are contained in the terms of reference, which were published on 8 October 2019.[4] Those areas of harmful online activity that are not included in this review, such as cyber bullying and sexually explicit electronic messages between children, are made clear in the terms of reference. Child Sexual Exploitation (CSE) is included where it involves online child sexual abuse.

The challenges presented by cyber enabled crime are not unique to Scotland. In 2015, colleagues at Her Majesty's Inspectorate of Constabulary in England and Wales (now Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services) produced a report, 'Online and on the edge: Real risks in a virtual world'.[5]

Many of the issues identified by HMIC back in 2015 remain relevant today and to Scotland, including:

- Volume of Indecent Images of Children (IIOC) presents very real challenges to law enforcement agencies
- Gap between a statement of priority by forces and the reality of practice
- Police forces need to recognise the full spectrum of online offending and its impact on children, analyse the demand on resources and plan effective responses
- Delays with investigations, particularly digital forensic examinations
- Police forces need to understand the nature and scale of offending and look to adopt new approaches.

Police Scotland itself acknowledges that investigation and prevention of online abuse is challenging for a number of reasons:

- technology provides opportunities for offenders to anonymise their activity
- social media companies are not robust in policing their own sites
- covert work around online child sexual abuse has been difficult due to capacity and capability, intelligence and operational support
- underreporting, as with most sexual crimes, is a real issue
- the grooming process is such that many children and young people do not recognise the signs of sexual exploitation and do not realise they are being groomed or abused
- the majority of children and young people are active online and, as a result of the manipulative nature of perpetrators, are at risk of online child sexual abuse.

[4] HMICS, Strategic review of Police Scotland's response to online child sexual abuse – Terms of Reference, 8 October 2019.

[5] HMIC, Online and on the edge: Real risks in a virtual world, July 2015.

In this HMICS review, we posed a number of broad questions designed to provide a thorough overview of Police Scotland's response to online child sexual abuse.

We assessed the response from a strategic, tactical and operations perspective, both locally and nationally. To gain an overview of local service delivery, we looked at three territorial policing divisions: Edinburgh, Tayside and Renfrewshire and Inverclyde.

The Police Scotland response spans a number of different business areas including the Specialist Crime Division departments of Public Protection; Intelligence; Special Operations; Digital Forensics; Cybercrime, and Safer Communities, as well as uniform and detective resources in local policing divisions. Most, and more frequently all, will be involved in the end to end process of online child sexual abuse investigations.

Key Findings

- There is a risk that online child sexual abuse both as a form of child abuse and exploitation and cyber-enabled offending, may be lost within broader crime classifications

- The strategic direction of the force is unclear therefore staff are unable to link their operational activity to the overall aim

- There has been no overall strategic governance of the different parts of the force responsible for delivering different aspects of the response to online child sexual abuse

- There is an acknowledgement by Police Scotland that online child sexual abuse has not been given sufficient prioritisation

- Demand management, prioritisation and tasking weaknesses are symptomatic of governance and organisational structures that would benefit from a comprehensive review

- Specialist support functions need to refocus on those that are most in need of protection rather than their traditional focus on drugs and firearms

- Police Scotland can learn more from the experiences elsewhere through its strategic network

- Police Scotland has introduced effective processes to deal with National Online Child Abuse Prevention packages

- Police Scotland's response is generally reactive with very limited evidence of proactivity

- Local multi-agency child protection arrangements are robustly observed, including those occasions when national police resources are dealing with cases

- Police Scotland has different service delivery models in place to deliver overt operational activity in different areas of the country

- For Police Scotland to deliver on the transformational Cybercrime, Technical Surveillance Programme of change, prioritisation and investment are required

- Police Scotland has taken no action towards achieving accreditation for digital forensics, nor has the issue of where the function is best located (Police Scotland or SPA Forensic Services) been resolved

- Prevention strategies are not being informed by organisational learning due to the absence of analytical products and the lack of evaluation means their effectiveness and impact are unclear

- Different funding arrangements are compounding silo working and having an adverse impact on the delivery of integrated, cohesive prevention work

- The absence of online covert activity by Police Scotland has created a proactive void that undermines any challenge to the legitimacy of Online Child Abuse Activist Groups (OCAG)

Recommendations

Recommendation 1

Police Scotland should improve the means by which recorded data can accurately inform assessment of the scale and nature of online child sexual abuse.

Recommendation 2

Police Scotland should review the level of analytical support provided to the Public Protection business area and consider the appointment of a dedicated analytical resource.

Recommendation 3

Police Scotland should ensure a strategic governance framework is in place, which provides support, direction, scrutiny and quality assurance to the force's response to online child sexual abuse.

Recommendation 4

Police Scotland should undertake an Online Child Sexual Abuse Strategic Threat Assessment to accurately identify the scale, nature and threat to children from online child sexual abuse.

Recommendation 5

Police Scotland should review the current arrangements for allocation of specialist support in relation to online child sexual abuse to ensure the allocation is fair, equitable and meets the needs across the country.

Recommendation 6

Police Scotland should review the resources and structure of the Internet Investigation Unit and Communications Investigation Unit to ensure that the force is able to meet current and future demand in relation to initial risk assessment, triage and intelligence development.

Recommendation 7

Police Scotland and the National Crime Agency should work together to ensure that all capabilities are being exploited to their full potential and intelligence is shared effectively.

Recommendation 8

Police Scotland should work with the Crown Office and Procurator Fiscal Service to establish a pragmatic and realistic approach to digital forensic examination requests.

Recommendation 9

Police Scotland should review its capacity and capability to conduct undercover online covert operations in support of its policing priorities and ensure that undercover online operatives are sufficiently equipped and supported to identify and adequately assess the risk to children as a result of online offending.

Recommendation 10

Police Scotland should ensure that arrangements for deploying undercover online specialist resources are directed by formal tasking arrangements aligned to risk, priority and demand.

Is the nature and extent of online child sexual abuse understood?

1. Online offending and the use of various cyber devices and tools to commit crime has increased significantly in recent years and continues to grow exponentially.

2. Online child sexual abuse can take many forms including the taking, distributing or viewing of indecent images of children (IIOC), online grooming, inciting children to commit sexual acts online and live streaming of sexual abuse. Regardless of the nature of the conduct, online child sexual abuse is first and foremost child abuse and responses require to be compliant with child protection and Getting it Right for Every Child (GIRFEC) arrangements.

3. While aspects of offending of this nature are conducted remotely via the internet, the crime will always involve the abuse or attempted abuse of a child. Those who commit offences online do not necessarily commit contact sexual offences against children, but research shows that this can be the case.

4. Child Exploitation Online Protection (CEOP) research found a 55% correlation in respect of those who had offended in relation to IIOC and contact sexual offences.[6]

5. In January 2020 the Internet Watch Foundation, a UK charity responsible for finding and removing IIOC from the internet, reported a 14% increase in reports of IIOC, from 229,328 in 2018 to 260,400 in 2019. Of these reports, 132,700 revealed images of children being sexually abused, a 26% increase from the 105,047 images in 2018.

6. The remote nature of the internet and its ability to allow individuals to conceal their identity or operate anonymously has facilitated criminal activity that is predicated on targeting those who are vulnerable to exploitation.

7. Children are increasingly living their lives online and, having not experienced a life without the internet, are often significantly more knowledgeable and experienced than the adults responsible for their safety and wellbeing. This can mean that children and young people are vulnerable to abuse and harm online, particularly when unsupervised.

8. The global nature of the internet means that online child sexual abuse can include a cross border or international dimension. IIOC viewed in Scotland may have been as a result of abuse having taken place, and relevant imagery uploaded, from anywhere in the world. Similarly, offenders engaging in grooming children for the purposes of sexual offending can do so from any location. This presents real challenges for law enforcement.

9. Even more challenging are the features associated with the 'Dark Net'. Conventional search engines do not apply to the 'dark net', and communication via multiple relays aids encryption. This has the dual impact of providing enhanced opportunities for criminal conduct such as sharing IIOC, and rendering conventional digital investigatory methods ineffective.

[6] CEOP, A Picture of Abuse, A thematic assessment of the risk of contact child sexual abuse posed by those who possess indecent images of children, 2012.

10. The broader threat posed by cyber enabled and cyber dependant crime, including the specific risk from those who use the internet to facilitate sexual abuse of children, has been recognised at UK and Scottish Government level and are addressed in the respective papers:

    - Online Harms White Paper: April 2019[7]
    - National Action Plan on Internet Safety for Children and Young People: April 2017.[8]

11. Police Scotland measures demand in this area through the numbers of recorded crimes; STORM (System for Tasking and Operational Resource Management) incidents; Scottish Intelligence Database (SID) logs and the number of actionable intelligence packages in relation to both suspects and children at risk (CAR).

12. In 2018, Police Scotland acknowledged the value of having an accurate understanding of this issue from a broader cybercrime perspective:[9]

    “Gaining an accurate picture of the scale and nature of the cyber threat facing Scotland is an essential step in combatting cybercrime”.

    However, it conceded that:

    “It is assessed that cybercrime markers, headers and qualifiers continue to be underutilised across all systems”.

13. Despite this recognition, the Strategic Assessment 2020–2023[10] highlights that failure to accurately record sexually motivated cybercrime continues to be an issue:

    “Understanding the true nature and extent of cyber-enabled sexual crime and child sexual exploitation is difficult due to data quality issues surrounding use of cybercrime markers for recorded crime.”

14. With this caveat, Police Scotland assessed that during 2018, in respect of the broader category of cybercrime:[11]

    - Recorded sexual crime represented 39.7% of all cybercrime
    - 21.9% of all cybercrime STORM incidents related to sexual offences
    - SID logs with a sexual marker represented 45.2% of all cybercrime logs.

15. There is a range of conduct and criminal activity that constitutes online child sexual abuse, consequentially the legislation that covers such offending is spread across a number of separate pieces of legislation. A list of the relevant legislation is contained in Appendix A.

16. Table 1 provides an overview of recorded Group 2, Other Sexual Crimes, which potentially relates to online child sexual abuse. Taking, distributing and possession of IIOC can confidently be regarded as a cyber enabled crime, however the other crimes listed may or may not have a cyber element. This is why it is important that operational staff apply a ‘cybercrime marker’ to crime reports, SID logs and STORM incidents where appropriate.

[7] HM Government, Online Harms White Paper, 8 April 2019.

[8] Scottish Government, National Action Plan on Internet Safety of children and Young People, April 2017.

[9] Police Scotland, Cybercrime Strategic Assessment January - December 2018.

[10] Police Scotland, Strategic Assessment 2020-23.

[11] See footnote 9.

17. The absence of a robust and reliable process by which to filter those crimes that have a cyber element has resulted in uncertainty about the actual extent of these crimes.

Table 1:

Cyber enabled online child sexual abuse	**2014-2015**	**2015-2016**	**2016-2017**	**2017-2018**	**2018-2019**
Taking, distribution, possession of IIOC	603	645	649	658	554
Potentially cyber enabled CSA					
Sexually coercive conduct against a child aged 13-15	333	350	408	392	548
Sexually coercive conduct against a child under 13	385	460	552	576	659
Other sexual crimes involving 13-15 year old children	417	485	452	391	393
Threaten to disclose / disclose intimate image	-	-	-	421	596
Other sexual crimes	64	144	429	492	407

(legislation covering the disclosure/threaten to disclose intimate images was not enacted until 2017-18)[12]

18. Crimes relating to IIOC recorded modest increases in the years 2014-2018; however, there was a 15.8% reduction in the number of cases from 2017-18 to 2018-19. With the exception of ‘other sexual crimes involving 13-15 year olds’, all other crime types have recorded substantial increases.

19. Given the shortcomings in recording processes (dependent on officers and staff applying the ‘cybercrime marker’), it is difficult to determine which of these other crimes relate to online child sexual abuse and whether online offending is increasing or decreasing.

20. Police Scotland however, has intimated that the number of online child abuse referrals has increased by 853% in the last five years to 2019, from 141 in 2013 (the inception of Police Scotland) to 1345 in 2018. Further, it projected that the percentage increase would rise to 1044% by the end of 2019.[13] It is now confirmed by Police Scotland that the number of referrals received by the year end for 2019 is 1961, an increase of 1290%.

21. The vast majority of online child abuse referrals come from the NCA, but some come from other sources such as concerned parents, schools and other partner agencies. Police Scotland’s Internet Investigation Unit prioritises and develops these referrals to create packages. Police Scotland obviously knows the number of NOCAP packages received and actioned, but currently systems are unable to provide data on how many of those packages resulted in a crime report or to attribute crime reports to packages. Further, the force is unable to quantify the portion of online child sexual abuse that is reported at local level from sources other than the NCA.

22. In addition, it reports a 65% increase in the number of recorded offences of communicating indecently with a child over the past six years to 2019, from 359 offences in 2013-14 to 592 in 2018-19.[14]

[12] Scottish Government, Recorded Crime in Scotland 2018-2019, 24 September 2019.
[13] See footnote 10.
[14] Police Scotland report to SPA Board – Response to online CSE, 28 March 2019, private session.

23. The significant increase in online child abuse referrals as reported by Police Scotland however is not reflected in the crime statistics at Table 1 in relation to Indecent Images of Children (IIOC). It is accepted that not all referrals will result in criminal charges, or some may in fact result in charges other than taking, distributing or possession of IIOC. That said, the relatively static numbers for recorded IIOC over five years suggests a capacity issue linked directly to resource availability, rather than crime trends.

24. The picture elsewhere in the UK is one of increased demand, with the NSPCC report, *'How safe are our children 2019 – An overview of data on child abuse online'* indicating that, *"there has been a year on year increase in the number and rate of police-recorded online child sexual offences in England and Wales and Northern Ireland."*[15]

25. It should be noted that greater awareness, increased confidence in reporting and, particularly in England and Wales, improved 'flagging' processes may be factors in the increases in recorded crime, rather than an increase in prevalence. Increases in reports have an obvious impact on police resources.

National Online Child Abuse Prevention (NOCAP) Strategy

26. At the inception of Police Scotland in 2013, the force introduced the NOCAP strategy to deal with offences involving the possession and distribution of Indecent Images of Children. The vast majority of NOCAP packages emanate from reports from the National Crime Agency, which is the receiving agency for intelligence from the US National Centre for Missing and Exploited Children. Since 2013, Police Scotland has experienced a 92% increase in actionable intelligence packages relating to IIOC, from 375 to 722. This resulted in 762 arrests and 381 child concern reports between 2016 and March 2019.

27. Further, where it is assessed that there is an ongoing risk to an identified child as a result of his/her own risk-taking behaviour, such as publishing self-generated intimate images, Children at Risk (CAR) packages are created for harm reduction intervention at a local level. In the same period between 2016 and March 2019, 287 such packages were created.[16]

Registered Sex Offenders and potential offenders

28. The National Offender Management Unit (NOMU) conducted a profile of all those registered as sex offenders and being managed under formal MAPPA arrangements as at March 2018.

29. Of the 5600 registered sex offenders (RSO) at that time, 1180 (21.1%) had IIOC as their index offence. The index offence is the principal offence by which they were convicted, therefore the true number of RSO with a conviction for IIOC is likely to be higher.

30. A further 21.5% (1204) had 'sexual activity with a child' as their index offence. It is unclear from this information whether the internet was a feature of their offending, however it is reasonable to assess that there will be a percentage to which this will be applicable.[17]

31. The national child protection prevention charity, Stop It Now, provides support services to individuals with problematic sexual thoughts and those at risk of offending. In conjunction with Police Scotland, they ran campaigns in respect of online child sexual abuse during 2018 and grooming during 2019. The official Stop It Now figures for Scotland in 2019 confirm that their web pages were accessed over 26000 times. Further, 3841 people used their online resource for adults worried about their sexual behaviour online, and 543 people used their resource for adults worried about their sexual thoughts and feelings towards children.[18]

[15] NSPCC, How safe are our children, 2019.
[16] See footnote 14.
[17] Stop it Now!, Police Scotland Registered Sex Offender (RSO) Profile for Scotland, April 2018.
[18] Stop It Now!, A year in review 2018/19.

Understanding the nature and scale

32. While it is vital that online child sexual abuse is identified and dealt with as a child abuse, failure to accurately categorise the specific nature of the abuse adversely affects prevention, disruption and investigatory strategies, as well as the effective allocation of resources.

33. At its inception, Police Scotland inherited disparate IT systems from legacy forces and it continues to work to overcome the challenges this presents in terms of how data is collected, recorded and retrieved across the country. As a result, whilst the data does exist, it is not in a readily useable format and is therefore of limited value from an analytical perspective.

34. Consequently any analysis conducted in terms of online child sexual abuse will either be restricted as a result of the limited and unreliable nature of the data, or be considerably cumbersome and problematic.

35. It is noted that Police Scotland has taken steps to address the deficiencies of its data collection processes, having recently appointed a Chief Data Officer and is in the process of developing data strategies to transform the available data into a more useable form.

36. Many of the territorial divisions have developed local problem profiles however they all relate to broader disciplines including Group 2 crimes, CSE or cybercrime, with a cursory mention of online child sexual abuse within. Only five out of 13 divisions provided such reports (A, G, J, K and U), as did the Analyst and Performance Unit (APU) and Safer Communities. While online child sexual abuse is a feature of the individual analytical products, HMICS found that the detail and focus varies.

37. When dealing with an online child sexual abuse case, local policing divisions are required to submit a NCAIU Tasking and Referral Form. The purpose of this form is twofold, firstly, where required, to request specialist support from NCAIU, and secondly to assist in determining the true scope and nature of child sexual abuse, including that which has an online element. Unfortunately not all divisions submit the relevant form, particularly where there is no request for additional resource.

38. The Online Grooming of Children in Scotland Strategic Threat Assessment[19] was produced in April 2019. Significant findings include:

- *95 offences of online grooming of children for the purposes of sexual offences were recorded in 2018-19*
- *This represents almost double those offences recorded in the period 2016-17*
- *Less than 10% of offenders were RSO at the time of the offence*
- *The majority of the offenders were unknown to police for previous sexual offending*
- *The number of relevant intelligence logs is low when compared to the level of grooming offending, assessed due to a lack of a dedicated intelligence marker.*

[19] Police Scotland, Online Grooming of children in Scotland Strategic Threat Assessment, April 2019.

Current Picture

39. There has been some activity to try to establish the scope and nature of online child sexual abuse across Scotland, however inhibitors have included challenges in relation to the use of ‘markers’ and incompatible data systems.

40. That said, most of the analytical work conducted relates to the broader disciplines with a limited focus on the online child sexual abuse aspect of child abuse.

41. There is an ongoing drive to improve the use of intelligence markers as they relate to cybercrime. The instruction to apply such a marker was first issued in a force memo in April 2016, and was reinforced by a further memo in October 2018. The Cybercrime Strategic Assessment January – December 2018[20] highlighted the inaccurate use of the cybercrime marker. The introduction of a marketing strategy, ‘Tag It, Mark It, Log It’ is aimed at achieving improvements in this area.[21]

42. In the absence of integrated data systems, HMICS considers it is an essential requirement to ensure the appropriate use of such intelligence markers to assess accurately the scope of online child sexual abuse across Scotland. HMICS notes that the absence of quality data has been of concern to business leads for some time and some localised efforts have been made to address this issue.

Recommendation 1

Police Scotland should improve the means by which recorded data can accurately inform assessment of the scale and nature of online child sexual abuse.

43. Scottish Government Project Funding has recently been secured to employ three additional dedicated analysts to Cybercrime Intelligence and Digital Forensics. However, none of these posts has a specific remit to analyse the scope and impact of child abuse, including that committed online. Further, there is no dedicated analyst assigned to the various business areas that are the strategic responsibility of SCD Public Protection. As a result, any request by Public Protection for analytical work has to compete with other business areas. The subject of online child sexual abuse, and indeed SCD Public Protection business area, would benefit from dedicated analytical support in what is undoubtedly a growing area of business.

44. In 2018 we conducted a *Thematic Review of Police Scotland’s approach to the development and operational delivery of the Annual Police Plan 2018-19.*[22] At that time we found an imbalance between intelligence analysis and performance analysis and asked Police Scotland to consider a more direct alignment of intelligence analysts and SCD. The structure however remains as it was and we are of the view that the absence of meaningful analytical products to fully inform the scale, nature and future threat of online child sexual abuse symptomatic of the flaws in the current structure.

Recommendation 2

Police Scotland should review the level of analytical support provided to the Public Protection business area and consider the appointment of a dedicated analytical resource.

[20] Police Scotland, Cybercrime Strategic Assessment January – December 2018.
[21] Police Scotland internal memorandum 2018.
[22] HMICS, Thematic Review of Police Scotland’s approach to the development and operational delivery of the Annual Police Plan 2018-2019, 13 December 2018.

What are Police Scotland's leadership and governance arrangements, and what is the strategic direction to tackle online child sexual abuse?

45. The Police Scotland Executive lead for online child sexual abuse is the Deputy Chief Constable Crime and Operations. The subject cuts across business areas, therefore the Assistant Chief Constable with responsibility for Major Crime and Public Protection, and the ACC for Organised Crime, Counter Terrorism and Intelligence both have strategic command roles. There is clear commitment from the current post holders at ACC and DCC levels to work together to tackle online child sexual abuse, however effective strategy and governance require to be in place to ensure this is maintained when individuals move posts.

46. The force has structured its strategic approach around the three principal strands of Prevent, Protect and Disrupt/Pursue offenders, and the significant threat of online child sexual abuse is reflected in various strategic products.

47. Child sexual abuse and exploitation is listed as a priority in the current Police Scotland Strategic Assessment, and protecting vulnerable people and tackling cyber related crime both feature in the current 2019-20 Police Plan:[23]

    "Our strategic assessment tells us we must direct our resources to protect vulnerable people and address issues that cause the most harm, including rape and sexual crime, domestic abuse, child sexual abuse and exploitation and human trafficking. Crime is also becoming more complex and we will enhance our capability to address the cross-cutting threat from cyber related crime."

48. The latest Police Scotland Strategic Assessment 2020-23[24] has graded CSE at the highest level, as a 'very high operational policing priority'.

49. '2026 - Serving a Changing Scotland'[25] strategy for policing in Scotland acknowledges the threat from cyber enabled criminality and outlines a long-term approach that includes enhancing its cyber capabilities as does the Joint Strategy for Policing 2020, which is currently out for public consultation.

50. A critical feature of the ability to assess accurately the scale of the issue and to anticipate and plan according to future demand is reliable analytical products that can inform discussions and decision making. So, while the various documents consistently reinforce the significance of CSA in the cyber world, significant weaknesses in data collection and analysis processes have failed to map a true picture of the problem.

51. This is partly why HMICS found that there was in effect no clear overarching strategic direction that clearly articulates Police Scotland's intention and aspirations in relation to tackling the threat of online child sexual abuse. While it is clear that online child sexual abuse now features more significantly than in recent years, there is still work to do to convert the various distinct elements into an identifiable, coherent strategic direction capable of being communicated internally and externally.

[23] Police Scotland, Annual Police Plan 2019-20.
[24] Police Scotland, Strategic Assessment 2020-23.
[25] Police Scotland, 2026 - Serving a Changing Scotland, 20 June 2017.

52. Our review confirmed that staff we spoke to in local policing and other areas responsible for delivering a front line response were unclear about the existence of a force strategic direction in relation to online child sexual abuse.

53. Police Scotland is an active member of important national (UK) strategic network arrangements including the jointly chaired National Crime Agency/UK Government Pursue and Prevent Boards and the National Police Chiefs' Council (NPCC). Online child sexual abuse features prominently in both forums.

54. These forums meet to progress strategic actions at a UK level and we found that this provides Police Scotland with the appropriate platform and interface from which to both contribute and benefit.

55. The Police Scotland Tackling Online Child Sexual Abuse (TOCSA) Strategic Group was established to provide appropriate governance and strategic direction in relation to online sexual offending against children. Membership includes ACC OCCTU and Intelligence, Detective Chief Superintendents from Public Protection, Intelligence, OCCTU and local policing. The group is chaired by ACC Major Crime and Public Protection and includes additional representation from the Analysis and Performance Unit and COPFS. The group was scheduled to meet on a quarterly basis but this had fallen away over recent years.

56. While all of the relevant constituent functions had a clear understanding of the organisational risk as well as the individual and collective risk to children presented by online child sexual abuse, we found that distinct departmental priorities created a 'silo based' approach.

57. HMICS found that the TOCSA Strategic Group has recently been reinstated in the strategic diary, however this group had not met for some considerable time. As a result, there was previously no structure in which to hold the respective Detective Chief Superintendents to account. It is reasonable to assume that the absence of this strategic structure has contributed to the disconnect between the constituent elements of the end-to-end response.

Recommendation 3

Police Scotland should ensure a strategic governance framework is in place, which provides support, direction, scrutiny and quality assurance to the force's response to online child sexual abuse.

58. The Tasking Online Child Sexual Abuse Tactical Group formulates policy and practice in support of the strategic group. It is chaired by the SCD Public Protection Detective Chief Superintendent and business delivery is supported by a Strategic Action Plan that is structured around the four strands of Prevent, Protect, Pursue and Disrupt.

59. This tactical level group has continued to meet regularly over the years, however it was reported to have had varying levels of commitment from some of the relevant departments and only able to exercise limited impact and influence. This was compounded by the fact that the strategic group had ceased to meet. However, the tactical group has recently been refreshed and seems to have successfully brought together key stakeholders from the relevant departments and is now driving policy in a collaborative manner. Tactical issues of concern such as backlogs, appropriate prioritisation and resourcing challenges are discussed and solutions sought.

60. Given the history of disparate approaches, this group has an integral role to play in ensuring appropriate cohesion and collaboration between departments in delivering the end-to-end response. HMICS considers that it is vital for the tactical TOCSA group to have the support of and mandate from the strategic TOCSA group.

61. Police Scotland has in place individual Strategic Assessments for thematic business areas (including cybercrime and online grooming) in addition to the overarching organisational Strategic Assessment that features online child sexual abuse. Separately the NCA, as a critical partner to tackle online child sexual abuse, has its own Strategic Assessment. These products were developed in isolation and whilst they do not appear to be in conflict with each other, it would be good practice for Police Scotland and the NCA to collaborate more on future assessments.

62. Despite this being a rapidly increasing area of police business, Police Scotland has no specific Strategic Threat Assessment that addresses the issue of online child sexual abuse. Rather online child sexual abuse is a cursory feature contained within a broader perspective. A Strategic Threat Assessment is an essential product in identifying the scale, nature and threat of any issue and in informing strategic planning. Its absence is impeding a coherent strategy for dealing with online child sexual abuse.

Recommendation 4

Police Scotland should undertake an Online Child Sexual Abuse Strategic Threat Assessment to accurately identify the scale, nature and threat to children from online child sexual abuse.

Are organisational structures and tasking and co-ordinating arrangements effective in supporting operational activity to tackle online child sexual abuse?

63. As outlined previously, online child sexual abuse cuts across various Police Scotland business areas. Police Scotland identifies the key functions as:

    - Overt response
    - Covert Response
    - Digital Forensics
    - Intelligence
    - Prevention

64. The overt, front line operational response is largely met by territorial policing (local divisions) and the National Child Abuse Investigation Unit (Public Protection, SCD); covert options are delivered by the Specialist Operations Unit (OCCTU, SCD); digital forensic services sit within the cybercrime unit (OCCTU, SCD); intelligence is the remit of the National Intelligence Bureau and Internet Investigation Unit (Intelligence, SCD), and prevention is primarily the responsibility of Safer Communities (National Safer Communities, SCD).

65. The distinct nature and different line management of each of these operational functions presents a challenge to coherent and co-ordinated activity. Our review found that historically and in the recent past there was a silo based approach where individual departmental priorities and resources were protected to the detriment of a collaborative response. There is clear commitment from the current post holders across functions at Detective Chief Superintendent, ACC and DCC levels to work together to tackle online child sexual abuse, however it will take time and leadership to ensure the previous protectionist culture is eliminated.

SCD Multi-Agency Tactical Tasking and Co-ordinating Group

66. One of the main purposes of Specialist Crime Division is to provide specialist support to front line policing and to ensure appropriate prioritisation and resource allocation. The Multi-Agency Tactical Tasking and Co-ordinating Group is the forum where bids for SCD resources are considered.

67. Local policing however reported that the process of bidding for specialist support through the Tactical Tasking and Co-ordination Group is rarely used: rather this is achieved through direct contact with the relevant department. This seemed to be as a result of low confidence in the formal tasking arrangements combined with the experience of having secured support through informal means. This is consistent with the findings of our 2018 report which states *"many of those we interviewed... indicated that most requests would be made by telephone and often relied on existing personal relationships".*[26]

68. The finite nature of resources and inevitable tensions of competing demands make this an unreliable arrangement. It fails to ensure that resources are allocated on the basis of priority and means the actual demand for specialist resources is not recorded.

[26] HMICS, Thematic Review of Police Scotland's approach to the development and operational delivery of the Annual Police Plan 2018-2019, 13 December 2018.

69. Of the seven, bi-monthly tasking documents (Action Logs covering the period October 2018 to October 2019) that we reviewed during our evidence gathering phase, the only potential reference to online child sexual abuse was in relation to the broader business area of cybercrime, in particular in respect of analytical products.

70. Our 2018 *Thematic Review of Police Scotland's approach to the development and operational delivery of the Annual Police Plan 2018-19*[27] report highlighted the failings of tasking arrangements in respect of demand for specialist support from the various SCD departments. We found a lack of consistency and transparency in the recording of specialist support requests and deployments. At that time we issued a recommendation (recommendation 6) that Police Scotland should develop appropriate reporting processes to address this.

71. This review found that the tasking arrangements continue to fall short of providing accurate and transparent deployment details capable of scrutiny.

72. The serious and organised crime (SOC) mapping process is the tool used to identify those serious and organised crime groups that present the greatest risk of harm to communities, and this in turn assists in determining the SOC priorities for the force.

73. Despite CSE, including that which is conducted online, being a form of SOC, the structure of the SOC mapping process does not lend itself to this type of offending, having been established to address the 'more traditional' crimes involving firearms, drugs and serious violence. As a result, child abuse rarely features as a proirity when allocating technical and physical resources. The current mapping process does not adequately provide the means by which to identify those that create the greatest risk of harm, and therefore it does not sufficiently protect those most at risk of harm.

Weekly NOCAP Strategy Group

74. A weekly inter-departmental meeting convenes each Monday, attended by the Internet Investigations Unit (IIU), Cybercrime Unit and NCAIU. This is effectively a tasking forum that facilitates discussion around the NOCAP packages that are actionable and deals with prioritisation and grading of risk. This forum is chaired by IIU and, using the KIRAT2 (Kent Internet Risk Assessment Tool), actionable packages are graded according to risk. This meeting provides an opportunity for overview of the current risk and the anticipated immediate specialist resource requirement across the force.

75. HMICS found that the process for assessment of the requirement for specialist resources is not reliable as packages that are distributed to overt resources require some additional local enquiry including warrant applications, and the relevant timescales in relation to this activity cannot be accurately determined. As a result, on a regular basis, specialist support such as onsite preview examination and equipment triage is requested in the form of a telephone call direct from divisions to the local Cybercrime Unit hub.

76. It was notable that territorial policing resources were more familiar with the weekly NOCAP Strategy Group meeting than the SCD tactical tasking meeting, which is a reflection of the current value of the SCD tactical tasking process in relation to online child sexual abuse.

[27] HMICS, Thematic Review of Police Scotland's approach to the development and operational delivery of the Annual Police Plan 2018-2019, 13 December 2018.

77. The use of less formal arrangements for securing specialist and/or additional resources is not in keeping with a balanced and impartial allocation of such resources and is not conducive to effective planning.

Recommendation 5

Police Scotland should review the current arrangements for allocation of specialist support in relation to online child sexual abuse to ensure the allocation is fair, equitable and meets the needs across the country.

Is the intelligence function efficient and effective in tackling online child sexual abuse, and what is the quality of the interface with other law enforcement agencies?

78. The global nature of online child sexual abuse requires interface with law enforcement across the world. The NCA is the principal law enforcement partner of Police Scotland and is the receiving agency for all intelligence submitted from international organisations, such as the US National Centre for Missing and Exploited Children (NCMEC).

79. The multi-agency Scottish Crime Campus at Gartcosh accommodates key SCD departments and their tactical leads, including National Intelligence Bureau, SOU, Cybercrime Unit and Digital Forensics Unit. The Scotland regional hub of the NCA is also located in Gartcosh. The philosophy of collaboration between law enforcement partners led to the creation of the crime campus, and it would be reasonable to expect this would result in a cohesive and co-ordinated approach to tackling online child sexual abuse.

80. Despite the critical responsibility that NCA has in tackling the global threat of online child sexual abuse in the UK, HMICS found a potential disconnect with Police Scotland that may impede more effective collaborative working.

81. Further, whilst undoubtedly forming a valuable part of the wider strategic network of statutory organisations, there was limited evidence of Police Scotland benefiting from the inevitable organisational learning opportunities that these strategic arrangements provide.

82. HMICS therefore considers that Police Scotland would benefit from reflecting on its current role within the broader strategic framework and work to enhance the opportunities available for continuous improvement in respect of its strategic, tactical and operational response.

83. HMICS found that much of this has already been identified with two continuous professional development (CPD) events scheduled for January 2020 to address CAID and Cybercrime Investigation: ‘From Examination to Court’. In addition, a joint strategic meeting between NCA and Police Scotland is being planned for early 2020 to facilitate discussion in relation to enhanced interface and joint working.

84. Intelligence in relation to NOCAP packages (relating predominantly to IIOC but including online grooming) are initially considered by the Internet Investigations Unit (IIU), who are responsible for further development of the intelligence to a point where it converts to an actionable package.

85. This includes intelligence that originates from outwith Police Scotland including the CEOP (Child Exploitation and Online Protection, command area of NCA) and NCA’s operation with a specific focus on ‘dark net’ activity.

86. Increased activity and pressure globally to encourage technology companies to take a more responsible approach to what their websites can facilitate, has resulted in an increase in reports to law enforcement agencies. US technology companies alone made over 18.4 million referrals in respect of child sexual abuse material to the NCMEC during 2018, 113,948 of which related to the UK. In the third quarter of 2018 for example, Facebook removed 8.7 million pieces of child nudity and sexual exploitation content.[28]

[28] HM Government, Online Harms White Paper, 8 April 2019.

87. Imminent improvements to technology to assist in detecting offending activity, increased co-operation from technology companies and a constant pressure on those companies to do more, will undoubtedly lead to more referrals and consequently more demand on law enforcement across the world.

88. A percentage of these referrals are Scotland-related and are received by Police Scotland in the form of intelligence via the NCA.

89. The two units predominantly involved in online child sexual abuse matters under the Pursue strand are the IIU and the Communication Investigations Units (CIU), both of which sit within the Intelligence function. As the point of receipt of all online child sexual abuse referrals, the IIU report that 95% of their daily business relates to this, and in particular to NOCAP packages.

90. The current resource level within the IIU is: one Detective Inspector, two Detective Sergeants (permanent posts), five Detective Sergeants (seconded exclusively for NOCAP, one of whom is SOU), and 21 Detective Constables.

91. With very few exceptions, all NOCAP packages require some level of essential telecommunications data to inform the intelligence picture, assess risk and validate suspect details and this is the function of the CIU.

92. As of 25 November 2019, IIU was in receipt of 1600 referrals for the year which is a 40% increase on the same period in 2018. This intelligence resulted in 750 NOCAP packages.[29] Police Scotland has since confirmed that the total number of referrals for the 2019 calendar year is 1961, which generated 913 packages.

93. As a result of this increase in referrals, dealing with NOCAP has significantly affected the ability of the IIU and CIU to service other areas of business.

94. Previously NCA carried out some development of intelligence prior to onward transmission, however Police Scotland took over this responsibility in order to reduce time delays thereby maximising the chances of the intelligence leading to a successful warrant application. Police Scotland has introduced various improvements to the process and this success has had the inevitable impact of increasing the workload of the IIU and the CIU.

95. Further, additional funding to Regional Organised Crime Units across England and Wales, and in particular to NCA, is likely to result in an increase in their capacity and with it an increase in referrals. The NCA is not responsible for the operational enforcement activity in Scotland, consequently the burden of triage, tasking and enforcement rests with Police Scotland.

96. Currently in Police Scotland, volumes in the context of resource levels are such that there is a blacklog within IIU that varies but, as an example, was sitting at 450 in November 2019. All of the intelligence packages under development are subject of an initial triage process and risk assessment using an accredited risk assessment tool.

97. The levels of referrals have continued to increase and are anticipated to continue to increase at a significant rate. As such, the resource levels committed by Police Scotland to deal with the initial risk assessment, triage and intelligence development in respect of NOCAP requires urgent review.

[29] Police Scotland during fieldwork November 2019 and follow up in February 2020.

Recommendation 6

Police Scotland should review the resources and structure of the Internet Investigation Unit and Communications Investigation Unit to ensure that the force is able to meet current and future demand in relation to initial risk assessment, triage and intelligence development.

98. The volume of NOCAP packages was identified as a risk on 5 June 2019 and included in the SCD Risk Register. This was escalated to a 'tier 2', national risk on 5 August 2019 under the risk category 'Public Confidence':[30]

> *"If there is insufficient capacity and capability within the Internet Investigations Unit to progress NOCAP packages, there is a risk that time critical online child protection investigations are delayed."*

99. The breakdown of posts within SCD at January 2020 is as follows.

Table 2:

	Police	**Staff**	**Total**
ACC Specialist Crime & Intel			
Intelligence Support	332.71	65.96	398.67
Specialist Crime Support	68.50	19.71	88.21
Organised Crime & Counter Terrorism	796.31	172.98	969.29
Total ACC Specialist Crime & Intel	**1197.52**	**258.65**	**1456.17**
ACC Crime & Protection			
Local Crime	20.00	13.27	33.27
Major Crime	335.74	43.26	379.00
Public Protection	203.34	19.60	222.94
Historic Child Abuse Investigation	18.35	---	18.35
Total ACC Crime & Protection	**577.43**	**76.13**	**653.56**
Safer Communities	**94.46**	**4.70**	**99.16**

100. Our review found that resources were an issue in terms of responding to the ever-increasing demand and risk presented by online child sexual abuse. There is particular pressure placed on the small team in the Internet Investigation Unit. Public Protection is the correct specialist area to lead the response online child sexual abuse, yet has fewer resources than other areas of Specialist Crime Division. HMICS would encourage Police Scotland to review the distribution of posts across SCD, in keeping with the force's strategic priorities and commitment to protecting those at greatest risk of harm.

101. The 2020-23 Strategic Assessment recommends that the force undertakes a review of the workforce capacity across SCD intelligence, special operations, digital forensics and NCAIU.

[30] Police Scotland Risk Register.

102. The volume of demand is such that it is overwhelming existing capacity, and this is expected to become ever more challenging in the form of processing and prioritising NOCAP packages. There is an opportunity to rethink how to deal with those intelligence packages that are assessed as lower risk following the application of the accredited risk assessment tool.

103. HMICS would support a move towards the consideration of alternative interventions in relation to those who are assessed as presenting lower level risk as part of a range of measures to overhaul the intelligence function, including resource commitment and the establishment of a threat desk.

Interface with NCA and other law enforcement

104. Police Scotland's principal law enforcement partner in respect of online child sexual abuse is NCA. They are the conduit for Scotland-related intelligence referrals from across the world, however, they do not provide investigative resources for online child sexual abuse and they do not carry the risk associated with any referrals they pass to Police Scotland.

105. HMICS found that this has presented challenges in the past in terms of time taken to carry out research (para 94), and this has resulted in revised processes. The NCA leads the UK Online Pursue response to 'dark net' offending. Our review identified differing views on the part of NCA and Police Scotland about how to use intelligence. Once Police Scotland has received the intelligence from the NCA, it carries the risk caused by any delay.

106. At the time of our review this delay had been acknowledged by both Police Scotland and the NCA and steps were underway to address this situation. Given that some of the most prolific and concerning activity takes place within 'dark net' space, HMICS considers this requires an urgent solution.

107. The NCA reports that there are rich opportunities to identify offenders and inform prevention activity that are available to all law enforcement, however they are not being utilised to their full capacity by Police Scotland.

108. Police Scotland contributes £5.2m annually to be part of the UK Organised Crime Partnership and should benefit from the assets and expertise held by the NCA.

109. HMICS found that there were missed opportunities to tackle online child sexual abuse that require to be urgently addressed and we would encourage Police Scotland and NCA to take whatever measures are required to establish common ground and address any issues.

Recommendation 7

Police Scotland and the National Crime Agency should work together to ensure that all capabilities are being exploited to their full potential and intelligence is shared effectively.

110. While Police Scotland has access to the Child Abuse Image Database (CAID) and NCMEC portals, each of these systems requires to be independently accessed during the IIU triage phase. This is a time consuming and cumbersome process. A business case has been submitted to introduce a management system that automatically links to both databases simultaneously. The introduction of such a system would significantly improve turnaround timescales for referrals.

Proactivity

111. HMICS found that Police Scotland puts significant effort into dealing with NOCAP packages, which relate to individuals with an unhealthy interest in children, and has developed effective processes to deal with the volume. To this extent, the force is contributing to keeping children safe online.

112. Our review found however that the success of NOCAP was the principal focus of Police Scotland activity, to the detriment of any degree of proactivity or undertaking to 'travel upstream' and go beyond just those individuals within local communities that are subject of the NOCAP packages.

113. HMICS found this to be the case in all of the constituent departments with a functional role in online child sexual abuse investigations.

Intelligence Requirement

114. The 2020-23 Force Strategic Assessment outlines an intelligence requirement to gather, develop and enhance intelligence in relation to:

- *the scale and nature of child sexual exploitation across Scotland to protect children from harm*

and in relation to the broader cybercrime:

- *cyber-enabled crime in order to improve our understanding of the threat, to prevent criminality and protect Scottish communities and interests*
- *the 'dark net' – in order to improve our understanding of the threat to prevent criminality and protect Scottish communities and interests.*

115. At the time of our review the Strategic Assessment had not yet been published and there was no associated communication strategy available. HMICS is therefore unable to assess how these intelligence requirements will be addressed.

116. The National Child Sexual Exploitation Intelligence Toolkit, published on 2 February 2017, identified an intelligence gap in relation to CSE and its primary aim is to:

- Raise awareness of the signs of CSE
- Improve the recognition and capture of CSE intelligence
- Fill intelligence gaps within and across Scotland to proactively prevent, disrupt and deter those who seek to sexually exploit children.

117. In our *Thematic Review of Police Scotland's approach to the development and operational delivery of the Annual Police Plan 2018-19*[31] we highlighted the positive development of the establishment of national threat desks to support some areas of business including firearms and human trafficking. The threat desk structure is effective in identifying threat and risk, to highlight intelligence gaps and to make recommendations to mitigate against emerging threats.

118. It is of note that, despite acknowledging the significant risk presented by online child sexual abuse, there is no threat desk structure to collate intelligence in relation to online child abuse obtained from various sources. An online child sexual abuse threat desk would facilitate qualitative intelligence assessment, which would more accurately identify areas of concern such as intelligence gaps, connections between offenders and prevention and disruption opportunities.

[31] HMICS, Thematic Review of Police Scotland's approach to the development and operational delivery of the Annual Police Plan 2018-2019, 13 December 2018.

119. Despite the intelligence gap, and Police Scotland's stated commitment to address it, we found only limited evidence that it was actively pursuing or developing means by which to extract the intelligence that is undoubtedly available from offenders who seek to sexually exploit children about their networks, websites and other offenders.

120. Opportunities to collect intelligence from non-statutory partners have been disproportionately impacted by the General Data Protection Regulation (GDPR) since its introduction in 2018. This missed opportunity has been recognised by Police Scotland who have subsequently developed a police information sharing portal. This is due to be piloted in the Highlands and Islands division with an estimated start date of February 2020.

How effective and consistent is the front line service delivery response to cases of potential online child sexual abuse and what is the level of support provided by specialist resources?

121. Intelligence packages (NOCAP) that have been developed to the stage that they are actionable are disseminated to front-line officers to conduct overt operational action. These packages have already been subject of KIRAT2 risk assessment and arrive at the division or department with a grading of Red (high priority) or Amber (standard risk).

122. The structures and resources that carry out the overt operational activity at divisional level vary across the country. However, HMICS did not find evidence that this variation adversely affected the quality of response locally.

West

123. Packages relating to the divisions in the West of the county (Greater Glasgow; Ayrshire; Lanarkshire; Renfrewshire and Inverclyde; Dumfries and Galloway, and Argyll and West Dunbartonshire), are allocated to divisional resources. These include Proactive Units, Community Investigation Units, Public Protection Units or Community Policing teams. Some divisions have a policy of consistently using specified resources to deal with NOCAP, eg Child Protection or Public Protection teams, while other divisions allocate packages according to capacity and resource availability. Those divisions that allocate packages to resources other than public protection teams ensure there are productive relationships between child protection officers and the officers tasked with executing the packages.

124. Those divisions with a policy of using specified resources benefit from a level of consistency, expertise, improved partner relationships and robust management oversight in relation to the progress of individual packages.

North

125. The North divisions (Highlands and Islands; North East and Tayside) apply a blended response. An aspiration of the NCAIU in the Highlands and Islands is to take responsibility for all NOCAP packages in the North. The volume of core business being undertaken by NCAIU however has made this unachievable.

126. As a result, NCAIU currently deal with all red, high-risk packages. All amber graded packages are allocated to local divisional teams. In common with the arrangements in the West, the local divisional allocation of packages varies.

127. Tayside division for example has established a dedicated Online Sexual Crime/NOCAP Team (OSCT) consisting of one Detective Sergeant, two Detective Constables and four Constables from divisional policing on one year attachments. This team sits within mainstream CID rather than Public Protection.

128. Other divisions in the North utilise resources according to capacity and availability, and rely on constructive interface between child protection officers and front line response officers. The geography presents particular challenges, particularly in respect of the islands where using local officers is the most pragmatic response to minimise delays in dealing with risk and harm.

East

129. The East (Edinburgh; Fife; Forth Valley and The Lothians and Scottish Borders) is the only area that currently operates with a dedicated unit to deal with all NOCAP packages. This is a unit that was introduced by the legacy Lothian and Borders Police. The unit's geographical remit expanded to include Fife and Forth Valley following the transition to Police Scotland. Until recently, the dedicated unit sat within Cybercrime (OCCTU), but has now moved across to SCD Public Protection where it sits within the NCAIU structure.

130. Given that online child sexual abuse is child abuse, it is difficult to understand the logic of the unit dedicated to dealing with NOCAP packages being under the line management of OCCTU. HMICS considers the transfer to Public Protection to be a welcome move and one that should be considered during any Police Scotland review of delivery models.

National Child Abuse Investigation Unit

131. The NCAIU operates from resource hubs located in Glasgow, Aberdeen, Inverness and Livingston. The hub in Dundee has been agreed and internal recruitment is underway.

132. NCAIU deals with all NOCAP packages in the East, regardless of the risk grading. It deals with all high-priority red packages in the North and only those packages in the West that are regarded as sensitive in relation to either the suspect or known victims.

133. The aspiration for NCAIU to assume responsibility for all NOCAP packages in the East and North (as an incremental arrangement in the medium term) has been impacted by the resource commitment to the Scottish Child Abuse Inquiry. That resource commitment is likely to continue until the conclusion of the Inquiry.

134. The NCAIU Detective Inspector attends the weekly NOCAP Straegy Group meeting chaired by IIU to ensure that child protection matters are appropriately and adequately considered.

135. The NCAIU can assume ownership of any online child sexual abuse investigation where it is considered necessary due to the complexity, protracted nature and/or sensitivities of the particular case. HMICS found that, on such occasions, local child protection arrangements were respected and prioritised, and divisional public protection units were provided with appropriate and timely notification to initiate local multi-agency child protection processes.

Summary of delivery models

136. The delivery model adopted across Police Scotland in relation to online child sexual abuse varies according to local structures and resources.

137. HMICS does not suggest that the model needs to be the same throughout the country. However, what does need to be consistent is the quality of response to cases of online child abuse.

138. Those divisions that are supported either entirely or in part by a dedicated, specialist response benefit from the professional expertise and consistency that those units provide. It also means that other divisional resources do not need to be identified to deal with the demand.

139. That said, there is an advantage for frontline response and community officers to gain experience in this area of business. Not all cases of online child sexual abuse come to police attention in the form of a NOCAP package. Where concerns about online grooming emerge locally, these are likely to be reported by a concerned parent or teacher to local response or community officers. Officers in the West of the country reported the advantages of sharing the experience beyond dedicated units.

Local Governance, Guidance and Quality Assurance

140. Police Scotland has published various guidance documents to assist operational officers in dealing with online child sexual abuse, including the Indecent Images of Children on Digital Media Standard Operating Procedure, NOCAP Investigation Toolkit and CSE Intelligence Toolkit. These were described by staff as being extremely useful and informative.

141. Our review found that national guidance was frequently supplemented by local training and awareness arrangements designed to better equip officers to deal with online child sexual abuse incidents.

142. Most divisions responsible for dealing with NOCAP packages relating to their area have appointed a Single Point of Contact, generally at Detective Inspector level. This facilitates a degree of governance and oversight in relation to the packages received and HMICS regards this as good practice.

143. The appointment of a Single Point of Contact Detective Inspector aligns well with the daily governance structures at divisions. There is a confidence that, as a requirement, all child concern issues are recorded appropriately on the Vulnerable Persons Database and are subsequently evaluated and triaged daily by the divisional Concern Hub. Daily management oversight arrangements vary across divisions, however general principles are consistent. Concern Hub staff ensure that the most significant issues are highlighted for further discussion as appropriate by senior management and/or business area managers.

Specialist Support

144. As mentioned previously in this report, divisions rarely utilise the SCD Multi Agency Tactical Tasking and Co-ordination group to secure specialist support, despite the fact that this is the appropriate forum in which to bid for SCD specialist functionality and resources. We have also highlighted earlier in this report the requirement for specialist resource provision to be more open and visible.

145. Requests for additional resources from NCAIU are infrequent, and primarily relate to online child sexual abuse that, following overt action, is assessed as being either protracted or far reaching in terms of additional suspects and/or victims.

146. During our review it was accepted by Police Scotland that the vast majority of NOCAP packages are treated as a stand-alone investigation. Routinely, no additional proactive work is undertaken in respect of the suspect, his/her associates and internet activity beyond that which is already documented in the intelligence package or that which is patently obvious during overt action.

147. Police Scotland’s Digital Forensic Examiners support divisional activity ‘on-site’ during the execution of NOCAP packages wherever possible. As discussed previously however, this support is frequently obtained as a result of direct contact with the one of the localised hubs located in Aberdeen, Edinburgh, Glasgow, Dundee and Inverness.

Is the digital forensic support function sufficient to meet demand?

Supporting Operational Activity

148. The department that provides specialist digital support to all cyber-related crime is Cybercrime Investigations and Digital Forensics which is located within SCD OCCTU. There are five digital forensic hubs located across Scotland in support of frontline operational activity.

149. Digital Forensic support is frequently sought in relation to NOCAP intelligence packages involving IIOC offending where preliminary on-site preview examination of devices can deliver a quick and effective assessment of the existence of IIOC.

150. In addition, all requirements from across Police Scotland for the forensic examination of digital devices and equipment, as an integral element of conventional investigatory and evidence gathering processes, are conducted by digital forensic examiners.

151. There are 70 digital forensic examiners across Police Scotland to support operational activity in the execution of NOCAP and other online abuse enquiries. Their role is to support the development of digital forensic strategies and prioritise the examination of digital devices. They aspire to attend all NOCAP warrant operations in support of local officers. Demand for this facility is such however that this cannot always be achieved. Decisions in respect of which operations they will attend are determined at the weekly NOCAP Strategy Group or following direct discussions with local divisional staff. Prioritisation is based on the risk to the safety of children as established through the accredited risk assessment process.

Child Abuse Image Database (CAID)

152. CAID is a database, developed by the Home Office and hosted by West Yorkshire Police, that holds images received from NCMEC in Canada and the US. It holds information on all IIOC encountered by police and NCA, in one place by use of their unique ‘hash’ identifier. CAID currently holds around 14 million images and some 250,000 videos.

153. This database assists police in negating the need for every IIOC to be viewed and verified by a member of staff, as well as assisting in victim identification. Police Scotland is both a user and contributor to CAID.

154. Currently the Crown Prosecution Service (CPS) in England and Wales, in an effort to address onerous quantities of IIOC having to be viewed, confirmed and verified, operates a reporting threshold system whereby, when the number of images recovered reaches a prescribed number, there is no requirement to confirm any further images. This is an operationally pragmatic model, given the increasing number of cases being reported.

155. There may however be a negative impact on the CAID database in that there may be additional images stored in the device of a suspect that has not yet featured on CAID. If that image(s) exists beyond the reporting threshold then it will not be uploaded as a new image. Further, and more critically, victim identification will be impeded.

156. Crown Office and Procurator Fiscals Service (COPFS) as the prosecutor in Scotland, does not operate a reporting threshold model for IIOC therefore all images require to be confirmed.

157. CAID’s technical capability is developing at pace and is able to match images and to trace devices used to make the image. HMICS found that the relationship between Police Scotland and the Home Office CAID team is strong and there are good lines of communication at an operational level.

158. The CAID Working Group is a sub-group of the Tackling Online Child Sexual Abuse (TOCSA) Group with a role to maintain and develop Police Scotland's use and contribution to the database. HMICS advises that Police Scotland should take account of its experience of the introduction of cyber kiosks, in particular concerns about consultation and ethics, when considering the benefits of enhanced technical capability.

Digital Forensic Examination Case Management

159. The preliminary examination of devices at the site of the enforcement activity eliminates the unnecessary seizure of devices and other digital equipment that would subsequently require a full forensic examination.

160. Cybercrime case management data for the three month period September, October and November 2019 confirms that 86% of devices submitted for digital examination were mobile phones. Sexual crime was the most prominent crime type and of that, rape was the most frequent crime, followed closely by IIOC.

161. The Digital Forensic Gateway is the receiving facility for all Examination Request Forms where triage and quality control functions are conducted. Gateway staff are co-located with the digital forensic teams to provide a robust and consistent process. We found that there remains a tendency for front line officers, due to a lack of experience or knowledge, to seize devices unnecessarily for subsequent examination. The deployment of digital forensic examiners to provide on-site advice and expertise reduces this demand.

162. Police Scotland operates with a significant backlog of devices awaiting forensic examination, however they have successfully reduced this from a typical number of around 1200 outstanding devices to 500 in December 2019. This is as a result of a review and revision of internal processes. HMICS acknowledges the considerable effort that has been made to reduce this backlog and would urge Police Scotland to ensure this is sustained.

163. Roll out of the Digital Device Triage System, commonly known as cyber kiosks, across the country is designed to enhance the cybercrime digital forensic capability of Police Scotland and assist in accelerating triage processes in relation to digital devices. The initial approach was not without controversy, and was subject to significant scrutiny.[32]

164. HMICS believes that the roll out of cyber kiosks will enhance Police Scotland's capability in digital forensic case management.

165. HMICS also acknowledge that the demand for digital forensics, and in particular the backlog, is influenced by COPFS who regularly make requests to conduct initial or supplementary forensic examinations. Advances in technology and the vast amount of data being held on devices are such that blanket requests to 'examine everything', made as a matter of routine, are increasingly unrealistic and have a substantial subsequent impact on Police Scotland's digital forensic capability. HMICS considers that a radical rethink regarding the practicalities of sustaining the current approach is required.

Recommendation 8

Police Scotland should work with the Crown Office and Procurator Fiscal Service to establish a pragmatic and realistic approach to digital forensic examination requests.

[32] SPA, Strategy, Policy & Performance Committee - Digital Triage Devices (Cyber Kiosks), 8 May 2019.

Technology/Skills Maintenance

166. Rapid developments in technology, the means to exploit technology for the purpose of committing crime, and the opportunity for anonymity that the internet provides, have dramatically altered the profile and nature of criminal offending. Consequently law enforcement must continually adapt to meet the pace of change.

167. Police Scotland recognises that historically there has been underinvestment in technical surveillance and cyber capability. This was recognised in an independent audit conducted in 2018 by an industry consultant[33] Clearly, all areas of policing that have a cyber element, including online child sexual abuse, will be impacted by this lack of investment.

168. The Strategic Assessment 2020-23 and '2026 - Serving a Changing Scotland' documents reflect the urgent requirement for Police Scotland to catch up. Further, the SCD Risk Register lists 'Forcewide Digital Skills and Knowledge' and 'Ensuring Cybercrime Investigation and Digital Forensic Skills Keep up with Technology' as Very High level risks. HMICS is aware that Police Scotland aspires to recruit a significant number of specialist support staff to assist in this area, however there has only been modest steps towards this since 2017.

169. In response to the recognised gap, two key transformational programmes of work were initiated in 2017-18: Cybercrime Capabilities Programme (CCP) and Technical Surveillance 21st Century (TS21C). These two programmes were consolidated in May 2019 to create the Cybercrime, Technical Surveillance Programme (CTSP).

170. A CTSP overview note dated 20 September 2019 highlighted 15 key operational issues including an inability to prioritise resources against demand, variable service levels across the country, a requirement to find alternative operational models to reduce digital forensic backlog and an acceptance that the force is reactive rather than proactive.[34]

171. The CTSP is designed to provide the force with a strategic understanding of the threat of cybercrime and technical surveillance and the necessary information to ensure they are sufficiently capable of exploiting investigative and preventative opportunities across the cyber-related business area.

172. This is a significant transformational change programme with governance structures provided by the CTSP Programme Board, CTSP Steering Group and the Scottish Sensitive Equities Board.

173. All the key risks that the programme seeks to address in the year 2020-21 could be said to be relevant to online child sexual abuse, however those with particular relevance include: an expansion of digital investigative capability; the establishment of 'dark net' investigative capability, and a structural review to identify an optimised model for cybercrime and technical surveillance.

174. HMICS found that Police Scotland has a clear understanding of the shortfall in respect of tackling cybercrime and has responded with a transformational programme that is both ambitious and necessary. To achieve improvements in this critical area of policing will require significant funding.

[33] Police Scotland, Cyber and Technical Surveillance Programme (CTSP) Overview, September 2019.
[34] Police Scotland, Cyber and Technical Surveillance Programme (CTSP) Overview, September 2019.

Structure of Digital Forensics

175. In 2016 we issued a professional advice note to Police Scotland, Options for the Governance of Forensic Services in Scotland[35] in which we highlighted that *"the Forensic Service does not currently provide forensic support for ICT/Cyber/e-crime as this function remains within Police Scotland"*. HMICS did not infer that the quality of digital forensic examinations was affected as a result of this arrangement, but pointed out the anomaly with other forms of forensic examination.

176. Our 2017 Thematic Inspection of the SPA Forensic Services[36] further highlighted this issue, with a recommendation that:

"Police Scotland should consider quality accreditation for digital forensics in line with the FSR recommendations, UK Forensic Strategy and wider good practice."

HMICS is aware that an internal paper was produced by the Cybercrime Unit in October 2017, which showed that Police Scotland had considered accreditation and on that basis, the recommendation above was closed. That said, the internal paper recommended that Police Scotland invest in a Quality Management system and create a cybercrime quality manager post in order to begin an incremental journey towards accreditation. This has not been progressed.

177. The SPA Digital Forensics Working Group was established in June 2019[37] to consider the HMICS 2017 recommendation and indeed whether it is appropriate for digital forensics to continue to be located within Police Scotland. HMICS notes that in the interim there has been no change to either the governance of Digital Forensics or the accreditation of those responsible for the examinations. We regard this as being a risk and open to further challenge.

[35] HMICS, Guidance Note to Police Scotland – Options for the governance of forensic services in Scotland, October 2018.
[36] HMICS, Thematic Inspection of the Scottish Police Authority Forensic Services, 27 June 2017.
[37] SPA, Board Meeting - Digital Forensics Working Group, 26 June 2019.

How effective is Police Scotland's covert capability to detect and disrupt offending and to keep children safe online?

178. The veiled nature of the online world clearly presents opportunities for those who would seek to target and exploit children. The same environment also provides opportunities for law enforcement to operate covertly to identify, intercept and disrupt those who present a risk to children online.

Structure

179. Police Scotland's Special Operations Unit (SOU) is responsible for the delivery of undercover online (UCOL) operations in respect of cyber enabled criminality and sits within the Organised Crime Counter Terrorism Unit of Specialist Crime Division.

180. Police Scotland's entire capability in terms of undercover (UC) operations rests with SOU, including that which relates to online activity. While UCOL deployment is suitable for a range of crime types, it is particularly suitable from a child protection perspective in pursuing those who exploit the anonymity of the internet to target children and induce them to engage in unlawful sexual activity.

181. In February 2018, HMICS published our Strategic Review of Undercover Policing in Scotland,[38] which described the strict legislative framework, supplemented by regulatory requirements and associated codes of practice that govern this area of policing.

Profile of UCOL Officers

182. An undercover officer is defined under Section 7 (1) of Regulation of Investigatory Powers (Scotland) Act 2000 and the Regulation of Investigatory Powers (Authorisation of Covert Human Intelligence Sources) (Scotland) Order 2014.[39]

183. Specifically, a UCOL officer is a nationally accredited officer who is deployed to establish and maintain relationships with an individual, network or organisation through the use of the internet with the covert purpose of obtaining information and evidence as part of an authorised operation such as online child sexual abuse and exploitation. An undercover online officer must attend and pass the nationally accredited College of Policing undercover online officer course or to have previously passed courses in place prior to the College of Policing course.

184. The officers that are deployed in UC and UCOL work do so as a result of having volunteered to undertake this role. The specialist training and accreditation that is mandatory does not include child protection training and, while it is preferable, there is no requirement for UCOL officers to have prior training or experience in child protection.

[38] HMICS, Strategic Review of Undercover Policing in Scotland, 7 February 2018.
[39] As above.

UCOL Activity

185. Our 2018 report confirmed that the main focus of undercover activity in the three years immediately following the inception of Police Scotland was drug related offences. Child sexual abuse and exploitation accounted for the second most targeted crime type however, clearly the margin between the two in terms of numbers of operations was considerable. By 2016 undercover activity overall had reduced.[40]

Table 3:

2013	15 operations	11 Drugs, 2 OSCA
2014	14 operations	11 Drugs, 0 OSCA
2015	13 operations	6 Drugs, 1 OSCA
2016	8 operations	2 Drugs, 2 OSCA

186. Less than 16% of the SOU undercover cadre are trained in UCOL. The team's capability is exclusively undercover deployment and they are required to rely on assistance for case development and intelligence support from other departments. Notwithstanding the increase in UCOL operations, our 2018 report noted that, *"we believe that undercover advanced officers and undercover online officers has been underutilised. This is a position that has been accepted by Police Scotland."*[41]

187. As part of the regular inspection of Police Scotland's use of statutory investigatory powers, the Investigatory Powers Commissioner's Office (IPCO) report of 2018 highlighted surprise at a lack of intelligence, analytical and investigatory support for UCO.[42] In particular the IPCO noted that;

"once an opportunity is identified by the undercover operatives, a request for overt resources has to be made to senior officers within the relevant division. In a number of cases evidenced during the inspection, there has been a delay in attracting the appropriate resources and therefore evidential opportunities have been missed."

188. While IPCO has highlighted the impact on evidential opportunities, of greater significance in the context of online child sexual abuse is the continued harm being caused to children.

189. HMICS is aware of evidence of a previous long-running UCOL operation in relation to online child sexual abuse that was successful, detecting 26 online offenders. However, the case did feature a lack of appropriate intelligence support (the issue highlighted by IPCO) that impacted on the ability to adequately manage risk and develop investigations.

190. The success of the operation shows the potential value of undercover deployment in terms of enforcement and intervention to reduce the risk to children. At the time of our review however an internal review of UC work resulted in the suspension of all operations including those that related to UCOL. While the instruction for a universal cessation has since been rescinded, there has been very limited UCOL activity since and this is clearly a missed opportunity.

191. A key finding in our 2018 report was:

Two of the key elements within the Policing 2026 strategy relate to online safety and the response to serious organised crime. The capacity and capability within Police Scotland to conduct undercover policing in support of these is currently limited and needs to be further developed.

[40] HMICS, Strategic Review of Undercover Policing in Scotland, 7 February 2018.
[41] As above.
[42] IPCO report 2018, held by Police Scotland.

192. Despite being advised in 2018 that the deployment of UCOL operatives was an underused tactic, Police Scotland has made little progress, and indeed there has been a regression in this area of business against a backdrop of increased demand.

Recommendation 9

Police Scotland should review its capacity and capability to conduct undercover online covert operations in support of its policing priorities and ensure that undercover online operatives are sufficiently equipped and supported to identify and adequately assess the risk to children as a result of online offending.

Tasking and Co-ordinating and Prioritisation

193. HMICS found evidence of the SOU self-generating UCOL operations, which were then approved at Detective Chief Superintendent level without going through the formal tasking and co-ordinating process. This approach to the allocation of scarce specialist covert assets is inappropriate. It does not take account of the demand for covert support from across the organisation, nor of the prioritisation arrangements aligned to prescribed risk assessment processes. Given the commitment to its own, self-selected operations, the SOU was unable to meet requests for undercover support for any other work.

194. To ensure that the operational activity of the SOU, in common with all other aspects of Police Scotland, is informed by risk, priority and demand, it should be directed by robust and effective tasking and co-ordination processes. Although the sensitivity of covert options and assets require protection, HMICS considers the SOU to be part of the wider police response and should not be permitted to operate in isolation.

Recommendation 10

Police Scotland should ensure that arrangements for deploying undercover online specialist resources are directed by formal tasking arrangements aligned to risk, priority and demand.

195. Since the inception of Police Scotland, SOU has formed part of the OCCTU business area and not the Intelligence function.

196. There is a valid debate in respect of whether undercover deployment is considered to be intelligence or evidence gathering activity, or if both are applicable. HMICS encourages Police Scotland to reconsider the current governance structure of SOU to establish where it is best located.

Future Proposals

197. In 2016 the Home Office launched the Police Transformation Fund (PTF) and announced the availability of an additional £100m of funds to support police forces in England and Wales to adapt to the challenges of the future.[43] The PTF is designed to assist in transforming how police use technology and to better equip them to deal with new types of crime.

198. All Regional Organised Crime Units (ROCU) and pan-London forces have successfully benefited from investment from the PTF (a total of £15.5m in years 2017-18 and 2018-19) specifically for the establishment of dedicated units to combat the threat of online criminality.

[43] Home Office, Police Transformation Fund announced in 2016.

199. Of particular note is the objective to provide an uplift of undercover resources to tackle online vulnerability, the project being scheduled to run between 1 April 2017 and 31 March 2020. The project is the subject of independent evaluation and an interim report, ‘Evaluation of the Police Transformation Fund Uplift in dedicated Undercover Online Resources to tackle vulnerability’, which was published in respect of the first six months of the operation. This produced positive comment in critical areas including:

“The suspect can be intercepted before crimes are committed and/or…crimes against children which would otherwise go undetected can be identified and interrupted.”

200. This investment in resource and capability elsewhere in the UK however does not extend to Scotland.

201. In October 2019, Police Scotland produced a proposal for internal consideration, suggesting that a dedicated online child sexual abuse team should be introduced to replicate the UCOL and Case Development structure that has been established in the ROCUs. This proposal, if approved, would include an uplift of 12 staff within SOU (two Detective Inspectors, one Detective Sergeant, two UCOL and seven Detective Constables) to enhance UCOL capacity and to create an intelligence support function.

202. Whilst it is outwith the remit of this review to evaluate any internal proposals tabled within Police Scotland, the features of this particular proposal would in part address some of the issues that have already been highlighted in previous scrutiny processes by various inspection bodies.

203. Irrespective of the future structure of covert UCOL deployment, it is essential that there is a seamless interface that facilitates the initiation of a timely overt response. The efficiency of this interface has not been tested in recent times given the hiatus in covert deployment however a more robust arrangement than that which previously existed is required.

Are Police Scotland's prevention strategies and activities effective in reducing the risk to children from online child sexual abuse?

204. Police Scotland Safer Communities is primarily responsible for the co-ordination and delivery of prevention activity. The Cyber Prevention Unit deliver key messages across Scotland regarding all cyber-related crime, including online child sexual abuse. It is not a mandatory requirement for staff to have previous experience in child protection, although some do. HMICS considers it important that online child sexual abuse prevention activity is informed by those working within the child protection arena. To this end, it is encouraging that national Safer Communities staff are members of the TOCSA Tactical group.

205. National Safer Communities, Cyber Prevention Unit, provides support by sharing guidance and processes with local policing divisions and national units to inform them and assist them in reducing the risks prevalent in cybercrime. These relate to cyber harm in general and include guidance on cyber bullying, hate crime, financial harm, as well as online child sexual abuse. They also utilise divisional Web Constables and Cyber Crime Prevention Officers to promote these operationally across Police Scotland and partners.

206. The Police Scotland website has been updated, adding information from partner agencies under the 'Keeping Safe' page. The site contains useful information for parents and carers and for children and young people and has links to sites such as ThinkUKnow, which contains useful information in relation to online safety and CSE.

207. 120 Officers have been trained in the CEOP Ambassador Course and can access CEOP and ThinkUKnow training materials. This included officers from Safer Communities, Public Protection Units, School Liaison Officers, Campus Constables and Control Room staff. These are tested and evaluated materials and provide a consistent delivery of information, and have been used in turn to train additional officers across Scotland.

208. HMICS observed good examples of local, joint preventative work with partners in the divisions that we visited and are aware of similar practice in other divisions.

209. Safer Communities run annual CPD Conferences relating to internet safety, and co-ordinate an annual 'Safer Internet Day' in conjunction with UKSaferInternet in which cyber prevention officers, Web Constables and partners are engaged to maximise awareness around social media activities. The department has developed audio/visual safety materials that can be accessed directly via schools databases.

210. A full review of national Safer Communities is currently underway and includes consideration of the implementation of a Preventions Task Force to look at a number of strands of prevention, including online child sexual abuse.

211. Child at Risk intelligence packages are created in relation to those children who have posted sexually explicit images of themselves on social media. Prescribed child protection protocols are implemented, with the focus of subsequent intervention being safety, wellbeing and prevention of abuse.

212. However, HMICS found that the use of Child at Risk packages and associated intervention activity were dealt with in isolation and not merged with prevention strategies. The application of Child at Risk packages should be considered as an integral element of wider prevention and intervention strategies.

213. While prevention activity is wide reaching and well developed in respect of children who may be at risk of sexual abuse, HMICS found that the picture in relation to offenders was not as mature.

214. In recognition of the threat and risk of online sexual abuse to children and young people, Police Scotland, in conjunction with the national child protection charity, Stop It Now, launched campaigns in 2018 and 2019 aimed at those engaged in online grooming of children for sexual purposes, online or webcam sexual extortion including live streaming of abuse and viewing and sharing indecent images of children online.

215. The campaigns were promoted heavily at local and national levels and involved various partners (Stop It Now, CEOP, COPFS, Barnardo's, NSPCC, Rape Crisis Scotland) and Local Authority Child Protection Committees. These campaigns led to notable increases in people accessing the Stop It Now UK and Scotland websites. The awareness of the campaign was supported by various media strategies and involved poster distribution, radio and social media, local and national press. The use of Facebook for example reached over 439,000 people and Twitter over 500,000 impressions.

216. In terms of awareness raising, the campaign was successful with over 26,000 occasions when the Stop It Now Scotland website was accessed. 3841 people in Scotland used 'Get Help', the Stop It Now online resource, and 543 people in Scotland used 'Get Support', a resource for adults worried about their sexual thoughts and feelings towards children.

217. However, there has been no evaluation in terms of how effective the campaign was in reducing offending or capturing intelligence around offenders. HMICS considers that it would be worthwhile to run similar campaigns in the future, however these would be enhanced by more meaningful evaluation criteria from the outset.

218. Police Scotland, with partners, has a statutory duty to manage sexual offenders in the community under the MAPPA arrangements. Some of those offenders are responsible for child abuse offences including those that relate to cyber-enabled offences such as IIOC and grooming.

219. A March 2019 report by Police Scotland NOMU stated that 21.1% (1180) of RSOs had IIOC as their index offence (main offence for which they are registered as sex offenders), while a further 21.5% (1204) had 'sexual activity with a child' as their index offence. Recording conventions are such that these are likely to be conservative numbers, with the true number expected to be higher.

220. Beyond the formal MAPPA arrangements that are in place throughout Scotland, in respect of engagement with offenders or potential offenders, SACRO (Safeguarding Communities Reducing Offending) and Stop It Now! are the main service providers in Scotland and Police Scotland has well established professional relationships with both organisations.

221. In terms of reducing the risk to children of reoffending and 'managing' individuals within communities, there is a recognised gap between the point of overt operational activity and (where relevant) a subsequent conviction that triggers an associated RSO status and requirement to submit to the formal MAPPA arrangements.

222. Police Scotland can manage individuals within the community who are assessed as being potentially dangerous persons (PDP). This includes individuals charged but not yet convicted of a sexual offence. The management arrangements in respect of PDP are similar in commitment to those who are subject to formal MAPPA, therefore the qualifying threshold is commensurately high. The number of PDPs varies, but as of December 2019, there were 49 listed across Police Scotland.

223. A Risk of Sexual Harm Order (RoSHO) is a preventative civil order created under the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005, designed to protect a child or children under 16 from those who present a risk of sexual harm. It is not a requirement for the individual to have been convicted, however they must have engaged in sexualised contact or communication with a child on at least two occasions. Of the 49 individuals assessed as potentially dangerous persons (PDP), 25 have Risk of Sexual Harm Orders in place, which indicates some form of sexualised behaviour towards children. Of the 25 RoSHOs, 16 include conditions to monitor internet use, which is indicative of risk in the online space.

224. HMICS considers the numbers of PDP and RoSHO to be low given the extent of known suspects/offenders. Neither PDP or RoSHO therefore are making a significant difference in terms of managing the volume of pre-conviction online child sexual abuse offenders that exist annually.

225. Police Scotland recognises the risks associated with the period between overt police action and potential court proceedings, when potential offenders can self-harm or complete suicide. As such, Police Scotland instigated work with SACRO to develop an intervention that could address the harmful behaviours immediately, without waiting for a conviction. SACRO developed a programme based on cognitive behaviour therapy to help individuals to change their attitudes and behaviour. The ‘CHOICE’ programme (Challenging Harmful Online Images and Child Exploitation) could be used by individuals on a voluntary basis pre-conviction, or could form part of a structured deferred sentence or other disposal following conviction.

226. The ‘CHOICE’ programme has support from Police Scotland and Scottish Government, and positive discussions have taken place with COPFS, however efforts that have been underway since 2017 to introduce the programme as a pilot, have so far been unsuccessful. This is despite it being free to access and accepted as fit for purpose by the Risk Management Authority.

227. Clearly Criminal Justice Social Workers based in Local Authorities have a remit for interventions with violent and sexual offenders using the ‘Moving Forward, Making Changes’ programme, however exploring the use of a shorter, less intensive programme, such as ‘CHOICE’, seems a sensible and proportionate response to individuals who present a lower risk of harm.

228. There is a clear gap in the prevention agenda within this pre-conviction period that cannot be addressed by statutory bodies alone. Charities such as Stop it Now and SACRO offer alternative services. There is a need to overcome professional barriers and protectionism, which is compounded by funding arrangements when services are competing for funding from Scottish Government. A report by Justice in 2019[44] highlights similar findings in relation to lack of co-ordination and support. Our assessment is that there are positive examples of prevention and effective intervention work, however there is no overarching plan. These efforts should be pulled together as part of a national strategy to deal with the reality of high and growing numbers of individuals involved in online child sexual abuse, to prevent and divert offenders, rather than relying solely on law enforcement.

[44] Justice, Prosecuting Sexual Offences, 2019. Section 6.87-6.99.

Prevention Analysis

229. Some work has been undertaken to get a better understanding of the profile of those who commit online child sexual abuse offences, such as the Analysis of Occupations of RSO with an Index Offence for Indecent Images of Children that was produced in March 2018 from the Visor (Violent and Sex Offender Register) database. There is still however a lack of knowledge in relation to issues including pathways to offending, and the identities of the organised crime groups that are involved in online child abuse.

230. Improved intelligence capture, data recording and analysis would not only enhance the picture in terms of the scope and nature of online child sexual abuse, but it would also better inform prevention and intervention opportunities.

Other Issues

Staff Training and Welfare

231. Staff have been supported in their respective roles by the publication of training and guidance documents including:

- Indecent Images of Children on Digital Media SOP
- National Online Child Abuse Prevention (NOCAP) Investigation Toolkit
- Child Protection SOP
- Child Sexual Exploitation Toolkit
- Child Sexual Exploitation Intelligence Toolkit
- National Guidance for Child Protection in Scotland
- Responding to and Investigating Reports from Online Child Sexual Abuse Activists Groups Guidance.

232. HMICS found that online child sexual abuse training is incorporated in the various child protection training and guidance materials, much of which is delivered via the Moodle online training platform.

233. Detective officers at SCD and Local Policing, directly engaged in child protection investigations, undertake specialist training including the National Child Protection Programme. All levels of the Investigators Development Programme contains child protection modules that incorporate online child sexual abuse.

234. Formal training and guidance has been supplemented by continuous professional development days for the benefit of staff, the most recent being a National Online Child Abuse Prevention Conference held on 13 August 2019.

235. HMICS found staff to be generally competent and confident in dealing with online child sexual abuse.

236. Officers and staff in specific specialist functions have access to annual online wellbeing assessments. This is however a voluntary arrangement and, while we saw evidence of some departments being particularly proactive in encouraging staff to utilise this service, there is no obligation to attend. The confidential nature of the service is such that managers are unaware which staff members have taken advantage of the facility.

237. The volume and nature of online child sexual abuse currently being undertaken by officers has the potential to have a significant impact on their wellbeing. This is especially the case for those members of staff who are directly exposed to IIOC, child sexual abuse or other graphic material relating to children. Wellbeing support is in place for the NCAIU, IIU and digital forensics staff.

238. The NCAIU have recently proposed a wellbeing support structure for staff that includes:

- Annual face to face assessment for all NCAIU staff
- Annual voluntary online assessment
- These would be staggered by 6 months, thereby ensuring staff have an assessment every 6 months.

239. In addition, NCAIU have provided National Mental Health First Aid training to supervisors in each of their regional hubs and an awareness input from the force Wellbeing Team for all Detective Inspectors and Sergeants.

240. HMICS regards this as best practice for consideration in other areas of business where staff are exposed to graphic material relating to online child sexual abuse, IIOC and child sexual abuse.

Online Child Abuse Activist Groups

241. An emerging issue in recent years has been the increasing activities of online child sexual abuse activist groups (OCAGs), frequently referred to as 'vigilante' groups. These are organised groups comprising of members of the public who purport to be children online for the purposes of identifying those that seek to groom and exploit children for sexual purposes. The OCAG members typically target suspected child abusers by engaging online via social media platforms, agreeing a rendezvous between the target and their online pseudonym in a public place, with the ultimate aim of maximum public exposure.

242. There are a number of known groups that operate in Scotland and who have strong links to similar networks across the UK, the most prominent and active operating in Scotland being Wolf Pack Hunters UK.

243. According to data from Wolf Pack Hunters, it has conducted more than 80 'sting' operations in Scotland from mid-October 2017 to the end of March 2019.[45]

244. Typically it is front-line officers who engage with OCAGs in response to a report that a suspect has been 'detained'. This is often a confrontational situation with activists recording the event on mobile devices. Frequently, live confrontations attract a public audience and have a significant community impact.

245. Police Scotland has developed a guidance document 'Responding to and Investigating Reports from Online Child Sexual Abuse Activists Groups' to assist front line officers responding to a call involving OCAGs.

246. OCAGs operate outside the legislative framework, which involves a strict authorisation regime for covert activity.The legitimacy of their digital evidence is contested and their actions present a risk to themselves, those they target, and other members of the public. Further, there are no safeguards in terms of validation of the 'intelligence case', nor the identity of the suspect. Their activity is therefore not legitimate or appropriate, and is conducted by individuals who have not been subject to the necessary vetting processes.

247. Notwithstanding the above, OCAGs regard themselves as well intended and performing a role in which the police are failing. There is no indication that their activities are likely to cease.

248. In response Police Scotland produced an OCAG Problem Profile in the first quarter of 2019. The Online Grooming of Children in Scotland Strategic Threat Assessment 2018-19 was produced in April 2019 and confirms that OCAG related activity accounted for 55% of all recorded online grooming crime reports in the fiscal year 2018-19.[46]

249. This figure makes it difficult to argue against the contribution made by OCAGs, particularly against a backdrop of limited covert activity by Police Scotland in the recent past.

[45] The Guardian, Scotland's child abuse activists: 'We embrace the vigilante label', 6 August 2019.
[46] Police Scotland, Online Grooming of Children in Scotland Strategic Threat Assessment 2018-19.

250. HMICS found there was a good level of awareness of the Police Scotland Standard Operating Procedures for responding to OCAG related incidents. The officers we spoke to during this review stated they now felt more confident and comfortable in dealing with OCAG related calls.

251. The National Police Chiefs' Council has recognised OCAG activity as a UK-wide threat, and Police Scotland has been involved at a senior level in the development of an overarching strategy. Police Scotland aligns itself to the UK strategy and has amended the NPCC documentation for a Scottish context. HMICS found officers at local divisions were familiar with the Police Scotland Standard Operating Procedures for reacting to OCAG related activity, however we found no evidence of awareness of the overarching UK-wide strategy.

Stakeholders' Views

252. As part of our review we sought the views of a range of agencies engaged in services to support children and young people. We received responses from the NSPCC, Aberlour, Children 1st and Chief Social Workers. We asked questions about the police response, any specific challenges encountered, examples of good practice, the perspective of children and carers, and the availability of support services.

253. There was a recognition of the complexities and challenges faced by law enforcement in tackling online child sexual abuse. Police Scotland's commitment to making it a priority in the Annual Police Plan 2019-20 was welcomed. There was a strong view that real progress could only be made through a co-ordinated strategic and operational response involving key partners: health; social work; education; housing, and the third sector.

254. The existence of international research into the impact on the victim of sharing child sexual imagery online was highlighted. This Canadian research contains valuable insights, which could inform changes to policy and services to meet the needs of survivors and their families.[47]

255. NSPCC research in 2017 on the impact of online child sexual abuse contained evidence of a wide variety of police response, both positive and negative. The length of time it can take to investigate a case can be traumatic and the assumptions that online abuse is less harmful than contact abuse, can also be damaging. Online and offline abuse are increasingly intertwined, and those children at most risk off-line will experience heightened vulnerability online. Lack of care and supervision from a responsible adult leave children increasingly exposed to the dangers online.[48]

256. HMICS was told that the lengthy nature of investigations and the time taken for cases to come to court were compounded by lack of information from the police about progress. Children and young people who gave their mobile devices to police for examination were left without their devices for considerable periods of time and often were not in a position to buy a replacement.

257. A key point made by respondents was that prevention activities should not be confined to schools, given that some of the most vulnerable young people are not regular attenders. Local police liaison officers for residential units were felt to be helpful in this respect.

258. The availability of support services for children, young people and carers was described as *"patchy, inconsistent, and at times non-existent."*

[47] Canadian Centre for Child Protection, Survivors' Survey - Executive Summary 2017.
[48] NSPCC, Impact of online and offline child sexual abuse: "Everyone deserves to be happy and safe", November 2017.

Appendix A - Main Legislation

Section 52 Civic Government (Scotland) Act 1982	Making, possessing or distributing indecent images of children
Section 52A Civic Government (Scotland) Act 1982	Possession of indecent images of children
Section 127 Communications Act 2003	Send or cause to be sent, by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character
Section 1 Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005	Grooming a child
Sexual Offences (Scotland) Act 2009. Sections 6, 23, 24, 33, 34	Various offences including causing a child to participate in sexual activity, causing a child to look at sexual images, hear or see indecent communications, sexual exposure, voyeurism, much of which can occur online as well as within the real world or by traditional communications methods
Sections 2-8 Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005	Makes provisions for Risk of Sexual Harm Orders (RoSHOs). Places Conditions on those who pose a risk of sexual harm to a child or children.

Appendix B - Glossary

APU	Analysis and Performance Unit
CAID	Child Abuse Image Database that is managed and administered in the UK by the Home Office
CEOP	Child Exploitation and Online Protection (Command Unit of NCA)
CIU	Communications Investigation Unit
CoP	College of Policing
COPFS	Crown Office and Procurator Fiscals Service
CPC	Child Protection Committee
CPD	Continuous Professional Development
CSA	Child sexual abuse
CSE	Child Sexual Exploitation is a form of child sexual abuse in which a person (s) takes advantage of a power imbalance to force or entice a child into engaging in sexual activity in return for something received by the child and/or those perpetrating or facilitating the abuse
CTSP	Cybercrime, Technical Surveillance Programme
Dark Net	A term used to describe concealed aspects of the internet that are only accessible by using specialist search engines and that provide an enhanced degree of encryption
ERF	Examination Request Form
GIRFEC	Getting It Right For Every Child
HMIC	Her Majesty's Inspectorate of Constabulary
IIOC	Indecent Images of Children
IIU	SCD Internet Investigations Unit
IPCO	Investigatory Powers Commissioner's Office
KIRAT2	Kent Internet Risk Assessment Tool - an accredited risk assessment tool
MAPPA	Multi Agency Public Protection Arrangements
NCA	National Crime Agency
NCAIU	National Child Abuse Investigation Unit
NCMEC	(US) National Centre for Missing and Exploited Children
NOCAP	National Online Child Abuse Prevention
NOMOU	National Offender Management Unit
NPCC	National Police Chiefs' Council
NSPCC	National Society for the Prevention of Cruelty to Children
OCAG	Online Child Abuse Activist Groups
OCCTU	Organised Crime and Counter Terrorism Unit, Police Scotland
PDP	Potentially Dangerous Persons
PSoS	Police Service of Scotland (commonly referred to as Police Scotland)
PTF	UK Government Police Transformation Fund
ROCU	Regional Organised Crime Units. Cross-boundary regional law enforcement resources in England and Wales tasked with tackling serious and organised crime
RoSHO	Risk of Sexual Harm Order
RSO	Registered Sex Offenders
SACRO	Safeguarding Communities Reducing Offending
SCD	Specialist Crime Division
SID	Scottish Intelligence Database
SOU	Special Operations Unit, Police Scotland
SPA	Scottish Police Authority
STORM	System for Tasking and Operational Resource Management
TOCSA	Tackling Online Child Sexual Abuse (Tactical and Strategic groups)
UC	Undercover
UCOL	Undercover Online
VPD	Vulnerable Persons Database – records incidents relating to vulnerability including mandatory categories of child or adult concerns, domestic abuse and hate crime

HMICS HM INSPECTORATE OF
CONSTABULARY IN SCOTLAND

HM Inspectorate of Constabulary in Scotland
1st Floor, St Andrew's House
Regent Road
Edinburgh EH1 3DG

Tel: 0131 244 5614

Email: hmic@gov.scot

Web: www.hmics.scot

About Her Majesty's Inspectorate of Constabulary in Scotland

HMICS operates independently of Police Scotland, the Scottish Police Authority and the Scottish Government. Under the Police and Fire Reform (Scotland) Act 2012, our role is to review the state, effectiveness and efficiency of Police Scotland and the Scottish Police Authority. We support improvement in policing by carrying out inspections, making recommendations and highlighting effective practice.

ISBN: 978-1-910165-56-0