ipcc
independent
police complaints
commission

NYP-CEOP

Investigation into the handling of intelligence by North Yorkshire Police in relation to Operation Spade

Independent Investigation
Redacted Report

IPCC Reference: 2014/035826

Contents

Redaction codes applied in this report

Code	Meaning
A	Information is personal or sensitive personal data.
B	Disclosure of information may prejudice law enforcement by revealing law enforcement techniques.
C	Non-disclosure is for the purposes of the prevention or detection of crime, or the apprehension or prosecution of offenders.
D	Information subject to legal professional privilege.
E	Information is relevant to, or may be used in, any actual or prospective criminal proceedings.
F	Non-disclosure is required on proportionality grounds.
G	Non disclosure is otherwise necessary in the public interest.

All redactions are made under redaction code A with the exception of [1-5] made under Redaction Code B

Introduction

1. Operation Spade was an investigation nationally coordinated by the Child Exploitation and Online Protection Centre (CEOP) into the acquisition by members of the public within the UK of indecent images from a video production company in Canada. This operation began in July 2012 following information being received from Interpol. At this time CEOP was a stand-alone organisation which was later absorbed into the National Crime Agency (NCA) in October 2013.

2. On 26 November 2013, intelligence was received by North Yorkshire Police (NYP) from CEOP relating to Operation Spade. A total of 25 suspects (believed to be resident in the North Yorkshire area at the time of the alleged offences) were named in Operation Spade related material.

3. There was no organisational progression of work in respect of the suspects featured in the Operation Spade related intelligence until the week commencing 29 September 2014.

4. CEOP sent NYP a letter requesting an Operation Spade update in September 2014. This prompted an internal review by NYP and subsequent referral to the IPCC on 7 October 2014.

5. On 10 November 2014, an independent investigation into the handling of intelligence by NYP in relation to Operation Spade commenced.

Terms of reference

6. The terms of reference for the investigation were:

   To investigate the handling of intelligence relating to Operation Spade by NYP following its receipt from the NCA on 26 November 2013. In particular:

   a) Whether NYP processed the intelligence appropriately in accordance with national and force policies.

b) The extent and nature of any access difficulties and what action was taken to ensure the intelligence could be processed once any access difficulties were identified.

c) Whether NYP's Intelligence Bureau was sufficiently equipped, in terms of expertise and resources, to deal with such intelligence.

d) Whether NYP responded appropriately to update requests from the NCA, including 10 December 2013 and 20 March 2014.

e) Whether NYP took any action in respect of the intelligence passed to it by the NCA between 26 November 2013 and 29 September 2014.

7. To identify whether any subject of the investigation may have committed a criminal offence and, if appropriate, make early contact with the Director of Public Prosecutions (DPP). On receipt of the final report, the Commissioner shall determine whether the report should be sent to the DPP.

8. To identify whether any subject of the investigation, in the investigator's opinion, has a case to answer for misconduct or gross misconduct, or no case to answer.

9. To consider and report on whether there is organisational learning, including:

- Whether any change in policy or practice would help to prevent a recurrence of the event, incident or conduct investigated;
- Whether the incident highlights any good practice that should be disseminated.

10. This investigation would not investigate any potential offences committed by any of the individuals identified in the CEOP/NCA intelligence forwarded to NYP relating to Operation Spade.

Subjects to the investigation

11. After consideration of the available evidence, it was determined that [redacted] may have behaved in a manner which may justify the bringing of disciplinary proceedings in that they may have failed to adequately progress and develop the intelligence relating to the initial dissemination of Operation Spade intelligence on behalf of NYP between 26 November 2013 and 29 September 2014.

12. On 28 January 2015, [redacted] was served with a Notice of Investigation and was later interviewed under the misconduct caution on 13 February 2015.

Background information

NYP Force Intelligence Bureau (FIB) function and roles

13. The main function of the FIB is to handle and process intelligence. This function was managed by Detective Inspector (DI) [redacted] with additional supervision provided by Detective Sergeant (DS) [redacted].

14. Both DI [redacted] and DS [redacted] had supervisory oversight over a number of different roles within the FIB which included three Intelligence, Research and Briefing Officers (IRBOs) named [redacted], [redacted] and [redacted].

15. An IRBO acts as an intelligence specialist, handling and processing intelligence. They also maintain the role of Single Point of Contact (SPOC) for various external agencies.

16. Generally, intelligence is submitted by email to the NYP FIBHQ mailbox, a generic mailbox which the majority of FIB staff have access to. IRBOs are responsible for monitoring and managing emails received into this mailbox as part of their roles.

Designation of CEOP and NYP CEOP SPOC role designation

17. CEOP holds their own list of designated CEOP SPOCs for police forces that should be included on the distribution of any intelligence packages/referrals.

18. DS [redacted] provided a statement to the IPCC in which he outlined that in 2013 and 2014 both himself, [redacted], DI [redacted] and the FIBHQ mailbox were named as SPOCs for CEOP intelligence. This practice was in place to ensure that they were all made personally aware of any referrals from CEOP which were sent to NYP.

19. There is also a separate role of NYP CEOP SPOC within the FIB that is allocated to an IRBO to act as the main facilitator for dealing with intelligence referrals from CEOP.

20. DI [redacted] confirmed in a statement that was provided to the IPCC that following consultation with DS [redacted], the role of NYP CEOP SPOC was re-allocated from [redacted] to [redacted] and she took over this role in October 2013. Their intention was to rotate the various SPOC roles in order to 'up-skill' the whole team and provide additional resilience and flexibility.

Handling of CEOP intelligence referrals

21. NYP had a documented process and procedure for handling intelligence referrals from CEOP.

22. DS [redacted] and DI [redacted] documented in their statements that they believed these documents were created by their predecessors and that neither had completed a formal review of this documentation during their time in the FIB.

23. The NYP CEOP process and procedure documentation states that following intelligence being sent by email from CEOP to all the designated CEOP SPOCs in NYP, an initial risk assessment is conducted

by the FIB DS or DI. This initial risk assessment would take into account the activity alleged and the full intelligence picture.

24. DI [redacted] has stated that this was an undocumented risk assessment and that if a package was deemed low risk, it was usually dealt with solely by the IRBO. If an initial risk assessment indicates a medium or high risk then further action would be taken by DI [redacted] and/or DS [redacted] as the intelligence may need to be dealt with immediately. It would be the responsibility of the IRBO to inform their supervision to highlight any issues of concern or potential change in risk assessment whilst they develop the intelligence package.

25. DS [redacted] described in his statement that the NYP CEOP SPOC records the receipt of all intelligence referrals from CEOP on an FIB CEOP spreadsheet (also named the CEOP Enquiries Register). This spreadsheet provides a general oversight of the progress of each intelligence package and every record is colour coded to indicate the following:

- Red - Indicates that the intelligence referral is still with the FIB waiting to be put together.
- Orange - Indicates that the package has been put together by the FIB and sent to an operational area for action (pre-charge).
- Yellow - Indicates that the package has been actioned and an outcome recorded (no further action or that someone has been charged).
- Green - Indicates that the package has been finalised, actioned and that CEOP has been updated.

26. Responsibility for maintaining this spreadsheet in relation to referrals from CEOP would lie with the nominated NYP CEOP SPOC. DS [redacted] confirmed in his statement "*I sometimes conduct ad-hoc reviews of this spreadsheet to ensure it is being updated, but I do not have capacity to review this on a regular basis."*

27. The NYP CEOP process and procedure documentation states that the NYP CEOP SPOC in the FIB then compiles an intelligence profile on the suspect(s) or victim(s) named in the intelligence incorporating results from checks carried out from a number of sources.

28. A Kent Internet Risk Assessment Tool (KIRAT) assessment is then completed for any identified male suspects over the age of 18. KIRAT is a risk assessment tool used to help identify, from the available intelligence, those individuals most at risk of contact offending. The purpose of this tool is to assist with risk management, prioritisation and workload management within indecent images of children (IIOC) investigations.

29. Completion of this risk assessment gives a low, medium or high priority indication. Low and medium packages will be given 14 days for an officer to action, high risk packages will be given 48 hours and any packages which are believed to be urgent would be given a target timescale of immediate (i.e. the same day).

30. The NYP CEOP process and procedure documents that once the relevant checks have been conducted and KIRAT assessment conducted (if required), the FIB DS or DI will review and authorise the intelligence package for dissemination to the relevant area DI for allocation to an officer for further investigation. Where packages have been identified as being very high risk the intelligence is disseminated whilst research is ongoing to allow an investigation to commence without delay.

31. Once the package has been allocated to the operational DI, the NYP CEOP SPOC will check regularly for updates and progression of the investigation and record the results on the FIB CEOP spreadsheet.

32. On completion of an investigation, a results sheet is completed by the officer in case (OIC) and the NYP CEOP SPOC will record the result and ensure that the originating force/CEOP are updated with the outcome.

Chronological summary of events

33. On 26 November 2013 [redacted] [redacted] (a manager at CEOP) sent an email to the FIBHQ mailbox, attaching 3 documents relating to Operation Spade (one of which was an encrypted presentation), followed by a second email containing password information.

34. Following an automatic notification email being generated by the NYP ISD Service Desk (an IT support function), [redacted] [redacted] requested that the first email be 'unblocked' as it had been stopped by the NYP firewall.

35. A further email was sent by [redacted] [redacted] to [redacted] [redacted], DS [redacted], DI [redacted] and the FIBHQ mailbox which enclosed an unencrypted document that described CEOP's initial child protection risk assessment regarding Operation Spade. This outlines the background of Operation Spade and clarifies that they had been unable to conduct a full risk assessment at that time.

36. The COPINE (Combating Paedophile Information Networks in Europe) scale is a rating system to categorise the severity of images of child sex abuse. Based on the information CEOP had at this time, the majority of purchased material was deemed to be Level 1 on the COPINE scale (the lowest grade), but they urged forces to undertake their own risk assessment.

37. The final email sent that same day was at 5.10pm from [redacted] [redacted] to the FIBHQ mailbox. In this email she states that she would add the presentation to the disc she is sending to NYP that contains screenshots relating to Operation Spade.

38. This email had two unencrypted documents attached. The first was a letter containing details regarding the Operation Spade referral received by CEOP from Toronto Police. The second was a Microsoft Excel

spreadsheet which contained a full list of NYP suspects and their associated order/purchase details.

39. The following day [redacted] sent two further emails in which she states that the disc (enclosing the screenshots) will include both the presentation and invoice details for any postal orders.

40. A full list of passwords to access the disc, presentation, screenshots and invoice details was provided in an email from [redacted] on 2 December 2013.

41. On 11 December 2013 [redacted] sent an email requesting feedback regarding any actions taken, results or decisions made in force, regarding the Operation Spade dissemination.

42. [redacted] responded by email two days later confirming receipt of the disc sent out by CEOP. She stated that despite trying on several computers, she had been unable to open the initial icon using the password previously provided and that she had been told that there was an error decoding each time. [redacted] asks [redacted] if there is anything else she can try to open the disc.

43. On 2 January 2014 [redacted] responded to this email, querying if a new disc was required and what encryption would be compatible with NYP systems.

44. A week later [redacted] requested advice regarding NYP encryption compatibility from ISD Service Desk, who responded on 14 January 2014 advising that a disc in [redacted][1] encrypted format should work fine.

45. During this time [redacted] sent an email to [redacted] (an area analyst) which had attached the 2013 CEOP Enquiries Register (FIB CEOP spreadsheet). This spreadsheet shows that the Operation Spade intelligence had been recorded.

46. Following an update request from the NCA press office, [redacted] sent an email to DS [redacted] on 17 January 2014 stating that there may be some arrests and that she was in communication with [redacted] to get the information as nothing to date had been compatible with NYP software. She confirmed that ISD Service Desk had been requested to help and that she hoped for a resolution the following week.

47. On 18 February 2014 [redacted] sent an email to [redacted] requesting for the disc to be sent in [redacted][2] encryption.

48. [redacted] formally requested feedback from NYP in an email she sent to [redacted], DI [redacted] and the FIBHQ mailbox on 20 March 2014. Attached to this email was an Excel spreadsheet feedback form which contained a list of all the NYP suspect names.

49. On 7 April 2014 [redacted] replied to [redacted] by email asking if she had any further details of the suspects named in the spreadsheet. She stated that this was the first time she had seen the names, due to not being able to access the presentation sent on the disc.

50. On 26 September 2014 an email was sent to [redacted] and the FIBHQ mailbox from an Intelligence officer at CEOP named [redacted]. A letter attached to this email explains that the NCA had referred CEOP's handling of Operation Spade to the IPCC and that they required an urgent update. A further Excel spreadsheet feedback form was also attached, again containing the full list of NYP suspect names.

51. On 30 September 2014 [redacted] (NYP Director of Intelligence) emailed DS [redacted] and DI [redacted] for an update in relation to Operation Spade, following receipt of an email he received the previous day from [redacted] (NYP Head of Crime Operations). This email enclosed a copy of the same letter from the NCA that had been sent to [redacted] on 26 September 2014.

52. Later that day on 30 September 2014, [redacted] provided an email update to DS [redacted] in which she explained that a disc had been received from CEOP on 9 December 2013 but NYP computer systems were not compatible to open it. She stated that she had asked CEOP for further information regarding the Operation Spade packages, but this had not been received to date. She also provided an update in relation to three separate Operation Spade suspect packages which had been created following details being referred to NYP by external police forces who believed that the suspects lived in the North Yorkshire area.

53. DS [redacted] then emailed DI [redacted] the same day in which he included the comment that he was "not satisfied that we are up to speed with it - I had not been briefed on issues – assume you weren't either".

54. DS [redacted] also expanded on [redacted]'s update relating to the three Operation Spade referrals sent from external forces.

55. The first dissemination report referred from an external police force was received by the FIB on 14 February 2014. [redacted] created an intelligence package which was sent to DS [redacted] on 21 February 2014. This package was reviewed, authorised and allocated that same day.

56. The second dissemination report was received by the FIB on 20 February 2014. [redacted] created an intelligence package which was sent to DS [redacted] on 11 March 2014. This package was again reviewed, authorised and allocated that same day.

57. The third package was received by the FIB on 9 September 2014 and was at the time being processed with an allocation date planned for 1 October 2014.

58. Both [redacted] and DI [redacted] completed internal duty reports on 1 October 2014.

59. [redacted] stated in her duty report that following liaison with ISD Service Desk regarding NYP encryption compatibility, she requested a second disk which was received, but again she was not able to access its contents. She states that following this she had further contact by phone with CEOP.

60. In DI [redacted] duty report he documents that on 1 October 2014 he was able to open the Excel spreadsheet attached to one of the original emails and that the outstanding suspects named in this spreadsheet were now being processed.

61. DI [redacted] clarifies in his statement provided to the IPCC that following a conversation regarding Operation Spade with [redacted] and DS [redacted], she directed him to the location of this email. DI [redacted] recalled that after a few delays (formatting type messages), he was able to open the Excel spreadsheet. He also confirmed that he was able to open the disc which was sent from CEOP on his work computer without any issues.

62. Following an internal review by NYP, the incident was referred to the IPCC on 7 October 2014.

63. Both DS [redacted] and DI [redacted] confirmed in their statements to the IPCC that at no point since the Operation Spade intelligence was received by NYP in November 2013 until 30 September 2014 did [redacted] or anyone else raise any issues, concerns, queries or ask for any guidance in relation to this intelligence

Interview with subject

64. On 13 February 2015 [redacted] was interviewed under the misconduct caution. She answered all questions which were put to her and a summary of the interview was produced.

65. [redacted] provided full details of her role, responsibilities,

structure of the FIB and also demonstrated a good working knowledge of the NYP process and procedure surrounding developing intelligence.

66. She confirmed that she had been the NYP CEOP SPOC since the end of September 2013 and that it was her responsibility to check whether any CEOP packages came in, so they could be developed and risk assessed. This involved receiving, recording and dealing with intelligence from CEOP. She also advised that it would be her responsibility to provide requested feedback to CEOP.

67. [redacted] clarified that this role had been re-allocated from her colleague [redacted] who was very unhappy about this decision. As a consequence, no handover of this role was provided to her and they barely spoke for the next few months. She clarified that [redacted] did not want to train her and that she did not want to be trained by [redacted]. She stated that she and a number of other colleagues in the department reported issues regarding [redacted] to their supervisor. This led to increased tensions and created a difficult working environment.

68. [redacted] confirmed that she received the initial emails sent from CEOP on 26 November 2013 and had requested that one of the emails be 'unblocked' as it had been stopped by NYP firewall.

69. She stated that she finished her shift at 5.00pm that day, 10 minutes prior to [redacted] sending a further email to the FIBHQ mailbox containing the Operation Spade letter and the Excel spreadsheet (which contained a list of all NYP subjects and transaction details). [redacted] was then off work for two days [redacted].

70. Upon her return to work on 29 November 2013, she spoke to [redacted] who had dealt with this email and saved a copy of it into a designated Operation Spade folder on their local drive (Q drive), where all important emails relating to Operation Spade were saved in. [redacted] briefly said to her *"CEOP are sending on a disc, the emails haven't worked."* [redacted]

[redacted] stated that no other information was passed to her by [redacted] as they were barely speaking at the time, therefore, she assumed that the details of the NYP suspects would be on the disc.

71. When asked if she would have read the email that was handled by [redacted] and saved for her reference, [redacted] stated that she would have expected to have read it on her return to work.

72. [redacted] could not recall seeing the Operation Spade letter attached to this email but recognised the information contained within it. She also stated that she had no recollection of seeing the spreadsheet attachment and first saw this when DI [redacted] successfully opened it towards the end of September 2014.

73. [redacted] later stated that she didn't think the attachment worked, but when it was queried that the attachment appeared to be unencrypted and not corrupt (as DI [redacted] was later able to open it) she replied "*I guess I never dealt with those emails*". She then stated that she cannot recall whether she just put the email to one side or whether she tried to open the spreadsheet and couldn't.

74. [redacted] recalled that a disc was received from CEOP on 9 December 2013, but despite trying on a number of different computers, she could not access the information it contained.

75. [redacted] stated that she had asked High Tech Crime in either December 2013 or January 2014 to open the disc, but they were unable to due to the disc's encryption.

76. [redacted] thought there might have been an issue with either the disc or password and expected all the NYP suspect details to be on the disc. She confirmed that she sent an email to [redacted] on 13 December 2013 asking if there was anything else she could try to open the disk.

77. [redacted] confirmed that she received a reply from [redacted] on 2 January 2014 asking her is a new disc was required and what encryption should be used. [redacted] stated that she had been off work for the majority of the Christmas period before returning on 7 January 2014 and that she did not remember chasing [redacted] for a reply to her email at any time.

78. [redacted] confirmed that she had requested advice regarding encryption from the ISD Service Desk who had replied to her on 14 January 2014.

79. [redacted] stated that she was seconded to another office from 15 January 2014 to 17 January 2014 but recalled sending DS [redacted] an email in response to an update request from the NCA press office. [redacted] recalls making DS [redacted] aware that there was an issue with the disc but could not recall any specific conversations that took place.

80. When [redacted] was questioned surrounding the amount of time which had passed since the initial dissemination, she stated that the timescales were not ideal, but advised that she felt as though she was actively working to resolve the issue, having contacted CEOP, ISD Service Desk and updated DS [redacted].

81. [redacted] confirms that she sent [redacted] an email on 18 February 2014 requesting for the disc to be sent in [redacted][3] encryption.

82. When asked to explain why it had taken so long to reply to [redacted] email (which was sent on 2 January 2014) she stated that she had been off work for approximately 2 weeks [redacted] and had 3 annual leave days during this period. She then stated that on the remaining days she would have been dealing with other operations which needed to be prioritised.

83. [redacted] confirmed that she had processed other packages that related to Operation Spade which had been sent directly to NYP FIB from external forces and that DS [redacted] had authorised these once the packages were complete.

84. [redacted] recalled being sent an email from [redacted] on 20 March 2014 asking for feedback on the Operation Spade packages. She described that she was shocked when she was an attached spreadsheet which contained a list of the names of all NYP suspects and could not understand why she had not seen the names earlier as this was the information she had been waiting for. She confirmed that she did not flag up any issues to her supervision at this stage.

85. She confirmed that she sent a response to this email on 7 April 2014 requesting further details of the NYP suspects named in the spreadsheet.

86. [redacted] was questioned as to why it had taken her 18 days to reply to this email and stated that it was probably due to her being on leave, attending a PNC course (from 3 April 2014 to 4 April 2014) and due to her workload pressures and prioritising what needed to be done first. She stated that she couldn't understand why it took her that length of time to reply.

87. When asked to explain why after nearly two months had past since she requested a second disc, she had made no further efforts to chase up this information. She stated that she had "*put the ball back in CEOP's court*" by requesting a second disc.

88. [redacted] recalls emailing [redacted] back on 7 April 2014 to ask for further information relating to the NYP suspect names as she was not able to develop any intelligence packages based on their names alone. She stated that the tone of her email response indicated that there was a 'real sense of urgency'. When asked whether she brought this urgent issue to the attention of her supervision, she replied *"I'm not sure,*

I don't remember".

89. [redacted] recalled receiving both a brief phone call from [redacted] and a related email on 26 September 2014.

90. It was highlighted to [redacted] that there had been a large time gap between her last email on 7 April 2014 and the further contact from CEOP on 26 September 2014 where no emails have been sent in relation to Operation Spade. [redacted] stated that she was on a training course in April and came back to being the only person in the office as [redacted] had been on leave for 2 weeks and [redacted] was off [redacted] from March 2014 to August or September 2014. She stated that these factors had increased her workload.

91. She stated that she had been [redacted] and did not feel as though she had any help. She states that she alerted management as to how she was feeling and that she needed help, but this accumulated to her [redacted]. She also confirmed that there had been no formal handover over before she [redacted].

92. [redacted] confirmed that she returned to work in August 2014 for a few days and was then on annual leave for two weeks. Upon her return she worked mornings for 6 weeks before returning to full days and stated that her workload had not been reduced.

93. When queried specifically about the period between April 2014 to July 2014 when she was in work, but made no attempts to follow up with CEOP during this time, she stated that she was on her own and did not have time to chase a response. She clarified that she was expecting a response from CEOP which would have 'triggered the next stage for her', stating "*I did my bit and was waiting for that to flag up for myself*".

94. [redacted] stated that during this period she raised issues with her supervision regarding the size of her workload on a number of occasions.

95. [redacted] recalls completing a duty report in September 2014 and states that she made reference to a second disc being received, however, she had assumed there was a second disc because she had asked for one. When it was queried that she had recorded having further contact by phone with CEOP after requesting the disc, she stated that she could not recall there being any calls and that this period of time was *'hazy'.*

96. Having been shown the NYP CEOP policy and procedure documents, [redacted] stated that she had actually created this material after taking on the NYP CEOP SPOC role.

Policies and procedures

NYP force policy and procedures

97. No relevant NYP force policies have been identified by the IPCC, however there is a documented NYP procedure for handling intelligence received by CEOP. This provides procedural guidance around initial risk assessment, FIB research, allocation of intelligence to operational areas, tasking procedure, investigation by area and package completion.

ACPO and NPIA (2009) guidance on investigating child abuse and safeguarding children

98. The ACPO and NPIA (2009) guidance on investigating child abuse and safeguarding children provides information about investigating child abuse, child neglect and safeguarding children.

99. Section 2 of this report provides information relating to managing the police response to investigating child abuse. This includes:

100. 1.9 - Managing information about child abuse:

> *'When the police receive a referral from another agency, it should be recorded and subjected to a consistent decision-making and risk-*

assessment process.'

101. 1.9.5 - Assessment of external and internal referrals, reports and intelligence:

'The process of managing, recording and assessing referrals and other information relating to child abuse should be actively supervised (e.g. by a frontline supervisor of sergeant rank). This process should be audited by an officer of inspector rank or above.

102. 19.8 - Feedback to agencies and individuals who report or refer concerns about children:

'Forces should have in place systems to ensure that those who identify concerns for children are given feedback on the action taken, as far as possible, and when they have requested or agreed to it.'

Conclusions

Whether NYP processed the intelligence appropriately in accordance with national and force policies

103. The NYP CEOP process document states that an initial risk assessment should be conducted by the FIB DS or DI to take into account the activity alleged and the full intelligence picture to include any additional sensitivities.

104. Although DS [redacted] and DI [redacted] were aware that a referral would be received from CEOP regarding Operation Spade, they were not sent the dissemination email on 26 November 2013 at 5.10pm which contained the spreadsheet of all NYP subjects and letter describing Operation Spade. This email should have been sent from CEOP to all named NYP SPOCs and therefore sent to their personal email boxes rather than solely to the FIBHQ mailbox. As the FIB supervision were not made aware of this initial dissemination of intelligence, they were not in position to conduct an initial risk assessment or in receipt of sufficient

information to conduct this initial assessment.

105. A record of the Operation Spade intelligence was created on the 2013 CEOP Enquires Register, however, there was conflicting information regarding the status of its progression. The text field used to record the progress of intelligence was recorded as 'red', therefore correctly indicating at that time that the intelligence was still with the FIB waiting to be put together, however, the entry on the spreadsheet is coloured green (used as the quick reference), incorrectly indicating that the package had been finalised and CEOP updated.

106. [redacted] had responsibility for maintaining this spreadsheet in relation to referrals from CEOP. Although, there is evidence that this intelligence had been recorded, it is also evidence that the record contained conflicting information.

107. DS [redacted] confirmed that he would sometimes conduct ad-hoc reviews of the CEOP Enquires Register spreadsheet, however the colour of the entry would have incorrectly suggested that this package had been finalised, therefore not prompting any further assessment to be made.

108. It is the IPCC's opinion that the Operation Spade intelligence was not processed in accordance with national and force policies. A record of this intelligence was recorded on a dedicated CEOP spreadsheet (albeit containing contradictory information) but it was not subsequently subjected to a consistent decision making or risk assessment process.

109. The managing, recording and assessment of this referral was not actively supervised, however, it is the investigator's opinion that this was not due to neglect from the FIB supervision. Both DS [redacted] and DI [redacted] have stated that issues relating to accessing the information or obtaining further information from CEOP were not raised to them by [redacted], with the exception of [redacted] email to DS [redacted] in January 2014, in which she states there were access

issues, but that they were being addressed, with a resolution estimated within the week.

110. The process and procedure in place does not mitigate for any risks that the initial CEOP intelligence would not be progressed, or that any issues requiring supervisory oversight, attention or risk assessment would not be raised for the FIB supervision's attention.

111. Whilst it is accepted that a more intrusive and proactive approach by both DS [redacted] and DI [redacted] into the duties and workload of [redacted] may have highlighted issues, this increased level of oversight and effectively 'micro-management' was not employed and there was no information throughout this time period available to them to suggest that this should be the case.

The extent and nature of any access difficulties and what action was taken to ensure the intelligence could be processed once any access difficulties were identified

112. Swift and positive action was taken by [redacted] upon receipt of the initial CEOP email, requesting it to be unblocked due to it being stopped by the NYP firewall. The email contained an encrypted attachment which could not be scanned for viruses and therefore was not able to be received by NYP via email.

113. CEOP had sent an email on 26 November 2013 at 5.10pm which enclosed an Excel spreadsheet attachment containing a list of all NYP subjects and transaction details. This attachment was neither password protected nor encrypted and [redacted] confirmed that she used Microsoft Excel regularly as part of her role at the time.

114. In interview [redacted] was unable to provide a definitive answer as to whether she had overlooked this email or if she had opened the email but not been able to open the spreadsheet.

115. [redacted] documented in her duty report that she could not open

the attachment. In addition to this, DI [redacted] confirmed in his statement to the IPCC that [redacted] had told him in October 2014 that she had not been able to open the spreadsheet and had also directed him to its physical location.

116. This would suggest that [redacted] had sight of this email upon her return from illness in November 2013, but for unknown technical reasons, was not able to access the spreadsheet. There is no evidence to suggest that she seeked technical assistance or guidance in opening this spreadsheet (as she did at a later date when attempting to access CEOP's disc). In hindsight this would be considered to be the best course of action, however [redacted] had presumed that the details of the NYP suspects would be on the disc being sent by CEOP.

117. The exact reasoning for [redacted] not being able to open the Excel spreadsheet in November 2013 is unknown. This same document was opened by DI [redacted] on 1 October 2014 following a few delays which he stated were 'formatting type messages', however this was on a different computer and over 10 months later than originally attempted by [redacted].

118. [redacted] was unable to open the disc that had been sent from CEOP, as was NYP Hi-Tech crime who stated this was due to the disc's encryption. CEOP had confirmed that a number of forces were not compatible with PGP encryption and stated that they could use [redacted][4] encryption as an alternative.

119. Having checked internally with ISD Service Desk on what encryption would be compatible with NYP, the full extent and nature of the technical issues surrounding compatibility and access had been established and [redacted] requested a new disc from CEOP encrypted with [redacted][5] on 18 February 2014.

120. There is no evidence to suggest that this second disc was sent by CEOP

or received by NYP and despite [redacted] stating that she believed the details of the NYP suspects were on the disc, she made no attempt to chase or enquire as to its status.

Whether NYP's Intelligence Bureau was sufficiently equipped, in terms of expertise and resources, to deal with such intelligence

121. There were three permanent IRBOs based in the NYP FIB, two of which worked on a full time basis and one part time. All three IRBOs had worked in the FIB for a number of years and have a wealth of experience and knowledge.

122. The role of NYP CEOP SPOC was re-allocated from [redacted] to [redacted] around October 2013. [redacted] stated that [redacted] was very unhappy with this decision and as a consequence there was no formal handover of this role.

123. DS [redacted] confirmed in his statement that no additional training was provided, but he was confident that she could perform this role as the principles of intelligence handling and putting packages together were the same as to what she did on a daily basis.

124. [redacted] displayed that she was technically competent to undertake this role by processing two separate Operation Spade intelligence packages which had been referred to NYP directly from external forces. Both these packages were compiled by [redacted] and authorised by DS [redacted] in February 2014 and March 2014.

125. It is the investigator's opinion that NYP's Intelligence Bureau had sufficient expertise to be able to deal with this intelligence. The delays in question can not be attributed to a lack of technical or subject knowledge in this role, as demonstrated by [redacted]'s successfully completion of two referrals from external forces, but what appears to be more of administrative neglect and poor case management.

126. [redacted] stated in interview that the workload demands on her were very high, especially when her colleagues were absent due to annual leave and [redacted]. She stated that it had led to her [redacted] for approximately a month. [redacted] was absent from work [redacted] for a total of 40 days between 26 November 2013 and 29 September 2014.

127. It is the investigator's opinion that the NYP FIB had the resources in place to deal with this intelligence and that the periods of resource reduction would be considered a potential contributory factor, but not a reasonable justification for the length or delays involved.

Whether NYP responded appropriately to update requests from the NCA, including 10 December 2013 and 20 March 2014

128. [redacted] confirmed in her interview that it was her responsibility to provide requested feedback to CEOP.

129. There were a total of three formal requests for feedback made between 26 November 2013 and 29 September 2014 by CEOP.

130. The first formal feedback request was made on 11 December 2013 and [redacted] replied appropriately by email two days later, requesting assistance in opening the disc she had received from CEOP that week.

131. A second formal feedback request was sent by CEOP on 20 March 2014 asking for a reply by 16 April 2014. This email contained an attached feedback request spreadsheet containing the list of NYP suspects.

132. Despite [redacted] replying to CEOP on 7 April 2014 and within the requested deadline, it is the investigator's opinion that an 18 day response time was not appropriate in these circumstances. Given the revelation that this was the first time [redacted] had seen the names of the NYP suspects, this response time is considered to be

excessive and not proportionate to the circumstances which [redacted] described herself as 'urgent'. [redacted] was at work for 8 of these days, which would have presented her with opportunities to respond in a more timely fashion.

133. The third formal feedback request was received by [redacted] on 26 September 2014 by email and once again had an attached feedback request spreadsheet containing the NYP suspects. This email also contained information stating that the NCA would be referring themselves to the IPCC and that their request was urgent. [redacted] acknowledged that she was fully aware of this email and had also received a phone call from the NCA that same day.

134. Despite receiving this urgent update request and what is considered to be a further prompt to obtain information relating to the NYP suspect, [redacted] took no action.

135. It is the investigator's opinion that [redacted] did not respond appropriately to this feedback, either by immediately contacting CEOP or raising this to the attention of her supervision. DS [redacted] and DI [redacted] were only made aware of this request on 30 September 2014 directly from the NYP Director of Intelligence.

Whether NYP took any action in respect of the intelligence passed to it by the NCA between 26 November 2013 and 29 September 2014.

136. Initial dissemination emails from CEOP were received by NYP on 26 November 2013. Having been [redacted], [redacted] returned to work on 29 November 2013 and accessed an email sent in her absence that contained an Excel spreadsheet. [redacted] was unable to open this spreadsheet and awaited a disc to be sent from CEOP which she believed would contain information regarding any NYP suspects.

137. On 9 December 2013 [redacted] received the disc, but both herself and NYP Hi-Tech crime were unable to open it due to encryption problems.

138. On 13 December 2013 [redacted] sent CEOP an email requesting advice on how to access the disc.

139. CEOP replied on 2 January 2014 (20 days later) asking if a new disc was required. Due to this request being made over the Christmas period, [redacted] was only at work for 4 days in this period. There were no requests to obtain an update of chase CEOP during these 20 days.

140. Having been on leave from 28 December to 6 January 2014, [redacted] sent an email on 9 January 2014 to ISD Service Desk enquiring about disc encryption compatibility. They replied on 14 January 2014 advising what encryption was compatible with NYP.

141. Despite providing an email update to DS [redacted] on 17 January 2014 in which she stated that she was hoping for a resolution to the software compatibility issue the following week, it wasn't until a month later, on 18 February 2014 that she sent an email to CEOP requesting for a disc to be sent.

142. This response was sent 47 days (nearly 7 weeks) after CEOP had asked if a new disc was required. Essentially, it took 35 days to respond to CEOP to request a new disc once she had received the relevant advice from ISD Service Desk.

143. [redacted] stated in interview that this delay was due to her [redacted] and dealing with other operations that needed to be prioritised. [redacted] was off work continuously from 25 January 2014 to 9 February 2014. However, during this 35 day period, she was at work for 12 of these days (3 of these days were on secondment within NYP with access to her emails). This would have

provided her with opportunities to request this information sooner.

144. No attempts were made by NYP to chase or obtain updates in relation to this requested disc.

145. On 20 March 2014 CEOP sent a feedback request which contained an Excel spreadsheet with a list of NYP suspect names. Despite [redacted] being shocked when she saw these names for the first time and recognising the urgency of the situation, she did not reply to this email until 7 April 2014 (18 days later). [redacted] stated that the delay in replying was due to her workload and being away from work. [redacted] was in work for 5 working days during this 18 day period.

146. As of 7 April 2014, [redacted] was aware that there a number of NYP suspects relating to Operation Spade which had not been investigated. It had now been 132 days (over 4 months) since the initial dissemination of intelligence on 26 November 2014.

147. Following this single email response on 7 April 2014, neither [redacted] nor NYP took any action to obtain further details surrounding the named NYP suspects.

148. On 1 October 2014 DI [redacted] was able to access the original spreadsheet attachment containing the NYP suspect details and also the information on the disc sent by CEOP. Having identified that this intelligence had not been developed to date, the FIB promptly progressed the Operation Spade intelligence.

149. From 7 April 2014 until 1 October 2014, 177 days had past (nearly 6 months) in which the Operation Spade intelligence had not been progressed. [redacted] had been [redacted] from 3 July 2014 to 5 August 2014. However, during this period she had a total of 81 working days. [redacted] stated that she had been [redacted] prior to 3 July 2014. However, she was still working on a full time basis and deemed 'fit

for duty'.

150. There was no organisational progression of Operation Spade intelligence passed to NYP from CEOP between 26 November 2013 and 29 September 2014. During this 307 day (10 month) period there were potentially 25 suspects (believed to be resident in the North Yorkshire area at the time of the alleged offences) who remained unprocessed and potentially at liberty to continue offending.

Recommendations in respect of [redacted]

151. On the basis of the evidence presented above, it is the investigator's opinion that [redacted] has a case to answer for misconduct for failing to adequately progress and develop the intelligence relating to the initial dissemination of Operation Spade intelligence on behalf of NYP between 26 November 2013 and 29 September 2014.

152. Whilst it is accepted that a more intrusive and robust approach by supervision within the FIB may have uncovered these failings earlier, it is the investigator's opinion that the approach and actions taken by [redacted] were the main contributing factor as to why this intelligence was not progressed in a timely fashion

Organisational learning

153. Organisational learning has been identified for the force.

154. The operational risk that intelligence is not progressed by the FIB prior to an intelligence package being authorised and allocated appears to have not been addressed by NYP. The IPCC recommends that NYP implement appropriate internal controls within the FIB to help mitigate such risk and ensure that resilience is built into the material processes of handling intelligence. This would help mitigate against the potentially adverse impact that could occur as a consequence of errors by individuals.

155. Such controls should also ensure a more robust and formalised approach into supervising/monitoring the progression of intelligence by supervision, adding more resilience to the process of handing intelligence packages should the SPOC be absent for any period of time, ensuring the continuous progression of intelligence packages.

156. The IPCC also recommends that NYP review the current NYP CEOP process and procedure documentation as there appears to be no formalised process in place for the FIB DS or DI to have oversight of intelligence development/research prior to packages being submitted to them for authority to allocate.

Kris Kennedy
Lead Investigator, IPCC
16 March 2015