

Inspection of the Metropolitan Police Service

An inspection of the Metropolitan
Police Service's counter-corruption
arrangements and other matters
related to the Daniel Morgan
Independent Panel

Contents

1. Foreword	1
2. Summary	4
3. Introduction	26
4. Investigations and reviews concerning Daniel Morgan's murder	31
The first investigation (1987 to 1988)	31
The inquest (1988)	32
The Hampshire Constabulary investigations (1988 to 1989)	33
MPS Complaints Investigation Bureau (CIB) case review (1996)	33
Covert operations (1997 to 1999)	33
A cold case review (2000)	34
A covert and overt reinvestigation (2001 to 2003)	35
Report to the Metropolitan Police Authority (2006)	35
A further reinvestigation (2006 to 2011)	36
The CPS and MPS joint review (2011 to 2012)	38
Other investigations (2011 to 2021)	38
<i>The Report of the Daniel Morgan Independent Panel</i>	39
5. The MPS's approach to organisational learning	40
Slow to learn	40
A fragmented approach	41
6. Lessons learned and lessons still to be learned	43
National standardised procedures	43
Special Notice 6/99	44
<i>The Murder Investigation Manual</i>	44
The problems of resourcing murder investigations	45
Property management in the MPS	51
Case reviews	55

7. A description of the systems and processes to support the Panel	59
Legal representation	59
A non-statutory inquiry	59
The disclosure protocol	60
The MPS disclosure team	61
MPS disclosure to DMIP	63
Redaction of sensitive material	65
DMIP requests for additional material	66
The pre-publication process	67
8. The relationship between the Panel and the MPS	72
The DMIP's grievances	72
The disclosure protocol	73
Our conclusions regarding the disclosure protocol	75
Accessing the sensitive material	75
Our conclusions regarding accessing the sensitive material	77
HOLMES	80
Our conclusions regarding HOLMES	83
Contacting serving and retired officers and staff	85
Our conclusions regarding contacting serving and retired officers and staff	86
9. Other Panel-related matters	88
MPS governance and resourcing	88
Security	89
Discrepancies	90
The length of the inquiry	93
Our conclusions	93
10. Vetting – an important line of defence against corruption	97
The different levels of vetting	97
Renewing vetting clearance	98
Vetting of transferees	98
The MPS vetting process for recruits	98
The MPS reports a massive reduction in the number of unvetted personnel	98
Data accuracy and the links between HR and vetting records need to improve	99
Review of vetting files against the APP's checklist	99
Personnel in sensitive posts might not have enhanced vetting	99

Operation Fortress and warrant cards	101
The Vetting APP is open to interpretation	101
Managing the risk	104
Quality assurance processes in the FVU are good	106
Vetting for transferees to the MPS	106
Changes in circumstances are not being reported	106
Monitoring for disproportionality has improved	107
Areas where the MPS does not comply with the Vetting APP	108
11. Policies designed to prevent corruption	109
MPS counter-corruption policies mostly follow APP	110
Inconsistent understanding of counter-corruption policies	110
Failure to communicate and uphold clear standards is a high risk on the force risk register	111
Gifts and hospitality	111
Business interests	114
Notifiable associations	117
Ineffective, inconsistent, and fragmented processes to ensure compliance with force counter-corruption policies	121
12. Information security	126
Lawful business monitoring	126
Poor digital device management hinders counter-corruption capability	129
Encrypted apps are a risk to information security	130
The MPS Engaging with the Media Policy is misunderstood	131
13. Corruption-related intelligence	132
Sources of corruption-related intelligence	132
Strategic counter-corruption threat assessments	140
14. Capacity and capability to investigate corruption	143
The anti-corruption command	143
The specialist investigations unit	145
Local professional standards units	145
The future	147
15. The institutional corruption label	148
The DMIP definition of police corruption	148
The DMIP definition of institutional corruption	149

The NPCC definition of police corruption	149
Our views on the DMIP’s finding of institutional corruption	151
Annex A: Vetting checks	156

1. Foreword

In 1987, Daniel Morgan, a 37-year-old private investigator, was brutally murdered in London. The Metropolitan Police Service's investigation was hampered by police corruption.

Some 35 years later, despite several reinvestigations and reviews, Mr Morgan's murder remains unsolved. On behalf of all those who have worked on our inspection report, we send our condolences to Daniel Morgan's family and friends. The circumstances of the murder, and many of the failings that followed, represent a most unsightly stain on the Metropolitan Police's reputation. In 2021, following an eight-year-long review, the Daniel Morgan Independent Panel labelled the force as "institutionally corrupt".

We set out to establish what the force has learned from its failings and whether they could recur. We looked for evidence that someone, somewhere, at the highest levels of authority in the Metropolitan Police, had adopted the view that 'this must never happen again'. We wanted to see whether the force had decisively put in place all the measures necessary to make sure that it couldn't.

On a positive note, the Metropolitan Police's homicide investigation arrangements bear little resemblance to those of 35 years ago. The force solves the vast majority of homicides it investigates.

The force's capability to investigate the most serious corruption allegations is particularly impressive. These investigations are thorough and apply the most up-to-date methods. Other forces regularly call on the Metropolitan Police's expertise. The force's confidential reporting line also works well. The force has even introduced a dedicated team to support 'whistle-blowers' – a development we haven't seen in other police forces.

To its credit, the Metropolitan Police has, in recent years, greatly reduced the number of its personnel who have not been security vetted. But this alone isn't enough: the force doesn't know whether all those in sensitive posts – such as child protection, major crime investigation and informant handling – have been cleared to the level needed. This strikes us as unprofessional: it creates obvious risks.

In each of the two years before our inspection, more than 50 people who had committed offences were allowed to join the Metropolitan Police. Most offences were not especially serious, but they did include theft, handling stolen goods and wounding. And some recruits were closely connected to known criminals.

While a case might be made that accepting some of these people into the force was justifiable, after their recruitment the force failed to introduce sufficient measures (such as monitoring and closer supervision) to lessen the risks they posed.

We were also unimpressed by the force's application of its counter-corruption policies. We were surprised to find that police officers and staff did not have to disclose their association with journalists or extremist groups. This is despite national guidance to the contrary and a history of scandals.

The Metropolitan Police kept comprehensive records throughout its dealings with the Daniel Morgan Independent Panel. But, in more general terms, some of its administrative practices and record keeping were woeful. Over 2,000 warrant cards issued to personnel who had since left the force were unaccounted for. The force couldn't say to whom it had allocated mobile phones and tablets. Some of its records about the receipt of gifts and hospitality were in disarray. These all indicate an organisation which is not taking the risks of corruption anywhere near seriously enough.

Returning to the Independent Panel, the force provided meagre resources to support them, and should not have raised objections to all Panel members having access to the material they needed to see. However, we found no evidence of any deliberate or co-ordinated campaign to intentionally frustrate the Panel's work. The MPS did not ultimately deny access to any material. Based on the evidence we have seen, and recognising that there is extensive criticism within this report, we would not describe the Metropolitan Police as institutionally corrupt.

We also recognise that the Metropolitan Police responded promptly to the Panel's report. Within a few days of its publication, the force set up a team to deal with it.

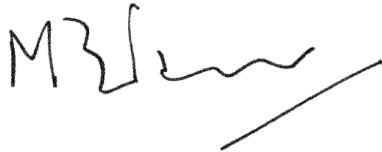
The Metropolitan Police Commissioner said that the force could "listen more", and become more "open and transparent" and less defensive. This is a step in the right direction, but it contrasts sharply with some of our previous experiences with the force. Since 2016, we have repeatedly raised concerns with the Metropolitan Police about certain aspects of its counter-corruption work, including: its inability to monitor its own IT systems; shortcomings in its vetting processes; its failure to adopt nationally approved counter-corruption recording methods; and its failure to form effective links with organisations that support vulnerable people (who may fall prey to corrupt police personnel, often through sexual abuse). Our advice largely went unheeded.

Inexcusably, 35 years after Daniel Morgan's murder, the force had not taken adequate steps to correct all that went wrong during its investigations. Arrangements for the storage of property and exhibits were especially dire: hundreds of items (including cash, jewellery and drugs) could not be accounted for; firearms had not been correctly stored; and some property stores were overflowing and lacked adequate security (we even found that the security access code for one store had been inscribed on the outside of the door).

In too many respects, the findings from our inspection paint a depressing picture. The force has sometimes behaved in ways that make it appear arrogant, secretive

and lethargic. Its apparent tolerance of the shortcomings we describe in this report suggests a degree of indifference to the risk of corruption.

Our report contains descriptions of five causes of concern and two areas for improvement. It includes 20 recommendations for change. If public confidence in the Metropolitan Police is to be improved, they should be among the Commissioner's highest priorities.

A handwritten signature in black ink, appearing to read 'M Parr', with a long horizontal stroke extending to the right.

Matt Parr CB

Her Majesty's Inspector of Constabulary

2. Summary

On 10 March 1987, Daniel Morgan, a 37-year-old private investigator, was murdered in a car park behind the Golden Lion public house in Sydenham, London. He had been struck on the head with an axe.

There have been several investigations and reviews into Mr Morgan's death, none of which have led to a conviction for his murder. From an early stage, there were concerns that police corruption played a part in the murder, the failure to bring his killer to justice, or both.

In 2013, the Home Secretary, set up the [Daniel Morgan Independent Panel](#) ('the DMIP' or 'the Panel').¹ On 15 June 2021, the Home Secretary published the DMIP's 1,251-page report. It contained excoriating criticism of the Metropolitan Police Service (MPS). The Panel concluded that some aspects of the MPS's approach amounted to "institutional corruption".

On 16 July 2021, in the light of the report's criticism, the Home Secretary commissioned HMICFRS to inspect the MPS under section 54(2B) of the Police Act 1996.

Our role wasn't to reinvestigate the murder; it was to consider opportunities for organisational learning from all the Daniel Morgan investigations and reviews and assess how the MPS responded to them. We were also asked to consider the MPS's response to DMIP requests for disclosure and access to material during the inquiry. We were also asked to assess the MPS's understanding of, and response to, police corruption.

Investigations and reviews

The MPS has invested heavily in the Daniel Morgan investigations and reviews over the years; it is deeply regrettable that they have not resulted in those responsible being brought to justice. There are several reasons for this. They include poor – and, in some instances, corrupt – practices.

¹ References in this report to the DMIP include panel members, its staff, and representatives.

The first investigation (1987 to 1988)

The MPS started its first investigation on 10 March 1987, immediately after Daniel Morgan's murder. Although six men, including three who were then serving police officers, were arrested in connection with the murder, it did not lead to any charges.

The management of that initial investigation was very poor. And there was strong suspicion that at least some of those who were to be arrested were alerted beforehand through the improper disclosure of information (a 'tip off').

The MPS's failings meant that, from the outset, it lost opportunities to gather evidence. This affected subsequent efforts to solve the case.

Further investigations and reviews

A series of investigations and reviews followed which, directly or indirectly, related to Daniel Morgan's murder. They involved not only the MPS but also Hampshire Constabulary, the Police Complaints Authority (PCA)² and the Crown Prosecution Service (CPS).

The MPS's approach to organisational learning

We assessed the MPS's appetite for learning. We found that it had been slow to learn. Certain lessons that should have been learned over the years had been disregarded and mistakes repeated.

We recognise that the MPS is now taking organisational learning more seriously. But senior officers acknowledge that there is more to do, through their development of a "corporate organisational learning framework", and the ongoing implementation of a systemic approach to organisational learning in the MPS. But we still found the MPS's approach confusing. Some within the force had the same reservations. They told us that organisational learning lacks co-ordination and that the whole process is "fragmented".

However, the MPS contends that its "programme to implement organisational learning is, for the first time in the MPS, directly aligned to the [MPS's] strategic objective to '[l]earn from experience, from others, and constantly strive to improve'."

Lessons learned and lessons still to be learned

We considered some of the more significant changes that had been made, or should have been made, during the years since Daniel Morgan's murder. We took account of all the profound changes in policing during the many years since then. We considered, for example, scientific and technological developments, such as the use of DNA profiling to solve crimes and the introduction of computerised systems to support crime investigations. We also considered the findings from inquiries into other high-profile investigations.

² In 2004, the PCA was replaced by the Independent Police Complaints Commission (IPCC) which, in 2018, was itself replaced by the Independent Office for Police Conduct (IOPC).

MPS developments

We did not find any great changes in the way the MPS dealt with serious crime after Daniel Morgan's murder, until March 1999. The MPS then issued guidance, titled 'Major crime review'. The guidance was a significant milestone in the force's approach to major crime investigations. In conjunction with the 1998 ACPO *Murder Investigation Manual* (which had recently been introduced), it provided comprehensive direction for homicide investigations.

Resourcing murder investigations

Assembling sufficient resources for a murder investigation during the 1980s and 1990s was a recurring problem in forces throughout the country. Certainly, dedicated teams of suitably trained and experienced homicide detectives did not exist in the MPS in 1987.

The situation improved in the MPS after March 1999. The MPS increased staffing levels within 'area major investigation pools' to make them more self-sufficient. They fell within the jurisdiction of the MPS's homicide and major crime command (SC01) and continued to do so until 2019.

In June 2019, the MPS introduced its specialist crime command. It brought together three previously separate commands: SC01, the serious and organised crime command (SC07), and the Trident gang crime command (SC08). This consolidated approach is more flexible as it provides a greater resource pool that can be called on for major enquiries.

Family liaison

At the time of Daniel Morgan's murder in 1987, the extent of police involvement with a victim's family was very much at the discretion of the senior investigating officer (SIO). Despite the obvious importance of family liaison, it was not put on a formal footing until some years after Daniel Morgan's murder.

But even if the MPS's initial treatment of the Morgan family was not unusual by the standards of the day, there were plenty of opportunities to change as the years went by. However, the DMIP concluded that the family has been treated poorly throughout.

Based on the MPS's current commitment to training family liaison officers (FLOs) and the scale of their deployments, we concluded that the MPS has now put considerable investment into family liaison.

Crime training

An extensive examination of the MPS's crime training, and the quality of its courses, was beyond the remit of this inspection. But we wanted some assurance that all who might be involved in responding to the most serious crimes knew what they were doing, or where to turn for help.

Crime training has changed considerably since 1987. In so doing, it has taken account of scientific and technological developments and the very many changes in legislation.

Much of the training has been driven nationally, but a lot has still been at the discretion of individual forces.

The MPS provides a wide range of training courses for crime investigation, with national accreditation at four levels of increasing complexity. The force has also produced comprehensive investigative 'toolkits' to help all officers, which can be accessed via the intranet.

Crime scene management

Following Daniel Morgan's murder, the MPS should have secured the scene, thoroughly searched and examined it, and kept clear and accurate records of all who came and went. The MPS appears to have failed on all counts. These inadequacies so early in the investigation, and others which were yet to arise, would have created difficulties for any investigation that followed. There were similar problems during the investigation into Stephen Lawrence's murder in 1993.

However, since then crime scene management has developed in line with technological and scientific advances, and national policy.

Exhibits and property

The fact that property and exhibits were mismanaged during the initial Daniel Morgan investigation was clear from a very early stage. The MPS should have taken action to ensure exhibits and property were always correctly handled in the future. But some subsequent high-profile cases suggest that the MPS didn't fully deal with it.

During our inspection, we examined the arrangements not only for homicide cases but also for other serious offences and for volume crimes. Our findings painted a dismal picture. They fell into three broad categories: space, security and supervision.

We found that some property storage facilities were not fit for purpose. The stores were overflowing with items, which were piled haphazardly. We had particular concerns about firearms. And even if there was available space in a store, some provided little in the way of security; we found that seized property could not always be accounted for.

A clear lack of supervision, insufficient training, and the resultant incorrect handling of exhibits only exacerbates the problem. We understand that the MPS intends to introduce a new, electronic property management system in November 2022. The current situation is wholly unsatisfactory, and given the lessons of Daniel Morgan's case, impossible to defend. The MPS has much more work to do.

Case reviews

If a murder investigation review is to be worthwhile, it must be painstakingly thorough, open and honest, and the reviewing officer must be prepared to confront poor practice and highlight missed opportunities. The reviews of the Daniel Morgan investigation were largely ineffective.

The force's specialist crime review group (SCRG) now performs this role. A specialist crime command officer also chairs a case closure panel, which considers both solved and unsolved murders before investigations are closed. In addition to ensuring that all

reasonable lines of enquiry have been completed when a case hasn't been solved, the panel should identify any organisational learning from both sets of cases (that is, solved and unsolved).

The CPS and MPS joint review (2011–2012)

A joint CPS and MPS review following the collapse of a trial in 2011 identified 17 'good practice points' and made 1 overarching recommendation. The recommendation was to disseminate the review within the police and CPS, so that they could consider good practice points in future cases. It was virtually the only review of the Daniel Morgan case to identify opportunities for organisational learning.

But it is clear that the MPS paid little, if any, attention to the joint MPS and CPS report when it was produced in 2012. Although the MPS implemented almost 30 percent of the good practice points by default because of national changes and guidance, the remainder appear to have lain in abeyance until 2019. This too is wholly unsatisfactory. The MPS should have taken steps to ensure similar mismanagement of a case would not be repeated.

The Report of the Daniel Morgan Independent Panel

It is encouraging that the MPS has indicated that it will consider all matters that the DMIP report has highlighted, regardless of whether they are the subject of recommendations. Only eight days after its publication, the MPS established an operation (Operation Drayfurn) to respond to the report.

A deputy assistant commissioner (DAC) has overall charge of the operation and is answerable to the force's deputy commissioner. This level of seniority, and the prompt response, indicates the importance that the MPS has attached to the report. This commitment should be maintained.

The relationship between the Panel and the MPS

There was a huge amount of material for the Panel to review and it was important that the appropriate systems and processes were introduced from the outset. The DMIP reported that it faced major problems in gaining access to material and systems; it considered the problems unnecessary.

In our report, we group the DMIP's grievances under four headings: the disclosure protocol; accessing the sensitive material; HOLMES; and accessing retired and serving officers.

The disclosure protocol

The Panel was not established under the Inquiries Act 2005 and therefore it did not have statutory powers. Importantly, as a non-statutory inquiry the DMIP could not demand access to material and systems in the same way as a statutory inquiry. Therefore, a [disclosure protocol](#) ('the protocol') was needed, setting out the terms, responsibilities and expectations of the MPS and the Panel in relation to providing and receiving documents.

Reaching agreement on the terms of the protocol proved difficult. The Panel complained that the MPS held up progress on agreeing the wording of the protocol and thus frustrated the start of their work. The Home Secretary announced the establishment of the Panel on 10 May 2013, and it formally started its work on 17 September 2013. But the protocol was not agreed until November 2014, after the Panel's second Chair took up her post. The first DMIP Chair had resigned in November 2013. The MPS told us that, from its point of view, this created a hiatus and hindered progress until the second Chair's arrival in September 2014.

It seems that the most contentious matter was whether all Panel members would be allowed to see 'sensitive' documents which the MPS provided, or whether access would be limited to the Panel's Chair. All members of the Panel wanted to be able to see all the material. The MPS, on the other hand, preferred an approach where the most sensitive documents would first be reviewed by the Panel's Chair.

We recognise that the MPS had to adopt a cautious approach to protect highly sensitive material. However, we conclude that it should not have taken 18 months or more for the MPS to agree that all members of the Panel should be given access to all the material in unredacted form.

Accessing the sensitive material

Before the DMIP saw any documents, the MPS considered their content and copied any which they had valid reasons for believing contained sensitive information. They then redacted the copies by manually blocking out any material they deemed sensitive. However, in accordance with the protocol, members of the Panel and their legal representatives were permitted to view unredacted copies on MPS premises. This meant that the Panel had to travel to MPS premises in East London – where all the documents were stored – to view unredacted sensitive material. The Panel members felt that they wasted a lot of time travelling to and from East London.

We understand that, in late 2013, long before the disclosure protocol was agreed, the MPS prepared a redaction policy for use during the Panel's inquiry. The MPS said that it sent the policy to the DMIP. But even working to a recognised process, redaction can be a subjective exercise, defined by context and a comprehensive understanding of the subject matter. The DMIP considered that the MPS unnecessarily redacted a lot of material.

We can appreciate both the MPS's and the DMIP's points of view over this matter. However, the MPS might have adopted an overly cautious approach at times.

Nevertheless, we concluded that the DMIP's complaints in this regard had more to do with convenience than being denied access to material. The DMIP accepted that, ultimately, it was not denied access to anything. And arrangements for viewing sensitive material accorded with the disclosure protocol, to which all parties agreed.

HOLMES

Access to the MPS's HOLMES computer system was an issue throughout the inquiry. The Panel considered that access to HOLMES was essential for its work. It was confident that, with proper access, it would have been able to finish its work much sooner.

The MPS, on the other hand, contended that it had a general obligation to protect information held on the HOLMES system. It was particularly important in Daniel Morgan's case because it was still a 'live' investigation and the MPS was anxious to ensure that it did not prejudice any future proceedings. Furthermore, the MPS was concerned that HOLMES held information which, if released to the public, could put lives at risk.

Nevertheless, in October 2014, the MPS agreed to allow unrestricted access to the HOLMES system, on MPS premises, to the Panel members and their legal representatives. The Panel saw this as an interim solution but still wanted to be able to access HOLMES from its own premises through a HOLMES terminal or a suitable laptop computer. The MPS eventually agreed to supply a terminal in 2015, and did so again in 2018, but on both occasions the Panel declined because of the cost.

The MPS also considered the laptop computer option but, for several years, rejected it for legitimate security reasons. However, the MPS changed its position in 2020, when technology allowed the MPS to transfer material to the more secure Cloud system. The MPS then provided the DMIP with an encrypted HOLMES laptop.

We concluded that there should never have been any doubt about the DMIP accessing the HOLMES database. This was an inquiry into a murder case involving police corruption; for obvious reasons, the DMIP needed to compare HOLMES records with physical documents. The MPS should have recognised this from the outset. But we are satisfied that – from late 2014 – the DMIP had proper access to it.

That said, once the DMIP had been granted access to HOLMES, the argument about who, where and how they had access grew out of all proportion. In our view, the MPS took the correct course of action about security and declined to provide a laptop until technology provided a secure option. We noted, too, that the MPS did show some flexibility: it agreed to let the DMIP have a HOLMES terminal installed in its own offices. The Panel chose to reject the MPS's offer.

Accessing retired and serving officers

Early in the inquiry, the MPS issued a force-wide intranet appeal about requests for information from the DMIP. But the appeal did not make clear that anyone could approach the DMIP directly with information, rather than going through a force central point of contact. In the Panel's view, such a process might have deterred anyone who wanted to provide information in confidence.

The MPS subsequently circulated a second force-wide intranet article to all personnel saying that they could contact the DMIP directly. However, we agree that the wording of the MPS's initial appeal created the impression that it wanted to control, or otherwise interfere with, the DMIP's contact with serving officers and police staff.

The DMIP also accused the MPS of withholding correspondence after it failed to promptly send letters on its behalf to two former officers. We found that the MPS had taken over four weeks to forward the letters, but that included a Christmas and New Year holiday period. We acknowledge that the DMIP may have become frustrated by the delay but consider it unduly harsh to intimate that the MPS had in some way adopted underhand tactics to frustrate the inquiry.

Other Panel-related matters

MPS governance and resourcing

At the outset, the MPS established a small disclosure team to assist the DMIP, and a strategic oversight group to provide governance. The oversight group was led by an assistant commissioner (latterly the Commissioner) and included other senior officers. But we found a lack of continuity when they moved to different roles.

We were unable to find any evidence that the oversight group met between 2015 and 2019, after the first assistant commissioner temporarily left the force and responsibility passed to another officer of the same rank. Meetings resumed in 2019, when a third assistant commissioner, supported by an officer of commander rank, assumed responsibility.

When the new assistant commissioner and commander took charge in 2019, they reviewed the situation. They found that the disclosure team was under-resourced. They discussed matters with the Panel, who were frustrated and of the same opinion. The senior officers increased the size of the disclosure team, which improved matters.

We concluded that governance and resourcing problems provided a strong indication that the MPS's practical commitment to supporting the inquiry was not as great as it should have been.

Security

For security reasons, the MPS was reluctant to allow the Panel to see everything it wanted in the way it wanted. This is demonstrated especially by the MPS's approach to HOLMES and sensitive material.

The DMIP was never content with the MPS's approach to redacting sensitive material. It was particularly aggrieved when it found that the member of MPS staff who generally made redaction decisions did not have appropriate security clearance; all the DMIP's staff, on the other hand, did have. This should not have happened.

However, we also found some apparent justification for the MPS's security concerns. According to the MPS, when the DMIP sent a courier to collect the first batch of MPS material in October 2014, the MPS conducted a security check and found that the courier had six criminal convictions, including offences of dishonesty and involving weapons.

And, in August 2021, when the DMIP was due to return some material to the MPS, with which it had been provided, it was unable to produce all the items. The DMIP could not be specific about all the missing items, which it said had been "shredded" in error. The MPS's records indicated that there were 42 missing items.

Discrepancies

We found some discrepancies between the DMIP report and the MPS's records. This included details of when the MPS provided the DMIP with material, when the DMIP was able to start working on that material, incorrect reporting about the availability of documents, and incorrect reporting about other matters.

The length of the inquiry

When the Home Secretary announced on 10 May 2013 that the Panel was to be established, Daniel Morgan's family had already waited over 26 years for answers. But the family still had to wait another eight years for the DMIP to publish its findings. The DMIP has largely attributed the delay in completing its own inquiry to the MPS's lack of co-operation.

We find it difficult to understand why matters relating to the disclosure protocol, travelling to East London to view sensitive material, and access to HOLMES would – either individually or collectively – have extended the inquiry for seven years beyond an initial estimate of one year.

We looked at other potential reasons for why the inquiry took so long. We concluded that the main reason for the length of the inquiry was the scope of the DMIP's inquiry, as defined in its terms of reference.

Rather than 'drawing a line' and looking back at events over the previous 26 years, the DMIP's work was concurrent with ongoing MPS and IOPC corruption investigations. This meant that the DMIP did not receive its final documents from the MPS until March 2021.

Undoubtedly, the volume of material also contributed to the length of the inquiry. At the start, it filled almost 600 crates. It is perhaps understandable that the task at hand was underestimated at the outset. But the potential timeframe should have become more apparent as time progressed. However, when the DMIP considered the MPS's offer of a HOLMES terminal in 2015, the Panel told the MPS that it would have completed its work by July 2016.

Vetting

Vetting – an important line of defence against corruption

Vetting is required for anyone who wishes to become a police officer, a member of police staff or a volunteer. It is also used to ensure that those who have access to police equipment, information and premises through their job, such as contractors, have a suitable background and history.

In the MPS, the vetting checks are carried out by the force vetting unit (FVU).

Vetting decisions – either to accept or reject an applicant – can only be based on the information available to the vetting team at the time they perform the relevant checks; they are made at a snapshot in time.

The MPS reports a massive reduction in the number of unvetted personnel

In December 2018, at the time of our [previous vetting inspection](#), we established that the force had approximately 16,000 personnel (about 37 percent of its entire workforce) who had either never been vetted or whose vetting had expired.

During this current inspection, the MPS reported that this figure had decreased significantly to 671. We reviewed 40 vetting files to see if the checks recommended by

the College of Policing's Vetting Authorised Professional Practice (APP) had been completed. We found that, in every case, they had been.

Monitoring for disproportionality has improved

Encouragingly, we found that the MPS had introduced a process to identify any disproportionality in its vetting decisions. Disproportionality was identified but this has recently reduced. The MPS told us this was due to the work of a new 'equality cell'. Staff in this team attend events in the community, explain how the vetting process works and address any concerns about the process.

Data accuracy and the links between HR and vetting records need to improve

Although the MPS has approximately 44,000 personnel, the vetting database has over 61,000 records of personnel with current vetting. The MPS told us this was due to the presence of many duplicate records, which doesn't inspire confidence in the accuracy and reliability of the process. In response to our finding, the MPS said "this is an IT system functionality matter, not a process accuracy and reliability shortcoming".

Personnel in sensitive posts might not have enhanced vetting

People working in more sensitive posts generally need a higher level of vetting. The FVU was unable to say who occupied these designated posts and their current level of vetting. The MPS is introducing a new vetting IT system but until the new system is fully functional, the limitations in the current arrangements strike us as unprofessional. They create obvious risks. This is not a new finding.

The Vetting APP is open to interpretation

When assessing the suitability of applicants, the Vetting APP does not give a list of convictions or cautions that should lead to a vetting rejection. Each case must be considered on its own individual merits. APP appears to give forces considerable latitude to set their own standard in relation to the level of risk they are willing to accept when deciding on the suitability of applicants to become officers.

We have concerns about the MPS's interpretation of the Vetting APP and that the force may have lowered its vetting clearance thresholds based on a heightened risk appetite. In other words, the Vetting APP provides scope for the MPS (and other forces) to lower the standards: too widely; too readily; and too far.

The vetting panel reviews all cases where vetting is refused

The MPS reviews any vetting refusals and appeals at a monthly vetting panel (VP). The VP considers each case on its merits and either ratifies the refusal, recommends the refusal is changed to a clearance, or asks the FVU to interview the applicant to obtain more information. The MPS refers to this decision-making process as its 'risk appetite'. The FVU takes account of the VP's rationale when making decisions on subsequent cases, although it continues to assess each case on its own merits.

We found that there is tension between HR objectives to meet recruitment targets and the FVU objectives to admit only those with sufficiently high levels of integrity.

We established that, since 2018, there has been an increase in the number of people recruited with prior recordable offences. This coincided with the implementation of the Vetting APP and increases in recruitment under the 'uplift programme'. The combination of recruits with recordable offences, those with declarable associations, and the directorate of professional standards (DPS) not being aware of all of these, paints a worrying picture.

Managing the risk

In accepting that some recruits may pose a risk to the organisation, whether through previous convictions or their associates ('declarable associations'), the MPS should manage the risk. There are officers with an identified risk who have not been appropriately assessed by the DPS. This is unprofessional: opportunities to put mitigation measures in place to prevent corruption have been lost. We found that the MPS did not have sufficiently well-established and robust processes to implement risk mitigation measures. This is not what we would expect to see in a well-run force.

Changes in circumstances are not being reported

MPS personnel are required to report any change in their circumstances to the FVU. Despite attempts to make personnel aware of their obligations, between January 2021 and September 2021 the FVU had only received 48 change of circumstance forms. In a workforce of 44,000, it is extremely unlikely that this is a true reflection of changes during that period.

Areas where the MPS does not comply with the Vetting APP

Although the MPS does exceed the standards set by Vetting APP in some respects, we found three areas in which it does not comply, or cannot be sure whether it complies, with APP. These are in respect of designated posts, risk mitigation and changes in personal circumstances.

Policies designed to prevent corruption

The Counter-Corruption (Prevention) APP outlines what policies forces are expected to have to prevent corruption and provides guidance as to their content. Clear and concise corruption prevention policies help to guard against corrupt activity.

MPS counter-corruption policies mostly follow APP

We examined the MPS policies in respect of gifts and hospitality, declarable associations and business interests. These policies mostly followed APP but, in some important respects, didn't. Some personnel we spoke with had an awareness of the policies, but others' knowledge was extremely limited.

Gifts and hospitality

The receiving of, or the offer of, gifts or hospitality is a regular occurrence in many organisations. But in policing, if personnel accept gifts or hospitality in the course of their duties, their impartiality may be justifiably called into question, or even compromised.

In the places we visited, we found that responsibility for maintaining the records varied and the registers were often under-used. However, record keeping within specialist departments was significantly better than in basic command units (BCUs).

Business interests

Police forces have a responsibility to avoid any conflict between the business interests of their officers and staff and their roles within policing. Where an officer or their relative has a business interest, the officer is required by law to declare it. Where a force considers the business interest incompatible, the request can be refused. Or, it may be managed through the imposition of restrictions or conditions.

We found the MPS has a detailed business interest policy, which includes annual review, risk management and appeals processes. However, having a clear policy is one thing; robustly implementing it is another.

Without manually searching a series of individual electronic folders, the local professional standards units could not tell us: how many officers and staff had a business interest; how many had been approved with conditions; what the conditions were; how many had been refused; and the review dates.

In addition, personnel within the local professional standards units and the DPS told us they do not have the resources to monitor compliance.

Declarable associations

The purpose of this policy is to protect officers, staff and the force from people who may, or may be perceived to, compromise their integrity; for instance, those with unspent criminal convictions. In cases where the association presents a significant risk, conditions and restrictions may be applied. These should be subject to regular review and monitoring.

The current MPS Declarable Associations Policy contains a surprising omission and is out of date. It refers to the [National Policing Improvement Agency](#), an organisation that hasn't existed since 2013. It also does not include requirements for personnel to disclose any relationships with journalists, and any relationships with extremist groups.³

We also found three deficiencies in the risk assessment process: those making the risk assessment don't have access to all of the corruption-related intelligence; they have not been trained; and their assessment is wholly subjective and open to individual interpretation.

In common with the response in respect of business interests, the local professional standards units said that providing detail of: who had a declarable association; what the risk levels were; and what conditions had been set, would require them to manually open and read documents in multiple electronic folders. They also told us they had no time to monitor their low and medium-risk declarable associations.

³ After our fieldwork ended, the MPS informed us that the policy had been revised and was awaiting sign-off.

This means that officers' compliance with any conditions that may have been imposed goes unchecked. This situation needs to improve.

Ineffective, inconsistent and fragmented processes to ensure compliance with force counter-corruption policies

We found the processes in the MPS to ensure compliance with counter-corruption policies were, in the main: ineffective; inconsistent; fragmented; and hindered by a lack of resources and, in some instances, skills.

Many supervisors told us that they were not provided with sufficient information to manage corruption risks posed by their personnel. We spoke to many officers who did not have a current performance development review (PDR), or the associated checklist. The checklist is extensive. It prompts the supervisor to ask about, amongst other things, any business interests or declarable associations the individual may have, and to check that force counter-corruption policies are being complied with.

Information security

Lawful business and IT monitoring

Lawful business monitoring (LBM) is a legitimate activity for forces to monitor their information systems and methods of communication. IT monitoring is part of LBM and can be used to automate proactive checks on the use of all a force's IT systems and communication devices. Most forces proactively use IT monitoring to enhance their ability to identify corrupt personnel.

In January 2017 and September 2019, we warned the MPS about its lack of IT monitoring, yet we found it still does not have the capability to proactively monitor its IT systems. The MPS is – by a substantial margin – the largest force in the UK, yet is one of only a tiny number that does not have proactive IT monitoring capability. It is high time that the force took this matter much more seriously.

Poor digital device management hinders counter-corruption capability

We were told that the MPS's digital policing (DP) department has started to improve its management of mobile devices. Despite this, record keeping in respect of such devices was still poor. It is still – indefensibly – unable to state with any certainty who each phone or tablet is allocated to. The MPS is planning to introduce a new telephony system ('Intune'). If successful, this should enable better control of these assets. At the time of our inspection, the MPS had allocated 45,000 SIM cards, which emphasises the scale of the problem.

But we were pleased to see that the MPS does not allow encrypted apps on its force mobiles as a matter of routine, as this would make the monitoring of what officers and staff are sharing on their work phones very difficult. However, many officers and staff told us they do not have a force-issue mobile phone. They therefore use their private mobile phones, including encrypted apps, for operational purposes, which is a risk. In addition, many officers and staff told us that, whilst there is guidance on the use of phones, it is confusing and the instructions, for instance in respect of personal use of force-issue phones, are unclear.

Corruption-related intelligence

The MPS obtains corruption-related intelligence from a wide range of sources. These include a significant number of reports raised by the workforce through confidential methods. However, almost all the cases we saw involved the force reacting to items of intelligence that had been referred to the DPS, rather than proactively seeking it.

Organisations that work with vulnerable people can be a valuable source of intelligence to help identify officers and staff who abuse their position for a sexual purpose. Since 2017, we have recommended that forces establish regular links between their counter-corruption units and those agencies and organisations that support vulnerable people. During this inspection, we again found no evidence that the MPS was doing this.

Strong internal processes enable reports of suspected wrongdoing

All officers and staff we spoke to were aware of their responsibility to report wrongdoing and told us of their willingness to do so. The MPS has a confidential reporting system that is managed by the DPS. This is called the 'Right Line'. We found most of our interviewees were aware of the Right Line and how to use it.

Some told us about the potential consequences of reporting wrongdoing. They feared being ostracised by their team or labelled as a troublemaker if they were identified as having made such a report. The leadership of the MPS should be doing more to inculcate a culture in which concerns such as this do not exist.

The MPS is the only force in which we have seen a dedicated team to support 'whistle-blowers'. Anyone who is given 'whistle-blower' status will have a point of contact within the whistle-blower team throughout their career. Where time allows, the team also supports those who provide information but do not fall within the statutory whistleblowing criteria.

The categorisation of corruption-related intelligence still needs to improve

The MPS is one of a very small number of forces which is still not recording corruption-related intelligence in line with national Counter-Corruption (Intelligence) APP categories. It is using its own bespoke corruption intelligence categories. In our [2019 PEEL report](#) we identified this as an area for improvement. We similarly highlighted this in another 2019 report, [Shining a light on betrayal](#). The MPS still needs to ensure its corruption-related intelligence is categorised in accordance with the national categories.

Multiple systems for recording corruption-related intelligence presents a risk

The MPS records its corruption-related intelligence on multiple IT systems. This presents a risk as not all those who analyse corruption-related intelligence have access to all the information they need. We also found the management and storage of corruption-related intelligence to be confusing and disjointed. The MPS would benefit from storing all its corruption-related intelligence in a way that can be accessed by everyone who needs it for their role (for security purposes, a necessarily small group mainly within the DPS).

Developing intelligence

The DPS allocates lower-level corruption-related intelligence to local professional standards units to conduct enquiries. The DPS and the local professional standards units have no standardised method of recording or managing this intelligence. This creates a risk that the necessary actions aren't completed.

When sensitive intelligence is received, it is allocated for further development to those who have access to a wide range of covert tactics. Once developed, and if further investigation is needed, the case is allocated to the anti-corruption command (ACC).

Because relevant information is often held by several departments, without [people intelligence meetings](#), corruption risks can easily be missed. The purpose of these meetings is to exchange information on those officers and staff who are of concern. We found that the MPS does not hold such meetings.

The MPS counter-corruption strategic threat assessment lacks analysis

All forces should produce an annual strategic counter-corruption threat assessment. The MPS assessment contains an overview of the volume of corruption-related intelligence received by the DPS. We saw little evidence of any in-depth analysis of this information to identify the current threats. There was no information about: the locations of corruptors or corrupt activity; potentially corrupt officers or staff; potential corruptors; or where types of corrupt behaviour may be more prevalent.

The MPS counter-corruption control strategy and its implementation are poor

We found an abundance of control measures but a lack of meaningful detail on how they will be achieved. There was a clear lack of governance and direction. The MPS does not have a 'delivery plan' or any clear or apparent strategic lead overseeing it. The overall approach is ad hoc with no named individual with responsibility for the identified priorities in the threat assessment, or a method to track progress against the control measures.

We found a lack of awareness and knowledge of the strategic threat assessment and control strategy, even within the DPS. This means there are insufficient levels of understanding within the workforce of the threats the force faces and the pivotal role they can play in countering corruption.

More encouragingly, we learned that the MPS had established a counter-corruption board, the first meeting of which was due to take place in December 2021 (after our fieldwork had ended).

Capacity and capability to investigate corruption

We found a high level of capability within the anti-corruption command. We were told that all officers and staff have the skills, training and expertise to undertake complex counter-corruption investigations. The command also uses cutting-edge technology, seldom seen elsewhere.

The specialist investigations unit's (SIU's) role is to overtly investigate: incidents that involve death or serious injury to members of the public, following direct or indirect contact with the police; public complaints assessed as potential gross misconduct; allegations of serious corruption; and other matters of high risk to the MPS.

At the time of this inspection, the SIU establishment was 128 posts. But, only 95 were occupied, with most vacancies being at the detective constable level. Senior officers in the SIU told us that investigators become "overwhelmed", and that "the existing establishment is insufficient to deal with the workload".

The integrity assurance unit (IAU) is responsible for managing individuals in the MPS who have been identified as posing a high corruption risk. But the IAU's capacity is also insufficient. Consequently, officers and staff representing a high risk are only reviewed on an annual basis, or because the IAU has received intelligence about the individual. This approach creates a significant risk to the force.

In many cases, local professional standards units did not have the capacity to undertake all the work they were allocated and had huge backlogs. Officers told us that, in one BCU, this led to delays of up to a year before the unit could appoint an investigating officer, let alone complete the investigation.

Local professional standards units mainly consist of uniformed officers. As a result, they have limited capability to undertake anything other than straightforward low-level complaint and misconduct investigations. We were told that none of the units had any proactive capability or capacity. Officers and staff told us they had insufficient resources and skills to undertake proactive counter-corruption work.

The future

A transformation project started in July 2021, focused on making improvements in the DPS. The project's aim is to improve public confidence and satisfaction and reduce demand. It is due for completion at the end of 2022. At the time of our inspection, it was too early to comment on its progress.

We are encouraged that the MPS is reviewing the DPS and the local professional standards units.

The institutional corruption label

The Panel concluded that the MPS is "institutionally corrupt". In essence, the Panel defined this type of corruption as one where an organisation protects its reputation, rather than where any individual benefits from a corrupt act.

We concluded that the adverse matters we described in our report bore the hallmarks of limited resources allocated to the maintenance of professional standards, professional incompetence, a lack of understanding of important concepts, poor management or genuine error, rather than dishonesty (other than in the conduct of some individual officers in the context of specific investigations into Mr Morgan's murder). Importantly, we found no evidence of any deliberate or co-ordinated campaign to intentionally frustrate the Panel's work. It follows that we would not describe the MPS as institutionally corrupt based upon the evidence we have seen.

This should not for a moment be understood to be a finding that there are not serious areas of concern which have been, and continue to be, present in the MPS. It is essential that the MPS should be more open to criticism and prepared to change where necessary, including by implementing our recommendations. A further failure to do so (without good reason) may well justify the label of institutional corruption in due course.

Causes of concern

The causes of concern listed below are in addition to other relevant causes of concern raised in previous inspections and referred to in this report.

Cause of concern 1

The MPS's arrangements for managing exhibits and other property are a cause of concern.

Cause of concern 2

The MPS's lack of any concerted effort to establish relationships between the directorate of professional standards and organisations supporting vulnerable people is a cause of concern.

Cause of concern 3

The MPS's lack of proactive work to gather counter-corruption intelligence is a cause of concern.

Cause of concern 4

The MPS's lack of monitoring and oversight of declarable associations, business interests and gifts and hospitality is a cause of concern.

Cause of concern 5

The current professional standards operating model within the MPS is a cause of concern.

Recommendations

Recommendation 1

By 31 March 2023, the MPS should establish clear processes and responsibilities for responding to the findings in this report and ensure that its leadership practices and management structures exert sufficient control over the response.

Recommendation 2

By 31 March 2023, the MPS should:

- make adequate provision for the effective storage of property and exhibits, including the provision of sufficient capacity and robust security (including for firearms and other high-risk items);
- develop an effective process for the handover of property between BCUs/OCUs and the LDSS, including property that has been rejected before being accepted into the property stores;
- improve its record keeping in relation to stored property; and
- ensure it has sufficient supervisory oversight of the property process.

Recommendation 3

By 31 March 2023, the MPS should establish and begin operation of a process to:

- determine the vetting status of all personnel in designated posts; and as soon as possible thereafter;
- ensure that all designated postholders are vetted to the enhanced (management vetting) level; and
- provide continued assurance that designated postholders always have the requisite vetting level.

Recommendation 4

By 31 March 2023, the MPS should:

- ensure that all police officers and staff are made aware of the requirement to report any changes to their personal circumstances; and
- establish a process whereby all parts of the organisation that need to know about reported changes, particularly the force vetting unit, are always made aware of them.

Recommendation 5

By 31 March 2023, the College of Policing should amend the Counter-Corruption (Prevention) Authorised Professional Practice to make clear that gifts of cash should never be accepted.

Recommendation 6

By 31 March 2023, the MPS should review and update its gifts and hospitality policy and associated processes to:

- make clear that gifts of cash to individual officers and staff are unacceptable;
- ensure the registers to record gifts and hospitality are accessible, used and maintained;
- ensure that officers and staff are made aware of the policy and their individual responsibilities; and
- ensure that appropriate oversight is maintained of the process and registers, including dip sampling.

Recommendation 7

By 31 March 2023, the MPS should strengthen its business interests monitoring procedures to ensure that:

- records of business interests are managed in accordance with the business interests policy;
- records are easily accessible to enable reviews to be carried out effectively;
- all personnel are made aware of the policy and their individual responsibilities;
- the force actively monitors personnel compliance with decisions to refuse, or conditions attached to the approval of, business interests; and
- appropriate oversight is maintained of the process and records, including dip sampling.

Recommendation 8

By 31 March 2023, the MPS should ensure that the risk assessment process in respect of declarable associations:

- is always carried out by suitably trained assessors who have access to all relevant information and intelligence; and
- includes an element of objectivity by, for example, the use of a numerical risk matrix.

Recommendation 9

By 31 March 2023, the MPS should revise its declarable association policy and associated procedures to:

- place firm obligations on all personnel to disclose to the DPS any relationships with journalists, and any relationships with extremist groups;
- remove outdated references in the policy to the National Policing Improvement Agency and professional standards champions;
- ensure the records are accessible, used and maintained;
- ensure personnel are made aware of the policy and their individual responsibilities;
- maintain effective oversight of the process and registers, including the use of dip sampling (or other similar measures) for assurance purposes; and
- in future, keep the policy up to date.

Recommendation 10

By 31 March 2023, the MPS should establish and begin operation of a process to ensure that all supervisors are properly briefed on the business interests and declarable associations of all those whom they are expected to supervise.

Recommendation 11

By 31 March 2023, the MPS should take steps to ensure that:

- the integrity assurance unit (or another unit or units) is sufficiently resourced for the effective monitoring and reviewing of all MPS personnel assessed as presenting a high risk of corruption; and
- any counter corruption-related conditions the MPS places on personnel so assessed are effective in mitigating the risks those personnel present.

Recommendation 12

By 31 March 2023, the MPS should:

- convene, and hold on a regular and continuing basis, people intelligence meetings; or
- establish and begin operation of an alternative process to facilitate the presentation and exchange of corruption-related intelligence, to identify officers and staff who may present a corruption risk.

Recommendation 13

By 31 March 2023, the MPS should ensure that it has full IT monitoring capability, to effectively protect the information contained within its systems and help it to identify potentially corrupt officers and staff.

Recommendation 14

By 31 March 2023, the MPS should establish and begin operation of an improved system of digital device management, with accurate record keeping concerning:

- for each digital device, the identity of the officer or staff member to whom the device is allocated; and
- the uses to which each device is put.

Recommendation 15

By 31 March 2023, the MPS should update its policy on the use of mobile devices to include clear explanations of:

- the expectation that force-issued devices are for official police use only; and
- what the force considers to be acceptable and unacceptable use of force-issued devices.

Recommendation 16

By 31 March 2023, the directorate of professional standards should establish relationships with external bodies that support vulnerable people. This is to:

- encourage the disclosure by such bodies, to the DPS, of corruption-related intelligence regarding the sexual abuse of vulnerable people by police officers and staff;
- help these bodies' personnel to understand the warning signs to look for; and
- ensure they are made aware of how such information should be disclosed to the directorate of professional standards.

Recommendation 17

By 31 March 2023, the MPS should ensure all its corruption-related intelligence is categorised in accordance with the NPCC counter-corruption categories (and any revised version thereof).

Recommendation 18

By 31 March 2023, the MPS should develop an effective and auditable process to ensure that all corruption-related intelligence the directorate of professional standards allocates to other units is handled effectively.

Recommendation 19

By 31 March 2023, the MPS should revise its counter-corruption strategic threat assessment and control strategy, to include:

- analysis and an evidence base to support the reasons why particular forms of corruption are identified as current threats;
- a clear intelligence requirement;
- a plan in which named individuals are allocated responsibility for the actions set out in the control strategy, and held to account for carrying them out; and
- a communication process to increase the workforce's understanding of the threats the force faces.

Recommendation 20

By 31 March 2023, the NPCC, in consultation with the College of Policing, should amend its definition of police corruption and amend its national corruption categories. This is to ensure that:

- both become more useful to those recording, categorising and analysing corrupt behaviour; and
- the concept of institutional corruption is included in the definition and the categories.

Areas for improvement

The areas for improvement listed below are in addition to other relevant areas for improvement raised in previous inspections and referred to in this report.

Area for improvement 1

The MPS should provide a more consistent approach to counter-corruption training on local professional development days.

Area for improvement 2

The MPS should ensure that its annual professional development review checklist is completed for all officers and staff.

3. Introduction

Background

On 10 March 1987, Daniel Morgan, a 37-year-old private investigator, was murdered in a car park behind the Golden Lion public house in Sydenham, London. He had been struck on the head with an axe.

There have been several investigations and reviews into Mr Morgan's death, none of which have led to a conviction for his murder. From an early stage, there were concerns that police corruption played a part in the murder, the failure to bring his killer to justice, or both.

In 2013, the then Home Secretary, the Rt Hon Theresa May MP, set up the [Daniel Morgan Independent Panel](#) ('the DMIP' or 'the Panel').⁴ The Panel was asked:

"to shine a light on the circumstances of Daniel Morgan's murder, its background and the handling of the case over the whole period since March 1987. In doing so, the Panel will seek to address the questions arising, including those relating to:

- police involvement in the murder;
- the role played by police corruption in protecting those responsible for the murder from being brought to justice and the failure to confront that corruption; and
- the incidence of connections between private investigators, police officers and journalists at the News of the World and other parts of the media and alleged corruption involved in the linkages between them."⁵

Over the next eight years, they reviewed all the information and evidence associated with this case, including the subsequent reviews and investigations. They also interviewed witnesses.

On 15 June 2021, the Home Secretary published the DMIP's 1,251-page report. It contained excoriating criticism of the Metropolitan Police Service (MPS). The Panel's criticisms included:

- significant failings when investigating the murder;
- the involvement of corrupt officers;
- very poor treatment of Daniel Morgan's family; and

⁴ References in this report to the DMIP include panel members, its staff, and representatives.

⁵ [The Report of the Daniel Morgan Independent Panel](#), 15 June 2021, vol 1, p 3, para 4.

- obstructing the DMIP inquiry (particularly in relation to allowing the Panel access to MPS material).

The Panel concluded that some aspects of the MPS's approach amounted to "institutional corruption".

On the day of the report's publication, the Home Secretary asked us to consider how we could best focus on the matters the Panel raised, to ensure that the public would have confidence that the MPS was addressing them adequately.

About us

Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) independently assesses the effectiveness and efficiency of police forces and fire & rescue services, in the public interest. In preparing our reports, we ask the questions that the public would ask, and publish the answers in accessible form. We use our expertise to interpret the evidence and make recommendations for improvement.

Our commission

Following further discussion, on 16 July 2021, using her powers under section 54(2B) of the Police Act 1996, the Home Secretary commissioned us to inspect the MPS.

Terms of reference

Our terms of reference were to address the following questions.

1. How effective was the MPS's organisational learning response to the Daniel Morgan independent investigations and reviews?
2. How appropriately did the MPS respond to the Independent Panel's requests for disclosure and access to material?
3. How well does the MPS prevent, manage, understand, and investigate potential corruption?

Methodology

Our inspection took place between September and November 2021.

During our inspection we:

- examined matters raised in the DMIP report;
- scrutinised over 600 force documents, which included policies, procedures, and other material the MPS provided;
- reviewed the force's response to 175 items of counter-corruption intelligence;
- evaluated a sample of 40 vetting files;
- reviewed MPS data⁶ relating to vetting and counter-corruption;

⁶ The data included: the number of reports to confidential telephone lines provided for MPS personnel to report any concerns as to the integrity of officers and staff; the number of personnel assessed as being at high, medium and low risk of corruption; the number of vetted personnel; and the number of corruption-related intelligence reports received.

- conducted interviews and focus groups with MPS officers and staff;
- undertook reality testing⁷ across the force area by speaking with individual officers and staff;
- interviewed DMIP members and their supporting staff; and
- reviewed the MPS's progress against recommendations we made, and areas for improvement we identified, in our previous inspections.

This report's relationship with another inspection report

While this inspection was underway, the Home Secretary commissioned us to carry out a separate thematic inspection of police forces in England and Wales. This followed the murder of Sarah Everard by a serving MPS officer. That thematic inspection explores the police's counter-corruption arrangements, including vetting arrangements. It is being carried out in eight police forces, including the MPS. It will examine a wider range of related matters. The findings from the separate thematic inspection are scheduled for publication in 2022.

Contextual explanations

For ease of understanding, we have provided contextual explanations of:

- the content and purpose of the counter-corruption related professional guidance available to the police (part of the '[authorised professional practice](#)' (APP), provided by the [College of Policing](#));
- the potential for corruption to diminish public safety and confidence in policing;
- the structure and counter-corruption role of the MPS's directorate of professional standards (DPS); and
- the structure and counter-corruption role of the MPS's 49 local professional standards units, with which the DPS works.

College of Policing Authorised Professional Practice (APP)

The APP contains four sections that provide guidance to forces on how to protect themselves against police corruption:

- Counter-Corruption (Prevention);
- Counter-Corruption (Intelligence);
- Counter-Corruption (Enforcement); and
- [Vetting](#), the standards for which are set out in the statutory [Vetting Code of Practice](#).

To determine the likelihood of any of the MPS's failings described in the DMIP report being repeated, we examined the force's counter-corruption arrangements against the above APP. Because of the sensitive nature of some aspects of counter-corruption work, only the Vetting APP is published. Consequently, the chapter of our report that deals with vetting contains extensive and detailed references to the Vetting APP.

⁷ Reality testing involves unannounced visits to police premises to speak with officers and staff while engaged in their daily work.

The subsequent chapters, which deal principally with corruption-related intelligence and investigation, contain fewer and less-detailed references to the other three sections of APP.

The potential for corruption to diminish public safety and confidence in policing

Most police officers and staff are committed and professional, but there is a minority whose corrupt actions diminish public safety and confidence in policing.⁸ The thorough vetting of new recruits and, from time to time, the re-vetting of serving personnel, is an important line of defence. But, even if these are done perfectly, they cannot ever be a guarantee against corruption.

The APP states that the risks to operational security and organisational integrity increase significantly when police officers and staff experience personal difficulties. Such difficulties may include financial hardship and problems at work or at home, which can affect their judgment and make them more susceptible to corruption.⁹

There are significant corruption threats to forces if inappropriate relationships are not identified when officers and staff either enter policing or if they develop such relationships during their service. Personnel can become susceptible to the influence of numerous potential corruptors. These can come from a range of people such as criminals, family members and other people with an interest in accessing police information, such as private investigators and journalists. Officers and staff may act corruptly for various reasons, such as financial gain, misplaced loyalty, or because they have been blackmailed.¹⁰

The directorate of professional standards

The directorate of professional standards (DPS) is responsible for upholding the standards of professional behaviour of MPS officers and staff. This includes responsibility for tackling corruption and implementing the relevant APP.

The DPS is led by a chief officer of commander rank, supported by a detective chief superintendent, a senior police staff member, and several officers and police staff members at, or equivalent to, the rank of superintendent. The DPS comprises the following teams:

- anti-corruption command;
- intelligence bureau;
- specialist investigation unit;
- prevention and learning team; and
- misconduct hearing and litigation team.

⁸ *APP Professional Standards: Counter-Corruption (Prevention)*, College of Policing, 28 July 2015, p 5.

⁹ As before, p 27.

¹⁰ As before, p 27.

Local professional standards units

Within each [basic command unit](#) (BCU) and operational command unit (OCU),¹¹ there is a local professional standards unit. In total, there are 49 local professional standards units throughout the force. They operate under the direction of the relevant BCU/OCU commander. The local professional standards units are responsible for investigations into complaints and lower-level misconduct. They are not part of the DPS. They are resourced and managed by officers and staff from the BCU or OCU.

During our inspection, we visited all teams within the DPS, except for the misconduct hearing and litigation unit. We also visited eight local professional standards units.

¹¹ Specialist departments within the MPS, i.e. territorial support group, directorate of professional standards, roads and transport policing command.

4. Investigations and reviews concerning Daniel Morgan’s murder

Our role wasn’t to reinvestigate the murder; it was to consider opportunities for [organisational learning](#) from all the Daniel Morgan investigations and reviews and assess how the MPS responded to them. We acknowledge that there have been ancillary investigations over the years, such as into potential misconduct. This chapter of our report summarises those investigations and reviews. In the subsequent two chapters, we consider the opportunities for organisational learning they presented and whether the force has fully understood them and made changes as a result.

Regardless of their quality, the MPS has invested heavily in the investigations and reviews. The DMIP remarked that a reinvestigation that ran from 2001 to 2003 was “one of the most expensive and resource intensive re-investigations that the MPS has conducted”.¹²

It is deeply regrettable that so much time and expense has not resulted in those responsible for Daniel Morgan’s murder being brought to justice. There are several reasons for this. They include the poor – and, in some instances, corrupt – practices that the DMIP covered comprehensively in its report.

We found that there was some disagreement between the DMIP and the MPS about whether individual procedures were to be termed investigations or reviews.¹³ We have designated each as we felt most appropriate.

For the purposes of our inspection, we considered the following investigations and reviews.

The first investigation (1987 to 1988)

The MPS started its first investigation on 10 March 1987, immediately after Daniel Morgan’s murder. The DMIP referred to this investigation as ‘The Morgan One Investigation’. On 3 April 1987, six men, including three who were then serving police officers, were arrested in connection with the murder. The arrests didn’t lead to any charges.

¹² [The Report of the Daniel Morgan Independent Panel](#), 15 June 2021, vol 1, p 7, para 27.

¹³ As before, vol 1, p 4, para 6.

The DMIP found that, from the outset, “there were multiple very serious failings in the conduct of this investigation”.¹⁴ We agree that the management of the investigation was very poor. More specifically, the handling of the crime scene was “totally inadequate”,¹⁵ the process for managing exhibits was very poor, lines of enquiry weren’t pursued (including checking alibis) and searches for evidence were insufficient. And there was strong suspicion that at least some of those who were to be arrested were alerted beforehand through the improper disclosure of information (a ‘tip off’). Collectively, the MPS’s failings meant that, from the outset, it lost opportunities to gather evidence.

Despite the clear and obvious inadequacies during the first investigation, an MPS review of it, led by a detective chief superintendent, apparently found no fault. The review report has not been found. The DMIP concluded that it had taken place between October and December 1987, when the first investigation was still underway.

However, in a report relating to a 1988 investigation into a complaint made by Daniel Morgan’s business partner, a detective chief superintendent identified problems concerning property and exhibits. He summarised his findings as:

- a) “failure to account for all property coming into police possession in the property register or other recognised property documents
- b) failure to safeguard such property
- c) failure to ensure proper, unambiguous receipts for property
- d) altering property receipts by adding additional items after the recipient had signed for the property
- e) failing to restore property expeditiously as decreed in the Police and Criminal Evidence Act [1984].”

It is unclear whether the MPS took any action against the exhibits officer responsible. It appears that his poor performance was attributed to his lack of experience and poor supervision.

The inquest (1988)

On 13 March 1987, the Coroner for the Inner London South district opened the inquest. As is common practice, he then adjourned it pending the outcome of the continuing criminal investigation. Following subsequent Crown Prosecution Service (CPS) advice that there was insufficient evidence to charge any of those who had then been arrested in connection with the murder, the coroner decided to start the hearing at Southwark Coroner’s Court on 11 April 1988. It concluded two weeks later, on 25 April 1988, when the jury returned a verdict of unlawful killing.

The DMIP reported on the inquest in detail. We noted that, despite the inadequacies of the police investigation, the coroner commented on its thoroughness and the fact that a detective chief superintendent had found no fault with it when he reviewed it between October and December 1987.

¹⁴ As before, vol 1, p 4, para 8.

¹⁵ As before, vol 1, p 4, para 9.

The Hampshire Constabulary investigations (1988 to 1989)

Following the inquest, Daniel Morgan's family continued to raise concerns, which they had expressed from an early stage, about the conduct of the investigation. The family was especially concerned about potential police involvement in the murder. The MPS referred the family's complaints to the Police Complaints Authority (PCA).¹⁶ The PCA asked Hampshire Constabulary to investigate, under the PCA's supervision. A Hampshire Constabulary detective chief superintendent was appointed senior investigating officer (SIO). A memorandum dated 24 June 1988 provided vague terms of reference, instructing the SIO to "investigate allegations that police were involved in the murder of Daniel Morgan and any matters arising therefrom".

Although there is no evidence that the terms of reference were formally changed, the SIO decided that he should reinvestigate the murder. This reinvestigation is known as Operation Drake. In January 1989, it led to the arrest of three people: two men, who were subsequently charged with Daniel Morgan's murder, and a woman, who was charged with perverting the course of justice.

But the evidence was weak. When the three suspects appeared before Fareham Magistrates' Court on 11 May 1989, the charges were dropped.

Following this, the PCA and Hampshire Constabulary agreed to start a second investigation, more akin to the original terms of reference (that is, potential police involvement in the murder). This further investigation is known as Operation Plymouth. The SIO remained the same.

On 4 September 1989, the SIO submitted his final report to the PCA. He concluded that there was no evidence to implicate any individual officer, or the police in general, in the murder. He further concluded that there was no evidence that any member of the investigation team wilfully prevented the murder from being solved. He also made very little criticism of the initial MPS investigation.

MPS Complaints Investigation Bureau (CIB) case review (1996)

In August 1996, a team from the MPS Complaints Investigation Bureau (CIB) conducted a routine review of the case. It also considered allegations that a former police officer might have been involved in the murder. The team did not identify any new lines of enquiry.

Covert operations (1997 to 1999)

In the early 1990s, the MPS commissioner who was then in office decided to introduce a covert team to tackle police corruption. It was initially called Complaints Investigation Bureau 3 (CIB3), but later became the Internal Investigations Command. It is now known as the DPS anti-corruption command. The team used – and still uses – a variety of covert and sensitive police tactics to target suspects and gather evidence. During the 1990s, it ran a series of operations which, directly or indirectly, related to Daniel Morgan's murder.

¹⁶ In 2004, the PCA was replaced by the Independent Police Complaints Commission (IPCC) which, in 2018, was itself replaced by the Independent Office for Police Conduct (IOPC).

The series of covert operations started after a wide-ranging anti-corruption investigation (Operation Gallery), which ran from 1993 to 1996, indicated that a former police detective (then retired) and one of Daniel Morgan's close associates were involved in crime. This led to four further operations, which started in 1997. The first two (Operations Landmark and Hallmark) essentially involved surveillance, in preparation for the main operations that followed (Operations Nigeria and Two Bridges). Ultimately, the operations aimed to gather intelligence and evidence not only about the Daniel Morgan murder but also about police corruption more generally and its links to organised crime.

The MPS brought the series of operations to a premature conclusion when covert tactics identified an unforeseen offence of conspiring to pervert the course of justice that was about to take place. One of the suspects was a serving police officer. The MPS felt that it could not delay acting, although it exposed the covert operations and tactics.

In September 1999, the police arrested the serving officer and 11 other suspects. On 14 December 2000, the police officer and two of the other suspects were convicted of conspiring to pervert the course of justice. The police officer was sentenced to four years' imprisonment (which was increased to five following an appeal by the Attorney General), while his co-defendants were each sentenced to six years (increased to seven on appeal).

A cold case review (2000)

On 31 March 1999, the MPS issued Special Notice 6/99, which was a direction to the force about the investigation of murders and other serious crimes. It was an important milestone and we discuss it in more detail later in our report. Here, we are concerned with a process commonly referred to as 'cold case review'.

The special notice implemented Association of Chief Police Officers (ACPO) guidelines that had been introduced to the effect that unsolved murders should be reviewed at least every two years. When introducing the policy, the MPS acknowledged that it would be impractical to review every unsolved murder in the force area that was over two years old. The MPS therefore decided to apply the procedure to murders committed after 1 January 1997. However, the force would also consider older reviews if workload allowed.

The MPS clearly considered Daniel Morgan's case an exceptional one, as it then undertook a cold case review. The decision to do so would seem to have been supported by intelligence from the recent covert operations. The review started on 26 June 2000. A detective inspector from the murder review group (MRG) led it. He reported his findings on 6 October 2000.

The review made 83 recommendations; all were specific to the investigation. We do not criticise the review for that: its terms of reference were essentially to identify investigative opportunities rather than organisational learning. The DMIP concluded that the review was thorough, although it still missed some investigative opportunities. Importantly, though, the review recommended a further reinvestigation.

A covert and overt reinvestigation (2001 to 2003)

The MPS accepted the cold case review's recommendation to undertake a further reinvestigation. The MPS decided that it should comprise two elements: a detective chief inspector from CIB was to lead a covert operation (Operation Abelard One), while a detective chief superintendent from the MPS serious crime group (now the specialist crime command) was to take charge of a parallel overt operation (Operation Morgan Two). As it transpired, the covert operation started in April 2001 and the overt operation in May 2002.

These operations led to the arrest of eight people. On 7 March 2003, the MPS submitted a file to the CPS seeking decisions on charging three men with Daniel Morgan's murder, and charges against others for offences that included conspiracy to pervert the course of justice. The CPS was also asked to consider charging a former police officer with misconduct in a public office. The matters were referred to counsel. On 2 September 2003, the CPS wrote to the MPS saying that they agreed with advice received from counsel that there was insufficient evidence to proceed in respect of all matters.

Report to the Metropolitan Police Authority (2006)

On 27 October 2005, the Metropolitan Police Authority decided to commission a report on the case from the MPS under section 22(3) of the Police Act 1996. The report was to cover the murder and subsequent investigations. Of relevance here was a requirement to include in the report lessons the MPS had learned from the case.

On 31 January 2006, the MPS submitted its first version of the report to the Authority. The Authority duly rejected that version. Although the reason for the rejection is unclear, it would seem that the Authority considered the report inadequate. The MPS provided a revised version in April 2006.

The DMIP report includes a quote from the report to the Authority, in which the MPS accepted that its response to the murder had been flawed. However, the MPS was determined to learn from its mistakes:

"The Metropolitan Police Service is acutely aware of the damage caused to its reputation and the subsequent stress borne by the family as a result of this flawed investigation. The organisation is determined to do everything within its capability to put this right and ensure that any learning from this or other cases is captured and disseminated as widely as possible."¹⁷

In accordance with its terms of reference, the MPS report contained lessons learned and changes made in light of the Daniel Morgan case and other investigations, particularly that relating to the murder of Stephen Lawrence. In the report, a deputy assistant commissioner (DAC) listed the changes as follows:

- "The development of a comprehensive Murder Review Process
- The development and introduction of Decision Logs and Policy Files

¹⁷ [The Report of the Daniel Morgan Independent Panel](#), 15 June 2021, vol 2, p 641, para 149 (quoting from report to the Metropolitan Police Authority by DAC John Yates, 7 April 2006).

- The first actions at the scene of a serious crime
- The identification and management of critical incidents
- The detailed forensic examination of major crime scenes, use of cordons and taking into account modern forensic investigative capabilities
- The introduction of a proactive and highly skilled Anti-Corruption Command
- The development and introduction of an Anti-Corruption Strategy
- Approach towards the family of murder victims such as close liaison and informing them of events
- The development and introduction of Homicide Commands, dedicated teams who have an expertise in investigations of this nature
- The training of Senior Investigators through the national SIO [Senior Investigating Officer] development and accreditation programme
- The training of all investigators through the Professionalising the Investigative Process Programme
- The development and introduction of the Independent Advisory Groups and their involvement in Gold Groups pertinent to this form of enquiry.”

The DMIP was sceptical about the number of changes that had occurred specifically because of the investigations into Daniel Morgan’s murder. It noted that some practices were already in place before 1987, while other changes had occurred because of developments in national policy because of other investigations. The DMIP concluded that the MPS had exaggerated the amount of change that had been introduced because of lessons learned from Daniel Morgan’s case.

A further reinvestigation (2006 to 2011)

In March 2006, the MPS started a further reinvestigation of Daniel Morgan’s murder. It ran until March 2011 and is referred to as Operation Abelard Two.

An offender comes forward with information

The catalyst for the reinvestigation was an approach, in late 2004, from a criminal who wanted to speak about the murder. He had been charged with serious criminal offences and had been remanded in custody.

In February 2005, after consulting the CPS, MPS officers interviewed him. Records indicate that, at that stage, he was only prepared to provide information – presumably in return for a reduced sentence – but not to give evidence in court. The police brought his assistance to the attention of the judge when passing sentence. He was still sentenced to a substantial term of imprisonment.

The Serious Organised Crime and Police Act 2005 (SOCPA)

The criminal supplying the information was not dealt with as an ‘assisting offender’ under the [Serious Organised Crime and Police Act 2005 \(SOCPA\)](#), which came into effect in April 2006.

Under the SOCPA, the assistance provided by an offender may involve giving evidence in court (commonly known as 'Queen's evidence'), or providing information, or both.

The offender makes further contact

In January 2006, the offender who had first approached the police in 2004 made further contact. He wanted to speak again about Daniel Morgan's murder. Detectives met with him and he eventually agreed to take part in a debriefing process, as an assisting offender, under the SOCPA.

Following a lengthy and complex authorisation process, detectives debriefed the offender. The interviews were tape recorded. At their conclusion, he signed a 32-page witness statement.

Reinvestigation and charges

The MPS started a reinvestigation in March 2006. The reinvestigation involved re-visiting old lines of enquiry and pursuing new ones as they emerged. Detectives used both overt and covert tactics. They also debriefed other offenders who were prepared to assist the reinvestigation. Eventually, on 23 April 2008, the MPS charged four men with Daniel Morgan's murder. They also charged a former police officer with perverting the course of justice.

On 24 April 2008, the case was transferred from the magistrates' court to the Central Criminal Court. After a series of postponements, a trial date was eventually set for January 2011.

The case collapses

The case never got to trial. The judge heard a series of legal arguments between October 2009 and March 2011, in what is generally regarded to be the longest pre-trial hearing in English legal history. During 2010, the CPS offered no evidence against one man who had been charged with murder and the former police officer who had been charged with perverting the course of justice. They were acquitted. And on 11 March 2011, the three remaining defendants also walked free when the CPS similarly offered no evidence against them.

The prosecution case had relied heavily on three assisting offenders who had provided evidence under SOCPA agreements. During the legal arguments, all three were found to be unreliable. The court also heard that the police had breached the SOCPA guidelines on debriefing. But SOCPA wasn't the prosecution's only problem. Just as significant – if not more so – were disclosure failures.

The prosecution didn't meet its legal obligations under the Criminal Procedure and Investigations Act 1996 (CPIA). The CPIA requires the prosecution to disclose all material that might reasonably be considered capable of undermining the prosecution case or of assisting the accused. With material gathered over 24 years, then estimated to be in the region of 750,000 pages, this was always going to be a formidable task. Nevertheless, the judge found that the MPS had demonstrated a lack of due diligence in this regard.

In March 2011, the police conceded that they could not be sure that they had accounted for all relevant material. This and the loss of the assisting offenders' evidence meant the prosecution was untenable.

The CPS and MPS joint review (2011 to 2012)

Following the collapse of the Operation Abelard Two trial in March 2011, the CPS and MPS undertook a joint review, which focused primarily on the SOCPA and disclosure failures that had arisen. The Chief Crown Prosecutor for London and a MPS assistant commissioner agreed the terms of reference for the review:

- “Examine the methodology, decisions and tactics used by the prosecution team (police and prosecutors) to deal with the witnesses who were given agreements pursuant to the SOCPA legislation.
- Examine the methodology, decisions and tactics adopted by the prosecution team (police and prosecutors) in order to discharge their disclosure obligations, (to include any omissions).
- Consider any other significant key areas which may emerge during the course of the review.
- To make recommendations in relation to any lessons learnt or good practice which emerge from the review.”

The review team produced its findings in May 2012. It concluded that while there were issues regarding the unreliability of witnesses, the main reason for withdrawing the prosecution's case was disclosure.

Other investigations (2011 to 2021)

We briefly consider here other investigations that took place between 2011 and 2021. They are covered comprehensively in the DMIP report and primarily relate to the activities of the detective chief superintendent who was in charge of Operation Abelard Two. In essence, it was alleged that the officer had improperly supplied vast quantities of information to a journalist. When the officer's home was searched in 2012 and 2014, huge amounts of material belonging to the police and other criminal justice agencies were recovered.

The MPS and the IPCC (now IOPC) investigated these matters and referred their findings to the CPS. He was never prosecuted.

The DMIP was concerned that the police and the IPCC never properly investigated these matters. The Panel concluded that this was, in part, due to a desire to protect the police's reputation.

The same officer was also investigated regarding his conduct during Operation Abelard Two. It was alleged that he had attempted to pervert the course of justice by prompting an assisting offender to provide evidence against the murder suspects. Again, the investigation did not result in any charges.

The Report of the Daniel Morgan Independent Panel

The Home Secretary announced the establishment of the Panel in a written statement to the House of Commons on 10 May 2013. The Panel started its work in September 2013. It published its findings in June 2021. The Panel's report included 23 recommendations.

5. The MPS's approach to organisational learning

Before we examine specific organisational learning opportunities arising from the Daniel Morgan investigations and reviews, we assess the MPS's appetite for learning.

Slow to learn

On 13 March 2020, we published our [findings from an inspection of the MPS's response](#) to *The Independent Review of the Metropolitan Police Service's handling of non-recent sexual offence investigations alleged against persons of public prominence (the Henriques report)*. We found:

“an underwhelming approach to learning the lessons from the Henriques report during 2017, 2018 and most of 2019. There were many straightforward things the MPS could and should have done, such as updating training, policy and guidance documents.”

We found a similar story during this inspection. Lessons that should have been learned over the years had been disregarded and mistakes repeated. The DMIP concluded that failure to learn from past mistakes and failures is a feature of institutional corruption.

Just as we discovered during our 2020 inspection of the MPS's response to the Henriques report, we found during this inspection that the MPS is now taking organisational learning more seriously. But it is 'work in progress'. Senior officers acknowledge that there is more to do, through their development of a 'corporate organisational learning framework', and the implementation of a systemic approach to organisational learning in the MPS. We conclude that the publication of adverse reports has a galvanising effect on the MPS's appetite for learning.

In this report, we identify five causes of concern and two areas for improvement, and make 20 recommendations. Our first recommendation is overarching. It sets out our view of how the MPS should respond to our findings.

Recommendation 1

By 31 March 2023, the MPS should establish clear processes and responsibilities for responding to the findings in this report and ensure that its leadership practices and management structures exert sufficient control over the response.

A fragmented approach

We found the MPS's approach to organisational learning confusing. We were told that, during the last 12 months, its historical 'silo approach' had changed; we were less certain. We were unclear about how all organisational learning was collated, assessed, and acted on. Others within the force had the same reservations. We found an understanding of what should happen, but less conviction about what did happen. We were told that organisational learning lacks co-ordination and that the whole process is 'fragmented'. The MPS contends that its "programme to implement organisational learning is, for the first time in the MPS, directly aligned to the [MPS's strategic objective to '[I]earn from experience, from others, and constantly strive to improve'." Our future inspections will establish the extent to which the programme has proved effective.

The MPS informed us that, in April 2020, its 'corporate organisational learning' function was established within the continuous policing improvement command (CPIC), as the 'organisational learning and research' team. This team is responsible for the design and implementation of the MPS organisational learning framework, for co-ordination of organisational learning functions and for "thematic analysis of learning across functions".

The organisational learning and research team is distinct from the learning and development unit (LDU). The OL&R team is responsible for organisational learning (knowledge and memory) and the building of a network of 47 'organisational learning hubs' throughout the MPS. The hubs are intended to create a co-ordinated approach to organisational learning. The MPS informed us that some are already in place, with others in development, but that a "resourcing issue identified by [HMICFRS] remains the major barrier to implementing at speed".

There are also other groups within the framework. They include:

- the inquiry and review support command (IRSC);
- the prevention and learning team (P&L team);
- the specialist crime review group (SCRG); and
- the learning and development unit (LDU).

The IRSC

The IRSC was formed in 2015 as part of the MPS's response to high-profile inquiries, such as the national [Undercover Policing Inquiry \(UCPI\)](#), which was also established in 2015, and an [IPCC/IOPC investigation into allegations of corruption during the original Stephen Lawrence investigation](#), which started in 2014.

The IRSC manages the MPS's contribution to a small number of high-profile and/or complex inquests. But it is not responsible for organisational learning identified during all inquests; the DPS has an inquest team that manages the MPS's contribution to any inquests where the Commissioner is an interested party.

At the time of our inspection, the IRSC had a strength of almost 100 personnel and was responsible for the MPS's contribution to nine separate inquiries and inquests.

The P&L team

The P&L team is part of the DPS. The P&L team's role is to identify and disseminate learning from the DPS and IOPC investigations and also any learning from inquests, employment tribunals and civil actions. The MPS advised us that it is also responsible for carrying out "remedial action on identified learning".

The SCRG

For review purposes, the MPS has a dedicated team of experienced detectives. It is called the SCRG. The head of profession for investigations (commander rank) is responsible for the SCRG. Most of its work involves the review of murder investigations, but it also reviews other serious crime investigations, usually if requested to do so via its 'tasking' process. A homicide case closure panel is responsible for identifying organisational learning.

The LDU

The MPS informed us that the LDU is responsible for "individual learning (training and skills)", rather than organisational learning.

Governance

The professionalism AC chairs a quarterly organisational learning board. The MPS told us that this board "escalates to the executive people and learning board, and has several sub-governance structures such as the research faculty steering group (RFSG) and [organisational learning] high harm/risk group."

The same AC also chairs a monthly 'stocktake' meeting, which considers high-risk issues identified by gold groups.¹⁸ We understand that, at the time of our inspection, the MPS was running 100 gold groups. Identifying and recording the organisational learning from them all is a significant task, but the organisational learning board has introduced a process with that in mind.

The MPS informed us that a sergeant from the IRSC is responsible for reviewing the organisational learning from the stocktake meeting "in order to identify and highlight overlapping themes that might be addressed together. The [s]tocktake meeting is developing this [organisational learning] function." We were told that, before the introduction of this process, little had been identified or disseminated.

¹⁸ The generic command structure – nationally recognised, accepted and used by the police, other emergency services and partner organisations – is based on the gold, silver, bronze hierarchy of command. It can be applied to the resolution of both spontaneous incidents and planned operations. The MPS has supplemented the structure with a diamond level of command. The role of gold, silver or bronze commander should not be confused with the MPS's police rank of commander, although an officer of commander rank might perform one of those roles (typically gold commander). For more information see: [Operations: Command structures](#), College of Policing, 23 October 2013.

6. Lessons learned and lessons still to be learned

This chapter covers some of the more significant changes that have been made, or should have been made, during the years since Daniel Morgan's murder. Some featured in specific recommendations, while others would have been obvious to even the most casual observer.

In considering these matters, we recognise that it can be easy to criticise with the benefit of hindsight. This is even more so when there are 35 years to look back on, with all the profound changes that have happened in that time. In other words, we have tried to set our assessment in context. We have been mindful, for instance, that the Home Office Large Major Enquiry System (HOLMES) was only introduced in the 1980s, and that DNA profiling was still in its infancy. Indeed, the first conviction relying on DNA evidence was in January 1988, shortly after Daniel Morgan was murdered. Such advances in forensic science have greatly increased the police's understanding of how exhibits must be secured, preserved, stored and handled.

We also generally disregard missed investigative opportunities that were specific to a particular investigation; we are more concerned with organisational learning. But few of the reviews made recommendations that could be considered organisational learning. An exception was the CPS and MPS joint review from 2011 to 2012. And, of course, the DMIP has made several recommendations.

National standardised procedures

In 1981, following the 'Yorkshire Ripper' murders and other attacks on women in the north of England, Sir Lawrence Byford CBE QPM DL, then HM Chief Inspector of Constabulary, led an official inquiry into the flawed investigation. He produced his findings a little over six months later (the [Byford report](#)). It resulted in extensive changes in police investigative techniques, which forces adopted nationally. The changes included the introduction of Major Incident Room Standardised Administrative Procedures (MIRSAP).

The procedures were first introduced in 1982. They have been refined and developed over the years. The NPCC introduced the latest version of MIRSAP in November 2021 ([MIRSAP 2021](#)). It was the first major revision of the procedures since ACPO produced a revision in 2005.

From the outset, MIRSAP defined various roles in a major incident room and the way in which documents should be recorded and indexed. In 1982, police forces used a manual 'card index' system. The whole process became more efficient and effective from the mid-1980s, with the introduction of HOLMES.

The initial Daniel Morgan investigation did not have a HOLMES facility but relied on a far less efficient computer system, known as MICA. The first SIO told the DMIP that it was the first time he had used a computer system for a murder enquiry. Nevertheless, he should still have adhered to MIRSAP, which had already been in use for some years.

Special Notice 6/99

We did not find any great changes in the way the MPS dealt with serious crime during the 12 years after Daniel Morgan's murder. Then, on 31 March 1999, the MPS issued Special Notice 6/99, titled 'Major crime review'. It was a significant milestone in the force's approach to major crime investigations. It followed the publication of the [Stephen Lawrence Inquiry Report](#) a month earlier and the introduction of the first edition of the *ACPO Murder Investigation Manual* in August 1998.

The special notice, in conjunction with the much more detailed *Murder Investigation Manual*, provided comprehensive guidance on homicide investigation. Although it was issued over 20 years ago, the special notice was frequently referred to during our inspection as a document that introduced significant change. Failures during the Stephen Lawrence investigation had, to a large extent, led to the creation of the special notice, but many of those failures had also featured in Daniel Morgan's case.

The special notice covered a wide range of topics, including:

- crime scene management and record keeping;
- decision logs (formerly known as policy files), with a record of the SIO's decisions and rationale;
- family liaison;
- community concern assessments, to consider the impact on the community;
- management of intelligence;
- searches for evidence; and
- arresting and interviewing suspects.

The *Murder Investigation Manual*

The 1998 *Murder Investigation Manual* was a comprehensive document and was adopted by police forces nationally. Further editions were published in 2000 and 2006. Each edition included changes in legislation, technical and scientific developments, and national improvements generally. It served as national guidance until 2021, when it was withdrawn.

The [Major Crime Investigation Manual \(MCIM 2021\)](#) replaced the [ACPO 2006 Murder Investigation Manual](#). The NPCC Homicide Working Group introduced the new manual in November 2021, with the approval of the Chief Constables' Council. It covers all aspects of major crime investigation, including roles and responsibilities. It should be considered alongside other national guidance, such as [APP](#) and other NPCC guidance, including MIRSAP 2021.

It was not possible during this inspection to gauge how successfully the MPS has applied this current national guidance – and its own learning – to recent murder

investigations. We would need to conduct a separate homicide inspection to do so. That said, we recognise that the MPS solves the vast majority of the homicides it investigates.

The problems of resourcing murder investigations

The Panel rightly criticised the staffing levels and the capability and experience of personnel during the first investigation. The Panel was also concerned about Hampshire Constabulary's resourcing levels during its investigations, which started in 1988.

Assembling sufficient resources for a murder investigation during the 1980s and 1990s was a recurring problem, not just in the MPS but also in other forces throughout the country. Indeed, despite significant developments in major crime investigation over the years, we often find that a national shortage of detectives means it is still a problem.

In our [2018 annual assessment](#) of policing in England and Wales, we expressed concern about this shortage. More recently, in our [2019 report](#), we noted that it would take time for the effect of the police service's current recruitment programme to be felt in this area of policing.

Dedicated teams of suitably trained and experienced homicide detectives did not exist in the MPS in 1987. As in other forces at the time, SIOs often had to 'beg, steal or borrow' staff so that an investigation could even function at all. And even then, as the DMIP reported, the personnel who were made available might have been wholly unsuitable:

"Negotiation with local commanders was required for the secondment of police officers from various divisions and departments to a murder investigation. Such commanders were very often reluctant to lose staff for indeterminate periods. A Senior Investigating Officer had little or no control over who was attached to an enquiry, and staff often had little training for, and limited experience of, investigating murder."¹⁹

However, the MPS did have area major investigation pools (AMIPs), which were responsible for investigating serious crimes in their geographical areas. They provided personnel for a limited number of roles, but most of the investigation team had to be seconded from elsewhere.

The situation changed when Special Notice 6/99 took effect. The MPS increased staffing levels within the AMIPs to make them more self-sufficient. Staff deployed there were suitably trained and worked to an AMIP manual, reflecting the special notice's changes. The AMIPs were also to have their own intelligence capabilities.

AMIPs fell within the jurisdiction of the MPS's homicide and major crime command (SC01) and continued to do so until 2019.

¹⁹ [The Report of the Daniel Morgan Independent Panel](#), 15 June 2021, vol 1, p 60, para 168.

Specialist crime command

In June 2019, the MPS introduced its specialist crime command. It brought together three previously separate commands: SC01, the serious and organised crime command (SC07), and the Trident gang crime command (SC08). This consolidated approach is more flexible. This is because it provides a greater resource pool that can be called on for major enquiries, and which can better support the wider MPS and other law enforcement agencies.

The specialist crime command typically investigates homicides, gun and gang crime, drug supply offences, economic crime, cyber crime, kidnaps, child sexual exploitation, human trafficking, and modern slavery and prostitution.

Training

Crime training has changed considerably since 1987. In so doing, it has taken account of scientific and technological developments and the very many changes in legislation. Much of the training has been driven nationally, for example by the College of Policing and its predecessor organisations,²⁰ but a lot has still been at the discretion of individual forces.

An extensive examination of the MPS's crime training, and the quality of its courses, was beyond the remit of this inspection. But we wanted some assurance that all who might be involved in responding to the most serious crimes knew what they were doing, or where to turn for help. That included anyone whose role was to investigate the offence, as well as, for example, inexperienced patrol officers who may come across, or be sent to, a major crime scene. The MPS provides comprehensive investigative 'toolkits' to help officers at all levels, which can be accessed via the intranet. They include checklists for different stages of an investigation.

When we reviewed the MPS's response to the Henriques report in 2020, we found that officers and staff at various levels frequently criticised the force's training generally. Many interviewees thought there was an over-reliance on intranet circulations and NCALT (National Centre for Applied Learning Technologies) computer-based training. However, we accept that those methods have many benefits, and are particularly useful in disseminating information to a wide audience relatively quickly.

Since 2003, the national [Professionalising Investigation Programme \(PIP\)](#) has provided accreditation for those conducting investigations, at four levels of increasing complexity:

- PIP 1 – priority and volume crime investigations
- PIP 2 – serious and complex investigations
- PIP 3 – major crime and serious and organised crime investigations
- PIP 4 – strategic management of highly complex investigations.

²⁰ The [National Policing Improvement Agency](#) and the [Central Police Training and Development Authority](#).

The accreditation process involves registration, examination, training, and workplace assessment. Aspiring SIOs must complete all elements of the PIP level 3 [SIO development programme](#) before entry onto a professional register held by the College of Policing. Since 2017, the College has licensed the MPS to provide the SIO development programme.

In 2019, the specialist crime command introduced an induction course for all officers joining the department. It covers the fundamental aspects of major crime investigations but also provides the foundation for longer-term professional development. Specialist crime command provides its officers with homicide information packs. It has also distributed the packs to the wider force.

The MPS also provides a wide range of other investigation training courses. The areas they cover include:

- HOLMES;
- exhibits;
- general investigation;
- management of serious crime;
- family liaison;
- interviewing;
- intelligence;
- evidential reviews; and
- the use of investigatory powers.

Family liaison

The DMIP devotes a chapter of its report to the MPS's treatment of Daniel Morgan's bereaved family over the years. It was right to do so. In all but the most exceptional cases, the relationship between police and family is an important – and often crucial – element in a homicide investigation. Even in instances where one or more family members are responsible for a murder, there are usually other grieving relatives or people with a close connection to the victim. Indeed, the 2021 *Major Crime Investigation Manual* states that:

“[t]he term ‘family’ includes partners, parents, siblings, children, guardians and others who have had a direct and close relationship with the victim.”

The police approach to family liaison was very different in 1987. But, even if the MPS's treatment of the Morgan family was not unusual by the standards of the day, there were plenty of opportunities to change as the years went by. We appreciate that it can be difficult to establish a sound and constructive relationship when things start off badly, but the MPS should have made every effort to do so.

The DMIP found that “[b]eyond the initial contact with the family, there was little systematic liaison, unless the investigation required it, or there was significant information to pass on”.²¹

²¹ [The Report of the Daniel Morgan Independent Panel](#), 15 June 2021, vol 3, p 1,142, para 3.

The Panel concluded that “[t]he family’s grief has been compounded since the murder by their treatment at the hands of some police officers and representatives of other organisations”.²²

Force and national guidance

Despite the obvious importance of family liaison, it was not put on a formal footing until some years after Daniel Morgan’s murder. In 1987, the extent of police involvement with the family was very much at the discretion of the SIO. But there were fundamental changes in the late 1990s. The 1998 *Murder Investigation Manual* recognised the importance of family liaison officers, while the 1999 *Stephen Lawrence Inquiry Report* made six recommendations specifically about family liaison.

The Stephen Lawrence Inquiry reported: “One of the saddest and most deplorable aspects of the case concerns the failure of the family liaison”.

MPS Special Notice 6/99 recognised the significance of family liaison:

“The family liaison strategy is one of the most important considerations a SIO will have to address throughout the investigation.”

It offered limited guidance but said that the subject would be covered in full in an AMIP manual which was still being written. It also said that all AMIP officers were to be “given a familiarisation course in the role of family liaison”, while a “cadre of officers” had already received additional training.

The special notice also directed that family liaison officers must record all contact with a family or its nominated representatives in a family liaison log. It included some guidance on maintaining the log and said that the FLO must sign and date each page. However, SIOs were ultimately responsible for supervising all aspects of family liaison and were required to countersign and date each page. The MPS produced more comprehensive guidance (‘Family Liaison Policy Fundamental Guidelines’) in March 2001.

In 2003, ACPO provided further detailed guidance in the *ACPO (2003) Family Liaison Strategy Manual*, which was revised by the ACPO and National Policing Improvement Agency [Family Liaison Officer Guidance 2008](#). The 2008 guidance was used to develop further MPS policy, which the MPS produced in 2013.

The 2021 *Major Crime Investigation Manual* provides guidance on introducing and developing a family liaison strategy. The manual contains links to other documents where further information can be found, including APP. At the time of our inspection, the MPS was revising its own guidance to take account of national developments and to reflect its involvement with the [Grenfell Tower Inquiry](#).

²² As before, vol 3, p 1,143, para 4.

Considerable investment in family liaison

In 2016, the MPS reviewed its family liaison training, introducing greater involvement from experienced FLOs who had worked on a wider range of cases, including counter-terrorism investigations. And in 2018, the MPS introduced additional training for PIP level 3 SIOs. Current MPS training for those who are to be deployed as FLOs involves a five-day training course.

In February 2021, the force had 829 trained FLOs, and 132 [family liaison co-ordinators](#) to manage their deployment and provide support and guidance. During 2020, the MPS deployed FLOs on 312 occasions.

Based on the MPS's training commitment and the scale of its FLO deployments, we concluded that the MPS had put considerable investment into family liaison. This is encouraging.

Crime scene management

Since at least the 19th century, when fingerprints were first used to solve crimes, detectives have known that they must preserve a crime scene for careful examination and to prevent contamination – wilful or otherwise. This is even more important with an offence as serious as murder. Following Daniel Morgan's murder, the MPS should have secured the scene, thoroughly searched and examined it, and kept clear and accurate records of all who came and went. The MPS appears to have failed on all counts.

These inadequacies so early in the investigation, and others which were yet to arise – including those which related to the management of crime exhibits – would have created difficulties for any investigation that followed. They would also have allowed anyone with corrupt intent to flourish.

There were similar problems during the investigation into Stephen Lawrence's murder in 1993. The Stephen Lawrence Inquiry concluded:

“The scene of a murder may well be hectic and initially disorganised. But it is surely vital that more senior officers grapple with that disorganisation and attack the situation with energy and imagination. The senior officers of Inspector rank and upwards at this scene signally failed to act in this way. The lost opportunities for full and proper searches and investigation during the first hours after Stephen Lawrence's murder are to be deplored.”

MPS Special Notice 6/99 highlighted the importance of dealing with a crime scene properly. It stated, with the inclusion of a mnemonic for emphasis:

“Crime scenes are precious. The recovery of forensic material from a crime scene and the potential to provide evidence to detect the crime is well recognised.

The preservation of a crime scene is one of the primary responsibilities for police at any scene. The first officers on scene must do all that is possible to prevent:

- **M**ovement of exhibits;
- **E**vidence being obliterated;

- Additional material being added;
- Loss of evidence.”

It is regrettable that the special notice came 12 years after Daniel Morgan’s death and was prompted, at least in part, by the death of Stephen Lawrence. Nevertheless, the high-profile murder of a ten-year-old schoolboy in November 2000 indicates that it was effective. [The Damilola Taylor Murder Investigation Review](#), which was produced in December 2002, considered “that the initial crime scene management was effective”.²³

The Damilola Taylor review noted that local officers who were first on the scene of his attack “were followed quickly by members of a MPS Homicide Assessment Team (a quick response unit whose role is to secure crime scenes and seize evidence)”.²⁴

The homicide assessment team – commonly known as the ‘HAT car’ – was introduced because of Special Notice 6/99. It was officially renamed the ‘specialist crime car’ following the introduction of the MPS specialist crime command in 2019. (Those we spoke with still referred to it as the HAT car.) Four cars, each with two officers, now always operate throughout the force area. They attend homicides and other major offences to ensure that crime scenes are properly dealt with.

Crime scene management has otherwise developed in line with technological and scientific advances, and national policy. The 2021 *Major Crime Investigation Manual* provides links to APP to assist with crime scene management. The MPS’s Directorate of Forensic Services provides operational support at crime scenes where there is the potential to find forensic evidence. But difficulties can still arise with the way in which the police deal with items which they seize for their potential evidential value (‘exhibits’).

Exhibits and property

The police might take possession of items at any stage of an investigation but those they discover at the scene of a crime often prove most crucial. A forensic scientist who advised the DMIP concluded that the Operation Abelard Two reinvestigation:

“was marred by the inadequacy of previous investigations extending right back to the crime scene. Even if significant forensic evidence had been found it probably would not have stood up to scrutiny in relation to integrity, continuity, contamination etc.”²⁵

The fact that property and exhibits were mismanaged was clear from a very early stage; it wasn’t necessary to wait for subsequent reviews and reinvestigations to find out. A detective chief superintendent identified relevant issues in 1988 when he investigated a complaint made by Daniel Morgan’s business partner. The DMIP provided a much more detailed – and troubling – assessment over 30 years later. The Panel concluded:

“The failure to record the proper handling and management of exhibits seized, or the location in which those exhibits were stored, was unacceptable. Evidence may

²³ Para 3.1.5, p 13.

²⁴ Para 3.1.1, p 13.

²⁵ [The Report of the Daniel Morgan Independent Panel](#), 15 June 2021, vol 2, p 701, para 212.

have been lost, tampered with or contaminated. This failure had the potential to undermine any future prosecution.”²⁶

A recurring issue

Even without such a comprehensive report as the DMIP’s, the MPS should have taken action to ensure exhibits and property are always correctly handled. If nothing else, the brief report into the complaint in 1988 should have indicated that there was a problem. But some subsequent high-profile cases suggest that the MPS didn’t fully deal with it.

For example, the Stephen Lawrence Inquiry found that potentially important exhibits were lost or disposed of during that investigation in 1993. And there was potential contamination of evidence during the investigation into the murder of TV presenter Jill Dando in April 1999 (although it did not come to light until an appeal against conviction and retrial in 2007).

Special Notice 6/99 provided little assistance in this regard, although it frequently referred the reader to the *ACPO Murder Investigation Manual* for detailed guidance on various matters. Successive manuals provided advice on managing exhibits and securing forensic evidence. The 2006 manual, which was replaced during this inspection (it was replaced in November 2021), highlighted the care that needed to be taken as forensic science continued to develop:

“As the tests for DNA and other scientific techniques become more sensitive, it is increasingly important that SIOs are aware of the risk that evidence might become contaminated.”

Property management in the MPS

In light of the above comments, at the time of our inspection we expected to find that the MPS had well-established robust, professional arrangements for property management. We examined the arrangements not only for homicide cases but also for other serious offences and for volume crimes.

During our inspection, we spoke to hard-working and dedicated personnel who were trying their best, under difficult circumstances, to manage property in the MPS. Those we spoke with explained how property was “an enduring problem” for the force; they said the system was “fractured” and that it lacked supervision. And they demonstrated that there was “more property than storage”.

Our findings painted a dismal picture. They fell into three broad categories: space, security, and supervision.

Not enough space

We were told that property stores throughout the force held about 1.5 million items, of which over 50 percent were held at the central criminal exhibit stores for longer-term retention. The others were held locally across BCUs and specialist crime hubs.

²⁶ As before, vol 1, p 41, para 90.

Items are held locally, for an initial period, pending authority by the officer responsible for the investigation for the item to be destroyed, returned to the owner or moved to central stores for long-term retention.

In some BCUs, we found that facilities were suitable and had appropriate security measures, including CCTV cameras. But more often, the facilities were not fit for purpose. The stores were overflowing with items, which were piled haphazardly. We had particular concerns about firearms.

One BCU property clerk told us of an occasion when they opened a cupboard in the property store and firearms fell out. They said that some hadn't been checked to ensure they were safe. We had no reason to doubt this account but were unable to verify it because the firearms had been removed before our inspection.

In another property store (in a different BCU), we saw what appeared to be four shotguns propped against the outside of a firearms cabinet. The property staff we spoke with did not have keys for the cabinet. They told us that the keyholder, their manager, worked from a different police station and that the shotguns would not be secured in the cabinet until the manager attended. We did not examine the shotguns as they had been sealed in exhibits bags (although the MPS subsequently told us that they had been made safe and that they were correctly stored soon after our visit).

The MPS also informed us that its "policy is clear that firearms must not and cannot be handled by property staff until they have been made safe by an appropriate person". We also understand that in November 2021, following our inspection, the MPS issued further guidance and provided refresher training on firearms handling for all property staff.

We hoped to find that specialist crime command, which deals with some of the most serious offences, had better arrangements for property storage. One homicide unit we visited stored its exhibits in alarmed cages situated within a property store. Each team had its own cage, which was fit for purpose, and only exhibits officers could access it.

But we found a different situation elsewhere. Again, each homicide team had its own cage, but they were disorganised and crammed with items. Large quantities of property had been left inside the property store but outside the cages, which were full. One detective described the property store as "a disaster, tiny and not fit for purpose".

That said, we found that Operation Trident (which deals with gang-related gun crime) managed its own exhibits and property well at the same location. The operation's part of the store was organised, with separate safes for firearms, cash, drugs and jewellery. A member of the Operation Trident team questioned how his colleagues on the homicide teams ever managed to find anything.

A lack of security

Regardless of the lack of space, the MPS had introduced appropriate – though inconsistent – security measures for the homicide teams' property stores. At one location, cages had a double security entrance system (a swipe card and a keypad) and access was recorded in an auditable format. Another was fitted with locks and alarms and had both internal and external CCTV coverage. In all homicide cases, exhibits were recorded on HOLMES.

Despite these security measures, there were still instances when property which homicide teams had seized could not be accounted for.

We heard of two examples. One involved cash in the form of Dominican pesos (we were told that it was worth “a few hundred pounds” in sterling), which could not even be found when specially trained officers searched the property store. The other related to missing cocaine. The latter example is particularly disturbing: it was an important exhibit in a case and potentially of significant evidential value.

The situation in the BCUs was different again. Even if there was available space in a store, some provided little in the way of security. At one station, staff told us that the store, which was fitted with a digital keypad, was rarely locked. We checked for ourselves. We found that, if the door was ever locked, someone had thoughtfully inscribed the keycode on the door, above the lock. And in another location, we were told about an external property cage, open to the elements, that had become rat-infested. Apparently, it contained decaying cannabis plants supposedly awaiting destruction.

The lack of security, and the poor systems and processes generally, provide ample opportunity for corrupt officers and staff to steal, or otherwise interfere with, property and exhibits. We were told at one station that drugs, money and jewellery could not be accounted for. The MPS has also told us that, on arrival at police stations, exhibits are routinely left in unlocked ‘transit store’ rooms, before transfer elsewhere. Computer records at another store listed 109 items which had gone missing during the past two years. Our interviewees said that they identified the missing items when they compiled an inventory during a recent refurbishment of the store.

In response to our findings, the MPS informed us that, during the past five years, they recorded 3,428 items as ‘missing’ for a variety of reasons. The MPS pointed out that this equated to 0.05 percent of all items seized. Nevertheless, the examples we found (jewellery, cash and drugs), and the storage of firearms prompted us to immediately raise the matter as a cause of concern during our inspection.

Poor supervision

The MPS’s Locally Delivered Support Services (LDSS) department is responsible for managing property and exhibits. But, in the first instance, officers and staff working in the BCUs are expected to ensure that items which come into their possession are properly dealt with. Managers should make sure that those they supervise follow the rules.

A clear lack of supervision, insufficient training, and the resultant incorrect handling of exhibits only exacerbates the problem. LDSS rejects items that have not been properly packed and labelled and will only accept them when errors have been rectified.

While understandable, this creates a backlog. We were told that, in one BCU, there were over 5,000 rejected items. The MPS provides new recruits with theoretical training about property and exhibits but we heard frequent complaints that it was not enough: there needed to be more practical, on-the-job tuition to reinforce it.

All the systemic problems have led some officers and staff to seek alternative solutions. In contravention of force policies, they do not submit property and exhibits to the stores but retain them in their offices or lockers. There is a clear lack of trust in the functioning of the property system: some officers told us that, if they took items to a property store, there was a fair chance they would never see them again.

We saw the effects of this practice in several locations: bags of property lying around on landings, on windowsills and on office floors.

Putting things right

We examined a force risk register and found that it contained descriptions of 12 risks in respect of property storage. These risks included personnel recording insufficient detail in respect of seized property, the lack of capacity to store exhibits, unchecked firearms being stored in property store cabinets and the misappropriation or loss of exhibits. The force informed us that it was carrying out various actions to mitigate the risks, such as the introduction of a new, electronic property management system (Connect) in November 2022.

In the meantime, the current situation is wholly unsatisfactory, and given the lessons of Daniel Morgan, impossible to defend. The MPS has much more work to do. If it fails, some of the potential consequences are serious:

- cases collapsing at court when exhibits can't be found, or evidence is ruled inadmissible because of potential contamination (wilful or otherwise);
- litigation and compensation when items can't be returned to their rightful owners;
- an increase in corrupt practices as items are stolen or otherwise interfered with; and
- a loss of public confidence.

Cause of concern 1

The MPS's arrangements for managing exhibits and other property are a cause of concern.

Recommendation 2

By 31 March 2023, the MPS should:

- make adequate provision for the effective storage of property and exhibits, including the provision of sufficient capacity and robust security (including for firearms and other high-risk items);
- develop an effective process for the handover of property between BCUs/OCUs and the LDSS, including property that has been rejected before being accepted into the property stores;
- improve its record keeping in relation to stored property; and
- ensure it has sufficient supervisory oversight of the property process.

Case reviews

Reviews of the investigations have been a feature of homicide cases for many years. None resulted in Daniel Morgan's case being solved and some were particularly ineffective.

If a review is to be worthwhile, it must be painstakingly thorough, open and honest, and the reviewing officer must be prepared to confront poor practice and highlight missed opportunities. In other words, as the Stephen Lawrence Inquiry reported, it should be "searching and hard hitting and critical, if the ... [review] showed that mistakes had been made".²⁷ In that case, the Inquiry found that a review was "misleading and flawed" and "effectively indefensible".²⁸

Approximately a third of Special Notice 6/99, which was produced shortly after the *Stephen Lawrence Inquiry Report* and the first *Murder Investigation Manual*, was devoted to case reviews. It introduced a new framework to the MPS for reviewing murder investigations. It included reviews of:

- cases under investigation;
- solved cases (to identify good practice and lessons to be learned);
- undetected murders before an investigation is closed (to ensure that all reasonable steps have been taken to solve the case); and
- the further review of undetected murders at least every two years ('cold case reviews').

Under the framework, either a detective superintendent or detective chief superintendent was to lead each of three area murder review units. The head of each unit was answerable to a deputy assistant commissioner. The units' primary role was to review murder investigations.

The SCRG now performs this review role. When we reviewed the MPS's response to the Henriques report in 2020, we considered a recommendation relating to the SCRG:

"Senior Detectives should be reminded, or be made aware, of the full range of reviews that are available from the SCRG and should be encouraged to make use of them."

We found then that the SCRG had worked hard over the previous 12 months to promote its services, taking part in relevant senior detective meetings, and giving inputs on courses. As a result, senior detectives were well aware of the SCRG. We were also pleased to find a good level of awareness at BCU sergeant and inspector levels.

A specialist crime command officer chairs a case closure panel, which considers both solved and unsolved murders before investigations are closed. In addition to ensuring that all reasonable lines of enquiry have been completed when a case hasn't been solved, the panel should identify any organisational learning from both sets of cases (that is, solved and unsolved).

²⁷ [The Stephen Lawrence Inquiry](#), Sir William Macpherson of Cluny, 24 February 1999, para 28.19.

²⁸ As before, para 28.14.

The CPS and MPS joint review (2011–2012)

Following the collapse of the Operation Abelard Two trial in March 2011, the CPS and MPS undertook a joint review. They focused primarily on the SOCPA and disclosure issues which had arisen. The DMIP report covered the review, its recommendations and the MPS's response in some detail.²⁹ The Panel concluded:

“The Crown Prosecution Service and Metropolitan Police review process afforded an opportunity for the two organisations to consider in depth what had happened during the Abelard Two Investigation and to identify any lessons learned, or good practice ... The review report did not identify any issues which had resulted from current practice not being followed in this case and did not identify any lessons which might have been learned.”

Nevertheless, the review identified seventeen ‘good practice points’: eight related to disclosure, three concerned debriefing witnesses under the SOCPA, and six related to the control and direction of an investigation. The review also made one overarching recommendation, which was to disseminate the review within the police and CPS, so that they could consider good practice points in future cases.

Recommendations not implemented

In October 2019, the DMIP sought confirmation that the MPS and CPS had implemented the recommendation and good practice points. The DMIP considered the MPS's initial response insufficient and asked for more detail. In May 2020, the MPS provided a further response. It is clear from the MPS's May 2020 response that the force had paid little, if any, attention to the joint MPS and CPS report when it was produced in 2012. The MPS officer who provided the response stated:

“It would appear the 1-13 recommendations were not completed in 2012 but from making enquiries some of the recommendations were completed by other means, for example the Attorney Generals [sic] Guidelines Report of disclosure 2013 sets out five of the recommendations within the report.”

Recommendations implemented by default

The guidelines referred to were the [Attorney General's guidelines on disclosure 2013](#), which provided guidance on disclosure under CPIA. (The Attorney General issued [revised guidelines](#) in 2020.) In effect, therefore, the MPS implemented almost 30 percent of the good practice points by default rather than through conscious effort and direct action. The remainder, if not introduced by other national guidance (such as the [College of Policing's 2016 SOCPA guidance](#)), appear to have lain in abeyance until the DMIP's enquiries in 2019. For example, we found that only after the DMIP asked questions did the MPS prepare a disclosure ‘factsheet’ for general circulation and a presentation for inclusion in the detective inspectors' training programme.

In April 2020, the College of Policing provided the Panel with details of two courses relating to assisting offenders and SOCPA legislation. The MPS has also now introduced internal guidance and training, the content of which reflects the

²⁹ [The Report of the Daniel Morgan Independent Panel](#), 15 June 2021, vol 3, p 861, para 16.

review's findings. Therefore, the MPS has addressed the overarching recommendation for the review's dissemination.

Mistakes should not be repeated

The CPS and MPS carried out their joint review almost ten years ago. Much has changed since then. The first eleven recommendations related to CPIA and SOCPA. Force and national guidance and training on these matters has been introduced or updated, even if only recently in some instances. The final six recommendations concerned the control and direction of an investigation. The majority of those involved the CPS, which has introduced its own practices and guidance. The MPS considered that the two which directly related to them were case specific and unlikely to be repeated. The DMIP was less certain. It made the following recommendation:

“It is recommended that the Metropolitan Police introduce systems to ensure that the management arrangements which applied during the Abelard Two Investigation can never be replicated in any future investigation, and that proper management arrangements, in compliance with the Association of Chief Police Officers' Murder Manual, exist on all occasions.”³⁰

The manual referred to has since been replaced by the 2021 *Major Crime Investigation Manual*, but the principle remains the same: the MPS should not allow such mismanagement to happen again.

The Report of the Daniel Morgan Independent Panel

The Panel published its findings on 15 June 2021; in response, [the MPS Commissioner said](#):

“I recognise this is a powerful and wide-ranging report. We will take the necessary time to consider it and the associated recommendations in their entirety.”

But the MPS is also looking beyond the recommendations. It has learnt lessons from the Henriques report. In response to that report, the MPS only considered explicit recommendations and did not address other issues which were clearly set out. They too needed urgent attention. For example, Sir Richard Henriques (the author of the report) had recorded in considerable detail his concerns about the force's applications for and use of search warrants but had not included any specific recommendations. The problems were so obvious that none should have been necessary. Until 2019, the MPS did not act on his findings in that regard.

More encouragingly, the MPS has indicated that it will consider all matters that the DMIP report has highlighted, regardless of whether they are subject of recommendations.

The DMIP report included 24 recommendations, but one was duplicated: a recommendation made on page 1,115 of volume three appeared again on page 1,139. Therefore, the MPS will consider a total of 23 recommendations. It will also look at other matters raised in the report that might need attention.

³⁰ As before, vol 2, p 660, para 42.

Operation Drayfurn

On 23 June 2021, the MPS established Operation Drayfurn to respond to the DMIP report. That was only eight days after the report's publication. A deputy assistant commissioner (DAC) has overall charge of the operation and is answerable to the force's deputy commissioner. This level of seniority, and the prompt response, indicates the importance that the MPS has attached to the report. This commitment should be maintained.

Operation Drayfurn sits within the IRSC. It comprises two teams: a closure team and a response team. The former has been in existence, with various staffing levels, throughout the DMIP inquiry. At the time of our inspection, it included a superintendent, a senior MPS lawyer and a former (retired) inspector who had been employed on a contract basis for this purpose. The closure team was dealing with any residual matters, including the retrieval of documents from the DMIP and the archiving of inquiry material.

The response team included three constables, a member of police staff and several detectives: a superintendent; a chief inspector; an inspector; and two sergeants. The superintendent also had other responsibilities but reported to the DAC on progress each week.

The operation has identified six broad themes which the MPS needs to consider for the future:

- professionalism;
- working with panels and inquiries;
- organisational learning;
- the conduct of investigations;
- disclosure of information; and
- information security.

In addressing these matters, the MPS acknowledges that it will have to work with other organisations which are also affected: the CPS, NPCC, the Investigatory Powers Commissioner's Office (IPCO), the Home Office, and the College of Policing. The MPS has also established a professional reference group, which had met twice by the time of our inspection. The group includes an academic, who specialises in leadership, ethics and professional practice.

Operation Drayfurn is working to a timetable. When we visited, it intended to complete all its action plans by the end of 2021, and to start putting them into practice from early 2022. Only after that will it be possible to assess whether the MPS has been successful and the extent to which any changes have been effective.

7. A description of the systems and processes to support the Panel

We were asked to consider the MPS's response to DMIP requests for disclosure and access to material during the inquiry. Here we describe the systems and processes that were put in place to help the DMIP achieve its objectives. There was a huge amount of material for the Panel to review and it was important that the appropriate systems and processes were introduced from the outset. And essentially, the rules of disclosure to the Panel needed to be clearly set out and understood.

Legal representation

Throughout the inquiry, the DMIP was represented by a firm of solicitors. These solicitors, and counsel whom they instructed, dealt with legal matters on behalf of the Panel. The firm also contracted a legal services company to deal with certain functions. We refer to all as the DMIP's 'legal representatives'.

Lawyers from the MPS's Directorate of Legal Services (DLS) represented the force.

A non-statutory inquiry

The Panel was not established under the Inquiries Act 2005 ('the Act') and therefore it did not have statutory powers. We consulted counsel about the difference between statutory and non-statutory inquiries.

The primary point of distinction between statutory and non-statutory inquiries – most commonly in the form of independent panels – is that the latter cannot compel witnesses or order the production of documents or other material. Only a statutory inquiry under the Act will have the power to compel evidence to be disclosed; a non-statutory panel depends on the continued co-operation of all parties to conduct its work.

Where there are disputes between a non-statutory panel and another party as to how to approach a particular issue, there is no clear mechanism for breaking the deadlock. It may be that only the government department which established the inquiry can operate as a referee. In contrast, under the Act, it is clear that it is the inquiry which is in charge.

An advantage of non-statutory inquiries will usually be that they can operate more flexibly and without the specific rules and procedures applicable under the Act. This would include working wholly or partly in private. For relatively small and specific matters, this may well be an important advantage. But where the inquiry is of any significant size – whether in terms of public interest, impact, numbers of parties

involved or the amount of evidence and documents to be considered – the formal powers of an inquiry under the Act might be more efficient and effective.

For example, access to the MPS's HOLMES system was a bone of contention throughout the inquiry. This might not have arisen if the DMIP had operated on a statutory basis. In its report, the DMIP referred to the Independent Police Complaints Commission (now the Independent Office for Police Conduct) and its ability to access HOLMES material. In doing so, it reported:

“However, from 2005 the Independent Police Complaints Commission (later the Independent Office for Police Conduct) received copies of HOLMES accounts from police forces, including the Metropolitan Police Service, upon request. The accounts were loaded on to their server for use by their staff in their investigations. HOLMES was used on both desktop computers and on secure laptops, although where the material had a Government security classification of ‘Secret’ or above, separate considerations have applied.”³¹

The [Independent Office for Police Conduct \(IOPC\)](#) has replaced the Independent Police Complaints Commission (IPCC). The IOPC was established in 2018 by the Policing and Crime Act 2017. Its duties include the investigation of misconduct and criminality by persons serving with the police.

By virtue of the Police Reform Act 2002 (paragraph 19(4) of schedule 3), IOPC staff can be designated to have the powers of a constable. This includes powers of entry, search and seizure under the Police and Criminal Evidence Act 1984. It also has powers under section 17 of the Police Reform Act 2002 to require chief officers to provide information, including electronic copies of or direct access to HOLMES accounts, in such form, in such manner and within such period as may be specified.

A non-statutory inquiry – such as the DMIP – could not demand access to material and systems in the same way.

The disclosure protocol

Without the powers of a statutory inquiry, the DMIP relied on its [terms of reference](#). They stated that there would be:

“exceptional and full disclosure to the Panel of all relevant documentation including that held by all relevant Government departments and agencies and by the police and other investigative and prosecuting authorities”.

To put this principle into effect in so far as it related to the MPS, a [disclosure protocol](#) (‘the protocol’) was needed, setting out the terms, responsibilities and expectations of the MPS and the Panel in relation to providing and receiving documents. But reaching agreement on the terms of the protocol proved difficult. The Home Secretary announced the establishment of the Panel on 10 May 2013, and it formally started its work on 17 September 2013. But the protocol was not agreed until November 2014, after the new Chair took up her position.

³¹ As before, vol 3, p 1,131, para 69.

A contentious issue

It is apparent from the DMIP report that the most contentious disclosure issue was whether all Panel members would be allowed to see 'sensitive' documents which the MPS provided, or whether access would be limited to the Panel's Chair. All members of the Panel wanted to be able to see all the material. The term 'sensitive' in the report referred to the tranche of documents in the MPS's possession graded either confidential, secret, or top secret. Those documents required handling with particular care.

The protocol is eventually agreed

After protracted negotiations, a disclosure protocol was eventually agreed. It was signed by the three parties to the agreement: the MPS, the DMIP and the DMIP's legal representatives. It is unclear whether all parties signed on the same day, but the agreement was dated 20 November 2014. The DMIP was then able to make similar arrangements with other organisations whose documents it required.

The protocol agreed between the DMIP and the MPS provided that all members of the Panel, and its legal team, should have access to all documentation, including sensitive material in unredacted form.

We consider the difficulty in reaching agreement over the protocol in more detail later in our report.

The MPS disclosure team

The MPS introduced a disclosure team before the DMIP was established. Its role was to provide material to, and otherwise generally assist, the Panel. Initially, the disclosure team comprised a detective chief inspector as disclosure manager, a detective sergeant as lead disclosure officer, and a detective constable as disclosure officer.

The staffing levels remained constant for three years but were then reduced. The detective constable died in service in July 2016. He wasn't replaced as the MPS couldn't identify another officer with a similar knowledge of the case. The detective chief inspector moved to a new role in October 2016 but remained available to the detective sergeant for advice.

At that stage, the MPS had completed the disclosure of all case files and considered that the one detective sergeant would be able to deal with requests for additional material. He was also responsible for redacting documents to remove sensitive material. He was promoted to temporary detective inspector in April 2019.

As the Panel knew, the detective sergeant wasn't independent, as he had worked on the previous murder investigations. But, again, it would have been difficult to find anyone else with a similar knowledge of the case.

In 2019, a detective chief inspector (now detective superintendent) and a sergeant joined the team to provide greater oversight and a more independent view.

The temporary detective inspector retired in April 2020 but was employed on a contract basis to continue this work.

Governance

An assistant commissioner established a strategic oversight group in 2013. The group included officers of commander and chief superintendent ranks. It also called on others for professional advice when needed, including representatives of the MPS's legal services, professional standards, and media departments.

Closure team

The disclosure team has now become the MPS's closure team. It continues to deal with any residual issues concerning the Panel. It is responsible for recovering items provided to the DMIP and for the storage of all material.

As we described earlier in our report, another team (within Operation Drayfurn) is dealing with the MPS's response to the report and organisational learning.

Assessing the volume of material

Before the DMIP was established – or even announced – the MPS met with Home Office officials and consultants from a multi-national company with expertise in identifying technological solutions. They first met on 18 January 2013, and then held a series of meetings to assess the scale of any future inquiry.

Gathering the material together

After the first meeting the MPS disclosure team identified premises in East London, which could accommodate the case-file material that the MPS had accumulated over the years.

The MPS advised us that the decision to store the material there was for operational reasons. The premises were secure and there was sufficient space to house the quantity of material that had been generated. It comprised approximately 1,000,000 pages and 17,500 exhibits.

Despite the volume of material, the DMIP's terms of reference were to estimate that its work could be finished within a year:

“It is envisaged that the Panel will aim to complete its work within 12 months of the documentation being made available.”³²

Later in our report, we consider why this forecast proved to be so inaccurate.

In April 2013, the disclosure team started to gather the material together in an office. At that time, it was stored in 583 crates. Some years later, but still a considerable time before the end of the inquiry, the MPS completed structural alterations and provided more suitable accommodation within the same building.

³² As before, vol 3, p 1,233, para 1.

The MPS schedule of material

We were told that two technology consultants, appointed by the Home Office, visited regularly during 2013. They considered the volume of material in the crates to determine the best method of disclosure to the Panel. The DMIP's legal representatives also attended on 17 December 2013, to assess the quantity of material and hence the scale of the inquiry.

The MPS team had catalogued all the material and had produced a schedule of 4,800 pages, which listed everything (later referred to as the 'catalogue of documents'). In December 2013, it had 48,331 entries, but by the time of our inspection the total had risen to 52,079 (further material was added during the inquiry).

The MPS team also produced a redacted version of the schedule of material. They provided it to the DMIP's legal representatives and explained their cataloguing system, which identified every document and where it was stored.

MPS disclosure to DMIP

The material which the MPS provided to the Panel essentially fell into four categories: initial reading, non-sensitive, sensitive, and additional material.

Initial reading material

Although the disclosure protocol was not to be agreed for almost another year, the MPS provided the DMIP with initial reading material on 18 December 2013. This took the form of an encrypted disc. It included copies of the redacted schedule, more than ten reports, relevant photographs and plans, a list of MPS acronyms, legal papers relating to the Operation Abelard Two case, and the 'MPS Review [disclosure] Team Redaction Policy'. The disclosure team also provided a suggested reading sequence for this material. At that time, the Panel only had three members and did not have a Chair.

The non-sensitive material

While the disclosure protocol was still under consideration and was yet to be agreed, the MPS also permitted the DMIP access to non-sensitive material at the MPS's premises in East London. This allowed DMIP staff to start indexing and coding each item before it was taken away for scanning onto an electronic case-management system (Lextranet). The Panel would then be able to access the documents electronically.

The DMIP's legal representatives employed a small indexing team for this cataloguing role. Its members were commonly referred to as 'box-loggers'.

DMIP's cataloguing of non-sensitive material

The MPS told us that four box-loggers started work at the MPS premises on 16 October 2013. Apparently, their numbers fluctuated thereafter because of a high turnover in staff – the MPS claimed that some only lasted one day – but we understand that at times there were as many as eight working there.

The MPS disclosure team said that they offered the box-loggers access to the MPS's catalogue of documents so that they could copy entries onto the schedule they were creating for the Panel, especially descriptive detail. The MPS thought that this would make the box-loggers' task more manageable and would speed up the whole process. The MPS said that the DMIP initially declined this offer because of issues of trust and allegations of corruption connected to the case.

The MPS said that, initially, the box-loggers attached a barcoded slip to every item in a crate. We understand that, in total, they created 109,000 slips. They started with the 17 crates containing the Operation Abeldard Two case files that had been provided to the CPS. These were readily available as the MPS had already reviewed their contents for [disclosure](#) purposes for court.

A very slow process

The whole process was very slow: the MPS told us that the box-loggers took six weeks to catalogue the first six crates. The MPS also said that on 18 May 2015, when the DMIP's cataloguing process had already been running for over 18 months, a box-logger showed them a DMIP estimate of how much longer the process would take. Apparently, it said that the three box-loggers then working on the task would take five years to complete it; if the staffing level was increased to nine, it would take 18 months.

The DMIP's change in approach

The MPS said that, because of the projected timescale, the DMIP then decided to accept the earlier offer for the box-loggers to refer to the MPS's catalogue of documents. Thereafter, the box-loggers simply copied descriptive detail of documents from the MPS's catalogue rather than reading through documents and composing their own entries.

The DMIP also changed its approach to barcoding at the same time. Instead of attaching a barcoded slip to each item in a crate, the box-loggers produced one for each box of material within a crate (which would often contain many items). This saved a considerable amount of time. We examined the crates and confirmed the change in the DMIP's approach.

The supply chain

After the box-loggers had catalogued a crate, the MPS sealed it ready for sending to the DMIP's legal representatives. The crates were sent in batches. The legal representatives scanned the contents onto Lextranet before returning the crates to the MPS's office. The legal representatives provided transport for the outward and return journeys.

Record keeping

The MPS kept very comprehensive records of each stage of the process. A member of the disclosure team recorded when each crate was sealed, when it was dispatched, when it was received by the DMIP's legal representatives and when it was returned to the MPS. At every stage of the process, a document was signed and dated by the person receiving the crate. The MPS also provided a fresh seal so that the crates could be re-secured before the return leg of the journey.

Records kept by the DMIP were less comprehensive. They told us that although they made a record of every document received, it did not necessarily indicate the date of receipt or when the Panel accessed the document after the scanning process.

Delivery of the first crates

Nevertheless, we found some accord between individual records: the MPS sent a first batch of 24 crates on 2 October 2014 (which was before the protocol had been agreed and signed); a second batch, consisting of 55 crates, was dispatched on 27 November 2014; and a third batch of 46 crates went on 23 December 2014.

The DMIP's different case-management systems

Some years into the inquiry, the DMIP transferred its data from Lextranet to another case-management system (Relativity). The transfer started in April 2018 and took 12 months to complete. However, the Home Office did not grant security accreditation for the Relativity system until July 2020. This meant that, from April 2019 until July 2020, the DMIP worked on two systems. The DMIP reported that this "further delayed the Panel's work".

Redaction of sensitive material

Redaction proved to be another contentious issue. We comment on it later in this report. Here, we describe the processes involved.

The MPS disclosure team worked ahead of the box-loggers and removed documents from the crates which they had valid reasons for believing contained sensitive information. They copied the original documents and then redacted the copies by manually blocking out any material they deemed sensitive. They inserted pink pieces of paper – which were readily identifiable – into the crates concerned to indicate where there were redacted copies of documents. The box-loggers did not see the original versions, which were kept separately.

Viewing arrangements

For security reasons, sensitive material could not be loaded onto Lextranet. However, in accordance with the protocol, members of the Panel and their legal representatives were permitted to view unredacted copies. Another feature of the protocol was that the 'providing organisation' – for the most part the MPS – would retain control of its own documents. The unredacted versions were to be inspected "at the providing organisation's own premises". This meant that the Panel had to travel to MPS premises in East London to view unredacted sensitive material.

Because of the amount of material that the MPS redacted, the Panel members felt that they wasted a lot of time travelling to and from East London.

Alternative viewing arrangements

In September 2019, agreement was reached for the DMIP to view unredacted sensitive material at a police station nearer to the DMIP's own offices. To facilitate this, the MPS disclosure team scanned the material onto an encrypted laptop, which was securely retained at the police station.

DMIP requests for additional material

The DMIP and MPS agreed a process for providing additional material and information which the Panel identified during its work and wanted to see (that is, in addition to case-file material which was stored in crates in East London). DMIP records indicate that the Panel made 426 requests for additional information or material but, again, the DMIP's records weren't as comprehensive as those the MPS produced.

The DMIP acknowledged to us that its own records were "not a complete picture" and that they didn't include all oral requests for additional material, such as those made by telephone or during meetings. The MPS's records, on the other hand were very comprehensive. The MPS recorded 726 requests for additional material or information and provided the DMIP with an additional 616 documents as a result.

We found that the DMIP's records were also incomplete in terms of data showing when the MPS responded to individual requests. Nevertheless (and notwithstanding its otherwise strident criticism of the MPS), the DMIP was generally satisfied with the MPS's responses and acknowledged the disclosure team's contribution in this regard.

The requests for additional material created a significant amount of work for the MPS and the disclosure team. The material was frequently to be found in different departments around the force; in some instances, it wasn't even in the MPS's possession (we were told of one example where material had already been provided to another inquiry and had to be retrieved). On receipt of a request from the DMIP, the disclosure team contacted the relevant department and asked for the material.

Unreasonable delay in providing the material was infrequent; the DMIP reported accordingly:

"Where the single point of contact [the MPS disclosure team] could respond directly, the Panel received prompt acknowledgement of the request made and very often received a substantive response on the same day."³³

However, the DMIP also cited an occasion where it only received a document (an operational decision log) "a year after it had first been requested and after a number of reminders had been sent".³⁴ We made enquiries. The MPS disclosure team had asked an MPS officer for the document, but he failed to attend to the matter for a considerable period. We found his excuses unconvincing; the MPS should have responded to the request much more promptly and dealt firmly with the officer.

³³ As before, vol 3, p 1,124, para 28.

³⁴ As before, vol 3, p 988, para 450.

But the disclosure team also provided other material of its own volition, which the MPS thought might be useful to the Panel in its work. Although the DMIP hadn't requested the material, they found it useful:

"It was also most helpful to the Panel that, on occasion, the single point of contact readily volunteered information to assist the Panel and help identify relevant material to meet its requests."³⁵

The MPS continued to provide material to the DMIP until March 2021. This was largely because the Panel examined several more recent investigations into allegations of police corruption, which had not even started when the inquiry was established in 2013.

Contacting serving and retired officers and staff

As the inquiry progressed, the DMIP identified both serving and former officers who might be able to assist with its work.

The MPS was better placed to locate the individuals concerned and the DMIP wanted the force to send out confidential correspondence on its behalf. The MPS agreed to do so but initially intended to enclose accompanying correspondence of its own, with information and advice for the intended recipients. The DMIP objected and the MPS withdrew its own proposed correspondence.

The pre-publication process

Many public inquiries involve consideration of sensitive information. We were advised by our counsel that as a non-statutory inquiry, how the Panel dealt in its report with evidence which was said by the party providing it to be highly sensitive could only be addressed between the Panel and the party, through a negotiated agreement.

The original disclosure protocol

The MPS told us that it initially took comfort from the fact that the protocol set out a process whereby it could object on security and other grounds to the publication of documents or parts of a document that they had provided. In particular, the protocol stated that the Panel would:

"only publish documents and /or parts of documents disclosed to it with the express written consent of the providing organisation which supplied the particular document in question."

In protecting the Panel's interests, the protocol said that organisations would not "unreasonably withhold consent". In the event that the Panel considered that consent had been withheld unreasonably, it would not publish the material concerned. However, in such a situation, the Panel may publish the fact that it considered that consent had been withheld unreasonably.

³⁵ As before, vol 3, p 1,124, para 28.

The final arbiter

Whatever the original protocol intended, it was clear that in practice the DMIP decided what to include in its report.

The DMIP supplied those who had provided material with details of the quotations and paraphrases which it proposed to publish. This allowed them to make representations about any redactions which they considered necessary. The DMIP considered their responses but, as the DMIP made clear in its report, the Panel considered itself to be the final arbiter:

“The Panel gave careful consideration to any representation made by any material provider. Where the Panel considered consent to publish was withheld unreasonably, it sought to agree a suitable change in wording to enable consent to be given. Ultimately, however, the final decision on publication rested with the Panel. Any such decisions were communicated in a timely fashion to the material provider.”³⁶

Anonymity

When considering whether to name individuals in its report, the DMIP applied an anonymity policy. The policy is available on the [DMIP website](#).

In applying the policy, the Panel said that it:

“sought to balance the public interest in shining a light on the circumstances of Daniel Morgan’s murder, its background and the handling of the case as required by the Terms of Reference, with the need to protect individuals from any risks to their safety and security and the right to privacy afforded to individuals by the Human Rights Act 1998.”³⁷

The DMIP said that it did not publish personal data unless it was in the public interest to do so. In deciding whether there was significant public interest in naming an individual, the DMIP considered several factors, including:

- whether the individual was so significant to the case that, by not naming them, the DMIP would not fulfil its terms of reference;
- whether the individual was a public figure; and
- whether the individual had already been named in connection with the murder investigation.

The DMIP said that it based its decisions on whether to anonymise (‘cipher’) individuals in the report on MPS risk assessments and “other criteria”.³⁸

³⁶ As before, vol 3, p 1,242, para 44.

³⁷ As before, vol 3, p 1,241, para 46.

³⁸ As before, vol 3, p 1,241, para 49.

The security review

Prior to the publication of the report, a small team of MPS officers conducted a security review intended to identify any concerns in relation to:

- “the protection of current covert police methodologies and intelligence principles; and
- the Metropolitan Police’s obligations under the European Convention on Human Rights, including security risks to covert human intelligence sources (informants).”³⁹

Arrangements for the security review were reflected in a separate protocol document (Protocol document for security check of the Panel Report). The officers undertaking this task were given sections of the report for inspection, which the Panel considered could give rise to a security issue. The officers could not disclose the content of the report with others and signed confidentiality agreements.

The security check protocol document was clear about who was to be the final arbiter on publication:

“For the avoidance of doubt, the Panel will make the final decision about the text to be included in the report.”

The Panel’s position was that the issue of the public interest in what to publish and any possible prejudice to future criminal proceedings was for the Panel to decide. In correspondence, the Panel made clear that it would make its own decision, “taking account of the position of the police and the family of Daniel Morgan”.

Panel members told us that they were mindful that the murder remained an open investigation and that this had implications for potential witnesses. This accorded with the original protocol, which urged the Panel to ensure that its final report was “in compliance with all its legal obligations” and that it:

“[did] not breach any security requirements including, in particular, the provision of information that might give rise to a risk to life or a risk to prejudice of future criminal proceedings.”

We understand that, prior to publication, the DMIP sought counsel’s advice on the likelihood of prejudicing any future court proceedings. On receipt of that advice, the DMIP considered making any amendments needed to mitigate perceived risks.

The MPS told us that in all but two cases it was able to reach a compromise with the DMIP. This might have involved re-wording intended entries in the report or using ciphers. Nevertheless, it was a contentious process. We understand that solicitors acting for individuals who may have been identified in the report even made representations in a bid to protect their clients from exposure. And the MPS contended that even ciphered individuals could be identified by people with a detailed knowledge of the case.

³⁹ As before, vol 3, p 1,242, para 55.

The fairness and courtesy processes

The Inquiries Act 2005 is supplemented by the Inquiries Rules 2006 ('the Rules'), made under section 41 of the Act. The Rules include that any person who is to be the subject of criticism in an inquiry report shall be sent a warning letter which summarises the basis for the proposed criticism and provides an opportunity for reasoned responses. Although a non-statutory inquiry, the DMIP decided to adopt a similar procedure. DMIP referred to it as the "fairness process".

The DMIP reported that, as part of this process, letters were sent to 86 individuals and organisations (both police and others) who were to be criticised in the report. It then considered the 57 responses it received prior to finalising its report. It also tried to notify anyone else who might be named, but not criticised, in the report. The MPS referred to this as the "courtesy process".

Reflecting the process for contacting serving and retired officers which we discuss elsewhere, the MPS sent out the letters on the DMIP's behalf. Very few of the intended recipients were still serving with the force. The DMIP provided the MPS with sealed envelopes containing letters for those who were to be named or criticised. The MPS forwarded the letters by recorded delivery.

The MPS told us that they started to receive batches of the letters from 21 September 2020. The last letters only arrived in March 2021, which allowed little opportunity for the MPS to trace individuals and for the people concerned to respond. In one very late case, the MPS had to contact the family of a former officer who had died in 1987.

Locating the people concerned

On receipt of the sealed envelopes, the MPS had to determine, in the first instance, whether the intended recipients were still alive. They contacted the MPS pension providers and made other enquiries to identify addresses and possible contact numbers, both for those who were alive and for relatives of those who had died.

We have seen a schedule, which the MPS produced, of the names of officers and staff whom they were to contact on the DMIP's behalf. Although the DMIP referred to 86 individuals (from different organisations) who were to be criticised, the MPS had to locate and contact 145 people (or their relatives): 47 officers and staff who were to be criticised, and a further 98 who were to be named but not criticised. Finding them all proved very difficult; some had moved as far as Australia.

If individuals had died, the MPS had to identify and contact the next-of-kin. There were four deceased officers on the 'criticised' list, and 13 on the 'courtesy' list. The MPS managed to find the next-of-kin for all but one.

Welfare and legal support

The MPS was rightly concerned about welfare issues. Some people were over 90 years old. They offered welfare support to all but eight former officers, who had been convicted of offences or otherwise dismissed from the force. They also offered legal advice, through the force's legal services department, to those who were to be criticised.

The MPS told us that the process caused much concern for retired officers and their families (including the families of those who had died).

8. The relationship between the Panel and the MPS

In the preceding chapter, we described the systems and processes which the DMIP and the MPS introduced so that the DMIP could achieve its objectives. It was not our function to review the conclusions of the DMIP. In any event, the work we have done on this inspection would not enable us to do so. However, in order to review the MPS's response to the DMIP report, and particularly the MPS's handling of disclosure, etc during the course of the DMIP's work (part 2 of our terms of reference), it is necessary for us to form our own view on the extent to which the MPS's relations with the DMIP were appropriate.

Therefore, here we consider how effectively the MPS and DMIP worked together, and whether the MPS supported the DMIP as it should have done.

The DMIP said that it "faced major, unnecessary problems in accessing material and systems", and concluded:

"While it [the Panel] received great assistance from organisations such as the National Crime Agency, the Independent Office for Police Conduct, and the Criminal Cases Review Commission, it did not experience, particularly from the Metropolitan Police, the necessary level of cooperation."⁴⁰

The DMIP's grievances

We have grouped the DMIP's main grievances under four headings:

- the disclosure protocol;
- accessing the sensitive material;
- HOLMES; and
- accessing retired and serving officers.

We consider each in turn; we include the MPS's responses and our own conclusions.

In all but 'the disclosure protocol' we consider the DMIP's complaints, the MPS's position and our own conclusions separately. In the case of the disclosure protocol, the DMIP's and the MPS's cases are so closely connected that we consider both together.

⁴⁰ As before, vol 3, p 1,139, para 111.

The disclosure protocol

The DMIP set out in its report criticisms of the stance that the MPS took when negotiating the contents of the protocol.⁴¹ The Panel complained that the MPS held up progress on agreeing the wording of the protocol and thus frustrated the start of their work:

“The Panel experienced very significant delays because of the difficulties of securing agreement to disclosure by the Metropolitan Police.”⁴²

The MPS’s view was that, because the DMIP was not constituted under the Inquiries Act 2005, a bespoke process would be needed for the disclosure of material, some of which was sensitive.

Agreeing the process proved to be a difficult undertaking.

Sensitive material

It is apparent from the DMIP report that the most contentious issue was whether all Panel members would be allowed to see ‘sensitive’ documents which the MPS provided, or whether access would be limited to the Panel’s Chair. All members of the Panel wanted to be able to see all the material.

The MPS, on the other hand, initially understood that it would be a ‘judge-led’ inquiry and that access to sensitive material would be limited to the Panel’s Chair. However, it soon became clear that Panel members did not want access to be restricted to the Chair alone.

Initial negotiation

The MPS said that, in July 2013, agreement was reached with the DMIP’s first Chair (a retired Appeal Court judge) about the disclosure of material. The DMIP refuted this. It said that the MPS’s assertion:

“was not reflected in documents produced by the Panel or the Home Office at the time, and the proposed approach was rejected by the Chair and the other members of the Panel.”

The DMIP said that, on 29 August 2013, its legal representatives sent a draft protocol to the MPS. It said that the Panel needed access to all documents in an unredacted form, except where prohibited by law. However, it recognised that “special provisions might be necessary for the most sensitive documents”.

The DMIP reported that, on 9 October 2013, the MPS wrote to the DMIP describing a process where the Chair could see all sensitive documentation and then “pass to the remaining members” what the Chair considered appropriate.

⁴¹ As before, vol 3, pp 1,118–1,122.

⁴² As before, vol 1, p 14, para 79.

The DMIP said that its lawyers sent a revised draft of the protocol to the MPS on 23 October 2013. It provided for disclosure of sensitive material to be made in the first instance only to the Chair.

On 28 October 2013, the DMIP sent a further revised draft, which provided for the whole Panel to see the unredacted sensitive material.

The MPS said that, in November 2013, it endorsed a protocol proposed by the DMIP's solicitors. The DMIP reported that the MPS responded on 12 November 2013. In doing so, the MPS agreed to the version of 23 October 2013, but rejected that of 28 October 2013.

The first Chair resigns

For personal reasons, the initial DMIP Chair resigned with effect from 13 November 2013.⁴³ The MPS claimed that his resignation temporarily hindered progress, as the Panel was not properly constituted until a replacement Chair was appointed. His successor was appointed in July 2014 but did not take up her post until September that year.

The MPS told us that, from its point of view, this created a hiatus. The MPS provided us with an example of the difficulties that this caused. The MPS said that, on 31 January 2014, the Senior Master of the Queen's Bench Division refused to disclose to the Panel material generated as a result of a civil claim against the MPS, because the Panel lacked a Chair and was not properly constituted at that time.

Negotiations continue without agreement

Despite the issues concerning the constitution of the Panel, the protocol was not left completely in abeyance. On 25 February 2014, an MPS solicitor wrote to the Home Office, indicating a potential compromise:

“The Metropolitan Police was, is and will remain flexible as to the precise arrangements and will seek to fit in with the preferred approach of the Panel. It would still much prefer an approach where the most sensitive documents are reviewed by a judicial (or legally qualified) chair before they are given any wider disclosure. But if that is not acceptable to the Panel we are not wedded to this approach.”

On 13 March 2014, there was a meeting between the MPS and the DMIP. The minutes of that meeting reflect the fact that responsibility for drafting the protocol had, for the time being, been given to the Home Office. A different model for the protocol was under consideration, based on that adopted for the [Patrick Finucane Review](#).

Notwithstanding these developments, there was constructive discussion and engagement between the respective legal teams on the approach to be taken.

⁴³ As before, vol 3, p 1,120, para 11.

The replacement Chair takes up post and the protocol is agreed

The replacement Chair was appointed in July 2014 but, for personal reasons, was unable to start work in London until September of that year. The matter of the protocol was only resolved after the replacement Chair took up post.

In November 2014, following further disagreement and negotiation, the protocol was eventually agreed and signed. It provided that all members of the Panel, and its legal team, should have access to all documentation, including sensitive material in unredacted form. This reflected the DMIP's proposal of 28 October 2013.

Our conclusions regarding the disclosure protocol

It is not necessary to include in our report a record of all the correspondence that flowed between the parties to the protocol, or the meetings between them. Suffice to say, it was a difficult and protracted process, with claims and counterclaims about what had been said and agreed – or disagreed – along the way.

We recognise that the MPS had to adopt a cautious approach to protect highly sensitive material; failure to do so could have had dire consequences. And we accept that the resignation of the first Chair disrupted the process. However, it should not have taken 18 months or more for the MPS to agree that all members of the Panel should be given access to all the material in unredacted form.

The Home Secretary commissioned the inquiry. The DMIP, in turn, reported to the Home Secretary and to Parliament. All its Panel members were security vetted to an appropriate standard. The MPS's approach should have reflected this.

The DMIP contended that:

“it was neither necessary nor proportionate for the processes for disclosure and document handling to have taken such a long time to be agreed with the Metropolitan Police.”⁴⁴

We agree.

We further concur with the DMIP's recommendation that:

“[a]rrangements must be made in future to ensure that any Panel has timely access to the material required to do its work.”⁴⁵

The protracted negotiations in this case should not have been needed. Arrangements for disclosure should have been established at the outset, when the DMIP's terms of reference were set.

Accessing the sensitive material

As we set out in the preceding chapter, a separate arrangement was made for the DMIP to access sensitive material. It involved travelling from the DMIP's central London offices to the MPS's premises in East London to view redacted material.

⁴⁴ As before, vol 3, p 1,122, para 24.

⁴⁵ As before, vol 3, p 1,122, para 25.

The DMIP's view on redaction

Even the redaction process itself proved to be a contentious issue. The DMIP appreciated that the protection of investigation material was right and proper but considered that some material “was excessively and inconsistently redacted” and that at times the redactions were “clearly unnecessary”.⁴⁶ This led to large quantities of redacted material and, in turn, to repeated visits by Panel members to East London. The DMIP was concerned that each return journey involved two hours of wasted travel time.

The MPS's view on redaction

The MPS pointed out that, regardless of the redaction process, the DMIP ultimately saw everything and wasn't refused access to anything.

The MPS followed the redaction policy it had sent to the DMIP in 2013 (referred to earlier). The MPS told us that they had two overriding considerations during this process: Daniel Morgan's murder was still an unsolved case and they did not want to compromise any future investigation and prosecution; and the police had a duty under Article 2 of the European Convention on Human Rights (right to life) to protect witnesses and others who had featured in their investigations. These operational and legal considerations meant that the MPS proceeded with justifiable caution and care.

There was also a recognised procedure for the DMIP to challenge the MPS's redaction decisions.

MPS lawyers advised the disclosure team when required but only considered that the team had wrongly classified material on one occasion (in relation to medical records). The disclosure team reclassified the material accordingly.

The MPS cited an occasion when the DMIP complained about a redaction which had removed the name of a public house. Without knowing the context, this might have appeared to be unnecessary redaction. However, the information was contained within a secret document and its inclusion would have revealed the location where a [covert human intelligence source](#) (informant) met with the police.

The DMIP's view on alternative arrangements

The DMIP said that, in May 2015, its Chair wrote to the MPS in an effort to make alternative arrangements for viewing the material. The DMIP's report included the MPS response. An assistant commissioner agreed that the MPS could provide access to the material in question at New Scotland Yard, but said that such an arrangement would have consequences:

“i. Two police officers would be required to convey sensitive material to and from New Scotland Yard, to avoid the risk of such highly sensitive material, including that relating to threats to life, being lost or misplaced during its move between locations. This would have resource implications and could delay other work, including preparing material for the Panel.

⁴⁶ As before, vol 3, p 1,136, para 94.

- ii. The quantity of sensitive redacted material would increase as more documents were disclosed, so the frequency of transportation to New Scotland Yard would inevitably increase.
- iii. The sensitive material was required for reference, during the preparation of the less sensitive material for data-indexing and digitalisation for the Panel. Relocation of these documents away from the bulk of the papers could cause delays.
- iv. Access would only be permitted at New Scotland Yard to the sensitive material. As a consequence, Panel members would have been unable to check the surrounding material which was sometimes helpful when viewing the sensitive documents.”⁴⁷

After consideration, the DMIP decided to continue with the existing arrangements of viewing sensitive material in East London.

The MPS’s view on alternative arrangements

This process continued until September 2019, when agreement was reached for the DMIP to view unredacted sensitive material at a police station nearer to the DMIP’s own offices. To facilitate this, the MPS disclosure team scanned the material onto an encrypted laptop, which was securely retained at the police station.

The MPS said that to provide this facility, it had to take sensitive material from the premises in East London to its IRSC’s offices nearer to central London. The material was then scanned onto an IRSC computer database (Relativity). The MPS claimed that they could not offer this alternative any earlier because the material in question was still being reviewed and redacted and because Relativity did not have a full search capability until then.

MPS records indicated that the DMIP only used the facility once; on 13 February 2020, the secretary to the Panel, the DMIP’s legal team and its senior researchers viewed the material on the laptop but did not visit again.

Our conclusions regarding accessing the sensitive material

Redaction

We understand that, in late 2013, long before the disclosure protocol was agreed, the MPS disclosure team prepared a redaction policy for the inquiry. We were also told that it was then agreed by the disclosure team’s oversight group and a force solicitor. The MPS said that it sent the policy to the DMIP on 18 December 2013. Email correspondence indicates that the MPS also forwarded the policy again on 2 June 2014, at the DMIP’s request.

⁴⁷ As before, vol 3, p 1,135, para 91.

We have seen the redaction policy that the MPS said it sent to the DMIP on 18 December 2013. It set out that the documents which were to be considered for redaction comprised:

- “Information/intelligence which alludes to the use of or identity of a Covert Human Intelligence Source (CHIS) or reveals methodology which if disclosed may undermine the MPS or National source handling system. [Including U/C and tasked witnesses deployments]
- Information/intelligence which alludes to the application for, use, deployment or product of a phone Intercept.
- Information/Intelligence provided as a result of applications to the Prison Advisory Service. (Subject to further discussion by Home Office with PAS-Operational Partnership Team)
- Information/intelligence concerning sensitive operational techniques, the disclosure of which may create serious risk to persons and/or property, or jeopardise future police operations, or present a real risk of serious prejudice to an important public interest. This would include (but is not restricted to) for example, revelation of observations posts where people have provided assistance to police with the expectation of anonymity. Also included would be the release of technical details and process of how covert assets such as probes are deployed and disguised.”

A supplementary note to the above further stated:

“The individual documents may themselves be subject to redaction in accordance with the same policy and further revealed as necessary in accordance with the protocol between the MPS, Morgan Independent Panel and Home Office yet to be finalised.”

This was produced almost a year before the disclosure protocol was agreed. Reference to redaction in the disclosure protocol was based on the security classification of documents under the Government Protective Marking Scheme (GPMS). Before October 2017, the MPS graded documents according to the GPMS. After that date, it adopted the replacement [Government Security Classification Policy](#), which was first introduced on 2 April 2014.

The disclosure protocol made clear that the Lextranet system, which the DMIP used, was only “accredited to hold documents with a protective marking up to and including RESTRICTED/OFFICIAL-SENSITIVE”.

Therefore, ‘providing organisations’ were asked to review documents and:

“(a) redact the bare minimum necessary to achieve the protective marking downgrade, so the document [could] be uploaded on to Lextranet; and

(b) where it [was] necessary to make a redaction to achieve the protective marking downgrade, provide the reason for the redaction and separately make the unredacted version available to the Independent Panel in hard copy.”

Even working to a defined process, redaction can be a subjective exercise, defined by context and a comprehensive understanding of the subject matter. We can appreciate

both the MPS's and DMIP's points of view over this matter. However, the MPS might have adopted an overly cautious approach at times.

But there would always be discussion and argument on this topic, bearing in mind that the MPS and DMIP were dealing with the classification of documents, some of which had been created several years ago. It is easy to imagine the classification of a document changing over a period, for example to reflect what was – and what was not – in the public domain at that specific time.

In addition to the above, the MPS and DMIP had to contend with the fact that, in 2017, there was the change to the Government Security Classification Policy, which had replaced GPMS. The MPS mapped the classifications between the new and old regimes as it saw fit. This would, inevitably, lead to differences of opinion about how individual documents should be classified.

As the Panel knew, the lead disclosure officer wasn't independent of the murder investigations that had gone before. He had been involved in the case over several years and was criticised over disclosure during pre-trial Crown Court hearings between 2009 and 2011. He was also criticised by the DMIP in its report, particularly in relation to redaction. But it would have been difficult to find anyone else with a similar knowledge of the case.

Despite the criticism in the DMIP report, a Panel member told us that the lead disclosure officer "did his utmost" to assist and acted with integrity throughout. The Panel member also recognised that this officer knew the entire history of the case, which was an obvious benefit.

Alternative arrangements

We concluded that the DMIP's complaints in this regard had more to do with convenience than being denied access to material. The DMIP accepted that, ultimately, it was not denied access to anything, but told us, "It was more about the MPS being difficult rather than preventing access to material."

MPS records indicate that the DMIP visited the East London premises to view material on a total of 41 days over the eight-year period.

Nevertheless, we are not convinced that alternative arrangements could not have been introduced before late in 2019, six years after the inquiry started. And we are not persuaded by the assistant commissioner's argument that taking sensitive material to Central London would have been to the detriment of work in South East London. The MPS is a very large organisation; two additional staff could easily have been found to provide transport and security. After all, it would not even have been a full-time role and it would not have required a fully trained police officer to do it.

However, despite the DMIP's complaints, the existing arrangements accorded with the disclosure protocol which all parties agreed to. The DMIP also confirmed them in an email to the MPS, dated 8 October 2015: "We accept that we will view any unredacted sensitive material at ... [the South East London premises]."

HOLMES

The DMIP's position on HOLMES

The DMIP devoted several pages of its report to its attempts to secure “proper access” to the MPS's HOLMES computer system. It was an issue throughout the inquiry; according to the Panel, it was never resolved. The Panel was confident that, with proper access, it would have been able to finish its work much sooner.

The Panel reported in detail its exchanges with the MPS about this matter over the years. We do not intend to repeat them all here; it isn't necessary to do so. Rather, we include a summary of the DMIP's position. In essence, it concluded that the MPS was determined not to permit proper access. The DMIP also claimed that the MPS never provided a reasonable explanation for its position.

The DMIP's position on requiring access

The DMIP considered that access to HOLMES was essential for its work. With allegations that police corruption had affected the murder investigation, it could not simply rely on the MPS's guarantee that all was in order. It had to be able to compare HOLMES records with physical documents to ensure that everything had been made available and that the integrity of the system was sound. It also needed to research the system for its own purposes.

As it transpired, DMIP panel members and certain other DMIP personnel were allowed access to the system, but DMIP researchers weren't.

The DMIP's position on secret information

In the first instance, in November 2013, the MPS told the DMIP that the system held highly sensitive material, including secret information. That was true, but HOLMES should not have been used as a receptacle for material classified as secret. Then, at a meeting on 5 December 2013, an assistant commissioner (now the Commissioner) “expressed a strong reluctance to allow the Panel access to the system, although she did not explicitly refuse it at that point”.⁴⁸

At a further meeting on 13 March 2014, an MPS detective chief superintendent reported that the same assistant commissioner was “not supportive” of the DMIP's requests to access HOLMES:

“primarily because almost the entire database (not just the Abelard Two Investigation) contained ‘Secret’ classified material in the form of the identities of informants, and the material on the system could not be redacted.”⁴⁹

The Panel duly obtained independent advice, which confirmed that, although it would be time-consuming, the system could be redacted.

⁴⁸ As before, vol 3, p 1,126, para 39.

⁴⁹ As before, vol 3, p 1,126, para 41.

The DMIP's position on access at MPS premises

After further negotiation, on 15 October 2014, the MPS agreed to allow unrestricted access to the HOLMES system, on MPS premises, to the Panel members and their legal representatives. The Panel agreed, as an interim measure, to appoint a HOLMES specialist to access the system on MPS premises but wanted its own HOLMES facility.

The DMIP's position on installing a terminal at their premises

The DMIP repeatedly asked for either a HOLMES terminal or a suitable laptop computer for use at its own offices. Eventually, in May 2015, the MPS agreed to supply a terminal, at a cost of £26,278.31. In view of the cost, and the DMIP's (very mistaken) belief that it was nearing the end of its work, it declined the offer.

In January 2018, however, the DMIP submitted a new request for a HOLMES facility after further significant quantities of material had emerged. (This may have related to new and ongoing investigations which the DMIP was also reviewing.) But, in March 2018, it discovered that the estimated cost had risen to over £85,000. This included decommissioning the system when the inquiry finished and additional expenditure to connect the DMIP's offices to the MPS's new IT network. The DMIP considered the cost too high and asked again for a HOLMES laptop.

The DMIP's position on security measures

The MPS refused the request for a laptop computer, on the basis that there was inadequate security at the DMIP's offices. The DMIP reported:

"This was despite the fact that the Metropolitan Police had ... [previously] ... approved the Panel's facilities to store 'Secret' material securely in its offices."⁵⁰

The MPS then conducted a further site survey at the DMIP's request.

The DMIP received the survey in January 2019. The survey asked for "significant structural enhancements" before a HOLMES laptop could be provided for use in the DMIP's offices. The DMIP challenged the findings and the MPS agreed that the alterations would not be necessary. However, the DMIP decided not to pursue the matter any further.

The DMIP claimed that the situation changed because of the COVID-19 pandemic, when staff had to work from home. They said that the MPS then agreed that the DMIP's HOLMES expert could use an encrypted HOLMES laptop at his home. The MPS provided the laptop on 2 September 2020. Before then, any access to the HOLMES system had been at MPS premises, under MPS supervision. The Panel told us that this allowed the MPS to see whatever the DMIP was looking at.

⁵⁰ As before, vol 3, p 1,131, para 63.

The MPS's position on HOLMES

The MPS felt that they had an obligation to protect information held on the HOLMES system generally. And in Daniel Morgan's case, it was particularly important because of the status of the investigation and specific security concerns.

The MPS recognised the Daniel Morgan case was still a 'live' investigation and was anxious to ensure that the MPS did not prejudice any future proceedings through its disclosure of information. And it was concerned that the HOLMES account held information which, if released to the public, could put lives at risk.

In any event, the MPS was unclear as to why the DMIP considered access to HOLMES so important, as the MPS had provided all the HOLMES material in hard copy.

The MPS's position on practical difficulties

The MPS said that, in October 2013, it explained to the DMIP the practical difficulties in allowing access to the HOLMES database. The MPS also questioned the value of doing so. It said that only between 50 and 60 percent of the relevant material was on HOLMES and that a lot – particularly older material – had lost functionality when migrated from one database to another. The HOLMES accounts also contained a large volume of sensitive material, which had not been recorded in a single location on the system.

In any event, the MPS did not consider that formal agreement regarding the Panel's access to the HOLMES database could be reached while the DMIP did not have a Chair and – in the MPS's view – was not constituted.

The MPS's position on secret information

The MPS felt that the DMIP did not appreciate the difficulty involved in sanitising the HOLMES accounts to remove secret information. It also claimed that a HOLMES expert appointed by the DMIP later agreed that the accounts would have had to be rebuilt to restrict access to sensitive material.

The MPS's position on access at MPS premises

The MPS said that they had clarified the situation about access to HOLMES at MPS premises in a letter dated 30 December 2014. While access to premises needed to be supervised, access to the HOLMES accounts there would not be supervised by MPS staff. We consider this in more detail later.

The MPS's position on the laptop option

The MPS sought specialist advice about providing a laptop computer. It concluded that a laptop – which could easily be removed from DMIP premises – would not provide the necessary level of security. If material on the HOLMES system fell into the wrong hands, it would have had the potential to compromise the safety of a significant number of people.

The MPS claimed that the DMIP's own expert had agreed at the time that access to redacted material could not be provided securely on a laptop.

The MPS's position on the HOLMES terminal option

The MPS pointed out that the DMIP decided, in 2015 and 2019, not to install a HOLMES terminal at its own premises due to the cost.

When the DMIP rejected the HOLMES terminal option on the second occasion, the cost had risen by approximately £60,000. The MPS explained to us that the cost was out of its control. By then, the MPS had changed the way in which it provided HOLMES. Previously, HOLMES had been an independent system, but it had been transferred to an encrypted MPS network. Because of this, providing a terminal at DMIP premises would have required considerable additional work.

The MPS's position on the Cloud

The MPS said that advances in technology eventually allowed the MPS to safely change its position. As soon as the MPS was able to migrate accounts to the more secure Cloud system, it provided the DMIP with an encrypted HOLMES laptop. The MPS considered that any laptop usage of HOLMES before then would have presented an unacceptable security risk.

The MPS pointed out that the DMIP report seemed to indicate that the MPS changed its position about a laptop because of the pandemic. However, by then, the MPS had provided remote access to HOLMES on laptops for MPS personnel, as accounts had been migrated onto Cloud.

Our conclusions regarding HOLMES

There should never have been any doubt about allowing the DMIP access to the HOLMES database. Any argument that access wasn't necessary because all material was available in hard copy doesn't stand scrutiny. This was an inquiry into a murder case involving police corruption; for obvious reasons, the DMIP needed to compare HOLMES records with physical documents. The DMIP would have failed in its duty if it hadn't insisted on HOLMES access. The MPS should have recognised this and been more accommodating from the outset.

Our conclusions regarding security

That said, once the DMIP had been granted access, the argument about who, where and how they had access grew out of all proportion. There is a counter-argument which, on balance, we favour, that while access to HOLMES caused some delay, it wasn't a matter of the MPS being deliberately obstructive. Rather, it was because the MPS wanted to protect the security of its information and systems. This line of argument would conclude that the MPS sought to take the right decisions about security and to follow national guidelines on HOLMES use.

We discuss security more generally later in this chapter.

Our conclusions regarding access and supervision

We are satisfied that – eventually – the DMIP had proper access to HOLMES. We found that the DMIP’s HOLMES expert first accessed it in February 2015; this was soon after the disclosure protocol had been agreed. In total, he accessed it on 313 occasions; over 75 percent were during the years 2015 to 2017.

And we are not convinced that his use of the system was restricted in any way by MPS supervision. It is understandable that he was escorted when he visited MPS premises; when visiting police premises (in London and elsewhere), HMICFRS inspectors usually are too. However, that is not to say that his work was then closely monitored.

A way of possibly resolving the matter would have been if the DMIP had a laptop which was not connected to the HOLMES system. The DMIP persistently requested a laptop to access the database.

Had the DMIP been conducting only a retrospective inquiry, HOLMES material could – subject to any security issues – have been downloaded onto a laptop computer (before Cloud) and taken away. But it would have had a ‘data-cut’ at the time the material was downloaded onto it. In other words, it would only have provided a ‘snapshot’ in time. As soon as new material was created on the database, the DMIP’s download would have been out of date. The Panel would have needed to keep returning to the MPS for updates.

In any event, for security reasons the MPS declined to provide a laptop until technology (the Cloud) made it possible. In our view, it was right to do so. And, until then, the MPS’s policy of allowing access at its own premises accorded with the disclosure protocol.

Our conclusions regarding a HOLMES terminal

The MPS did, however, show some flexibility: it agreed to let the DMIP have a HOLMES terminal installed in its own offices. This option was costed on two occasions. On the first, it came to about £26,000, while on the second (some three years later) it had risen to approximately £86,000 because of IT changes. The DMIP declined on both occasions because of the expense.

With the benefit of hindsight, the first quote would seem to have been a particularly cost-effective option. The DMIP’s total cost, as reported on its [website](#), came to well over £16 million. (And we understand that does not consider expenses that other parties incurred in responding to DMIP requests.) The installation of a HOLMES terminal in 2015 would only have represented approximately 0.16 percent of the DMIP’s total cost.

Contacting serving and retired officers and staff

The DMIP's concerns

Early in the inquiry, the MPS issued a force-wide intranet appeal about requests for information from the DMIP. The Panel was concerned about the wording of the appeal. It did not make clear that anyone could approach the DMIP directly with information, rather than going through a force central point of contact. In the Panel's view, such a process might have deterred anyone who wanted to provide information in confidence.

On 17 December 2014, the Chair wrote to the MPS asking it to:

“make it clear to all Metropolitan Police officers and staff that it is open to them to contact the Panel directly and to provide it with any information they consider relevant, in confidence and without reference to the single point of contact or anyone else in the Metropolitan Police.”⁵¹

The MPS subsequently circulated a further force-wide intranet article to all personnel saying that they could contact the DMIP directly.

As part of the process for contacting those who had retired, the Panel wanted the MPS to send out sealed letters from the DMIP to the individuals concerned. The MPS agreed to do so but initially intended to enclose accompanying correspondence of its own, with information and advice for the intended recipients. The DMIP objected to what it considered to be “an attempt by the Metropolitan Police to interfere with the independence of the Panel and to warn off potential interviewees.”⁵²

The MPS withdrew its proposal about accompanying correspondence.

The MPS's position on contacting serving and retired officers and staff

The MPS's position was that the intranet appeal only asked personnel to notify the MPS's single point of contact for the DMIP about any requests for information, but did not require them to do so. The MPS considered this a sensible measure and one which it routinely used when dealing with other organisations. However, the MPS said that it acted immediately when the DMIP raised concerns and made clear to all personnel that they could approach the DMIP in confidence.

⁵¹ As before, vol 3, p 1,134, para 84.

⁵² As before, vol 3, p 1,135, para 87.

Our conclusions regarding contacting serving and retired officers and staff

The MPS issued the first intranet appeal on 3 December 2014, under the heading “Information requests on the Daniel Morgan murder”. The appeal stated:

“It is likely the Panel will require answers to many questions in order to complete their work; and they may therefore approach individuals or units seeking information.

To ensure we have a full record of these requests and any potential responses, the Met panel support team have been appointed to act as Single Point of Contact (SPOC) between us and the Panel.

Should you receive a request from the Panel please notify the Met panel support team”.

We agree that this created the impression that the MPS wanted to control, or otherwise interfere with, the DMIP’s contact with serving officers and police staff. We were particularly concerned that the MPS may have wanted to see, and collate, details of “potential responses”.

We have found a similar, guarded approach during our previous inspections of the MPS (and some other forces).

The DMIP’s accusation of withholding correspondence

The DMIP also reported that on 18 December 2014 it provided the MPS with letters for two former officers. The DMIP asked that the letters be delivered “in the New Year”. When the DMIP discovered that the letters had not been sent by 16 January 2015, it accused the MPS of the “deliberate withholding of correspondence” and said that it was “unacceptable and completely without justification”.⁵³

The MPS response about withholding correspondence

The MPS explained its process for forwarding letters on behalf of the DMIP. In the first instance, the disclosure team had to contact the DPS to obtain an identity (‘warrant’) number for the individuals concerned. (The third-party pension providers needed the warrant numbers to determine whether they were still in receipt of pensions.) If the pension providers were able to identify the individuals, they provided the MPS with their last known addresses.

However, problems could still arise if those concerned hadn’t informed the pension providers of a change of address (they would still have received their pensions, which were paid into their bank accounts). Therefore, the disclosure team conducted any other further checks which they considered reasonable before forwarding the letters.

⁵³ As before, vol 3, p 1,135, para 89.

The MPS denied any suggestion that they had tried to withhold correspondence on the occasion referred to in the DMIP report. They told us during our inspection that the DMIP provided the letters on the Thursday before a Christmas and New Year holiday period. The MPS then had to make enquiries with – and wait for responses from – the MPS’s pension providers. The letters were sent out in January 2015.

Our conclusion about withholding correspondence

MPS records show that the two letters in question, which the DMIP accused the MPS of “withholding”, were the first to be sent on the DMIP’s behalf. We saw an accompanying letter, dated 11 December 2014, which the DMIP sent to the MPS with the sealed letters. It did not suggest that there was any urgency in forwarding them to the intended recipients: it only requested that they be delivered “*after* [our emphasis] the New Year”. (The DMIP stated in its report that it asked for the sealed letters to be delivered “*in* the New Year”.)

The envelope containing all three letters (that is, the two sealed letters and the accompanying letter), was date stamped 15 December 2014. Although it was then the busy Christmas postal period, the DMIP sent the letters to the MPS by second class mail. Nevertheless, the MPS accepted that they received them immediately before the holiday period, although they could not provide a precise date.

We were unable to establish the exact date when the MPS approached the pension providers on this occasion; nor could we establish how long it took for the pension providers to reply. However, we do know from a Post Office recorded delivery receipt that the sealed letters were sent to the intended recipients on 19 January 2015.

We acknowledge that, without adequate explanation, the DMIP may have become frustrated by a delay in sending the letters (wherever the blame lay). However, we consider it unduly harsh to intimate that the MPS had in some way adopted underhand tactics to frustrate the inquiry.

9. Other Panel-related matters

We briefly include here further matters which we believe are significant and worthy of consideration. They relate to MPS governance and resourcing, security, discrepancies between the Panel's report and MPS records, and the length of the inquiry.

MPS governance and resourcing

The MPS established a disclosure team to assist the DMIP. It was only ever a small team and it is to the credit of those involved that they completed so much work.

Governance

At the outset, the MPS also introduced a strategic oversight group. It was led by an assistant commissioner (latterly the Commissioner) and included other senior officers. But we found a lack of continuity when they moved to different roles.

We were unable to find any evidence that the oversight group met between 2015 and 2019. During that period, another assistant commissioner had taken charge of the group when the initial officer of that rank temporarily left the force. Meetings resumed in 2019, when a third assistant commissioner, supported by a commander who had no previous involvement with the DMIP, assumed responsibility.

Resourcing: a “one-man band”

When the new assistant commissioner and commander took responsibility in 2019, they reviewed the situation. They found that the disclosure team was “under-powered” and virtually a “one-man band”. They discussed matters with the Panel, who were frustrated. The DMIP felt the MPS's team was under-resourced too, and that its only member was also the MPS's chief decision maker on Panel-related matters.

The assistant commissioner and commander recognised that the lead disclosure officer had been involved with the case for a long time. They also saw that, as the inquiry was moving into a crucial phase and towards publication, he needed more support.

On 26 June 2019, the assistant commissioner wrote to the Chair and said that he intended to appoint a senior officer to provide oversight and an independent view. He subsequently introduced a detective chief inspector (now detective superintendent) and a sergeant to the team. Panel members told us that the situation then started to improve.

Our conclusion

We reported earlier that the MPS did not contribute more staff to assist with transporting sensitive material. Collectively, the governance and resourcing problems provide a strong indication that the MPS's practical commitment to supporting the inquiry was not as great as it should have been.

Security

The MPS was reluctant to allow the Panel to see everything it wanted in the way it wanted. This is demonstrated especially by the MPS's approach to HOLMES and sensitive material. The MPS based its case on security concerns. For its part, the DMIP made clear that it was well aware of both parties' obligations in that regard:

"Both the Panel and the Metropolitan Police had a duty to ensure that the material disclosed to the Panel was treated appropriately at all times, and that no harm to individuals potentially at risk should occur as a result of disclosure to the Panel. The Panel was, and has continued to be, fully aware of the security implications of its work and has done everything in its power to ensure the safe handling of all the information disclosed."⁵⁴

The DMIP also pointed out that the panel and all its staff had signed confidentiality agreements, and reported that the physical security measures it had introduced were sound:

"The Panel's offices had met all Government security requirements and had been assessed by the Metropolitan Police prior to the Panel commencing its work. Enhanced security provision required by the Metropolitan Police had been installed."⁵⁵

But security is about much more than just a lock and key; the right procedures need to be in place and robustly applied. We found some apparent justification for the MPS's concerns, even though we recognise that visits to East London to view unredacted material were inconvenient for the Panel.

The courier

According to the MPS, in October 2014, the DMIP sent a courier to collect the first batch of crates from the MPS's premises in East London. The box-loggers had finished cataloguing their contents and the material was then ready for scanning onto the DMIP's system.

The MPS informed us that the courier arrived at 11am on 2 October 2014 and produced his driving licence for identification purposes. The MPS conducted a security check on the Police National Computer (PNC). They found that the courier had six criminal convictions, including offences of dishonesty and involving weapons. The MPS refused to let him take the material away unaccompanied. However, to save embarrassment and prevent delay, the MPS released the material under the supervision of a Home Office member of staff, who escorted the courier.

⁵⁴ As before, vol 3, p 1,122, para 24.

⁵⁵ As before, vol 3, p 1,130, para 60.

Thereafter, the DMIP provided details of couriers in advance. While there were no further incidents of this nature, the MPS may have understandably felt that its general security concerns were justified.

Material not returned to the MPS

In some instances, the MPS provided the DMIP with material for temporary retention and use at the DMIP's offices. This was generally additional material which the DMIP had asked for relating to police procedures. It also included some sensitive material. The MPS provided such material on the understanding that it would be held securely and returned in due course.

On 17 August 2021, the DMIP informed the MPS by email that it was only able to return 49 out of 60 items that were due to be collected on that occasion. The email stated that "nine of the items were shredded by mistake"; it was unclear from the email what became of the other two.

The email did not contain much detail about the missing items. One was referred to as a "Folder of various DMIP queries". It was only after checking its own systems that the MPS determined what was missing. The MPS told us that there were 42 separate items.

This example – although it took place after the Panel had reported – illustrates why the MPS may have had concerns about the DMIP's security arrangements and about the reliability of its record keeping.

MPS security vetting

We found that the MPS wasn't infallible either when it came to security.

The DMIP was never content with the MPS's approach to redacting sensitive material. It considered that the situation was "severely aggravated" because the member of MPS staff who generally made redaction decisions (the lead disclosure officer) did not have appropriate security clearance. All the DMIP's staff, on the other hand, had appropriate security clearance. When the DMIP discovered this, which was late into the inquiry, the DMIP arranged for the Home Office to complete the lead disclosure officer's security clearance as soon as possible.

Although the individual concerned probably had a better knowledge of the case and all the material than anyone else in the force, the MPS accepted that his lack of appropriate vetting should not have happened. We agree. The MPS attributed it to "an oversight".

We raised concerns about MPS vetting in our [2018/19 MPS PEEL report](#). We were particularly concerned about the backlog of staff who needed vetting then. We discuss these issues in more detail in a later chapter of this report.

Discrepancies

We found some discrepancies between the DMIP report and the MPS's records. We provide some examples here.

Access to material

The DMIP reported several times that material was not made available to the Panel until January 2015. For example:

- “The Morgan One Investigation papers, and access to the data from the MICA computer system, were not made available to the Panel until January 2015, some 16 months after the start of the Panel’s work.”⁵⁶
- “The Panel had started to receive documents only in January 2015.”⁵⁷

We accept that the release of material was delayed because of disagreements over the disclosure protocol, and that the Panel might not have received material in the format it required until January 2015.

The MPS’s records show that the force supplied the DMIP’s legal representatives with 125 crates of material – ready for scanning – before the end of 2014. The DMIP’s box-loggers had been cataloguing and preparing the material for scanning since October 2013.

MPS records show that, on 17 December 2014, the disclosure team asked the DMIP’s legal representatives how much scanning they had then completed; the response was 131,223 pages.

In addition, the MPS records show that the force had provided the Panel with initial reading material on 18 December 2013; we have seen a dated and signed receipt. We noted, however, that the DMIP variously reported that it received that initial material in December 2013⁵⁸ and December 2014.⁵⁹

When the DMIP started work

The Panel said that it was unable to start “properly” until the end of 2015. The DMIP reported that it received the first material, in the format it wanted, early in 2015:

“The Panel received its first documentation, digitised and accessible on Lextranet, in January 2015.”⁶⁰

As the DMIP considered the material which it received, it made requests for the disclosure of additional material:

“Once the Panel was able to start looking at and understanding the contents of the material disclosed to it by the Metropolitan Police, it began to make necessary requests for additional disclosure of documents and other material relevant to its Terms of Reference.”⁶¹

⁵⁶ As before, vol 1, p 65, para 193.

⁵⁷ As before, vol 1, p 303, para 10.

⁵⁸ As before, vol 3, p 1,120, para 14.

⁵⁹ As before, vol 3, p 1,134, para 83.

⁶⁰ As before, vol 3, p 1,122, para 21.

⁶¹ As before, vol 3, p 1,123, para 26.

The Panel went on to say:

“By 13 May 2015, the Panel had already submitted 63 Additional Disclosure and Information Requests, which required cooperation from a range of different departments in the Metropolitan Police.”⁶²

We have seen MPS records which show that, by 13 May 2015, the DMIP had submitted 163 requests for additional documents and information.

December 2015

However, slightly earlier in its report, the DMIP stated that it could not start work properly until December 2015. (By that time, the MPS had provided all the non-sensitive material in 19 batches of crates.) The DMIP attributed the delay to difficulties in agreeing the protocol:

“the Panel considers it was neither necessary nor proportionate for the processes for disclosure and document handling to have taken such a long time to be agreed with the Metropolitan Police. The Panel, having been announced by the Home Secretary in May 2013, did not have access to all the initial documentation, and thus was unable to commence its work properly, until December 2015.”⁶³

However, the receipt of material in January 2015, and the requests for additional documentation arising from the Panel’s assessment of it, indicated that the Panel started work some time before December 2015.

Decision logs

In volume one of its report, the DMIP stated that it was unable to find material for a particular operation:

“The Panel has been unable to locate any formal Terms of Reference, strategy documents or a policy log for Operation Nigeria/Two Bridges among the documentation available to it.”⁶⁴

However, in volume three of the report, the DMIP seemed to refer to the material which it had said it was unable to find. In doing so, the DMIP quoted from it:

“[The] policy files/decision logs relating to Operation Nigeria/Two Bridges refer to the reasons for the large number of offences still to be investigated”.⁶⁵

⁶² As before, vol 3, p 1,123, para 27.

⁶³ As before, vol 3, p 1,122, para 24.

⁶⁴ As before, vol 1, p 421, para 8.

⁶⁵ As before, vol 3, p 1,081, para 344

The length of the inquiry

When the Home Secretary announced on 10 May 2013 that the Panel was to be established, Daniel Morgan’s family had already waited over 26 years for answers. The DMIP adopted the principle of “family first”, which was “fundamental”⁶⁶ to the Panel’s approach; it was incorporated in the Panel’s terms of reference.⁶⁷

The DMIP’s primary explanations for delay

The DMIP has largely attributed the delay in completing its own inquiry to the MPS’s lack of co-operation. It was highly critical of the MPS throughout its report; we provide a selection of its comments:

“The publication of the Panel’s Report was significantly delayed for a number of reasons, including the difficulties experienced with the Metropolitan Police”.⁶⁸

“The Panel experienced very significant delays because of the difficulties of securing agreement to disclosure by the Metropolitan Police.”⁶⁹

“The Panel would have been greatly helped in its work preparing this Report and would have been able to complete its Report much sooner, had it had access to the HOLMES system in its own offices from September 2013.”⁷⁰

“on each occasion on which a Panel member needed to access information classified as ‘Secret’, a lengthy journey to Metropolitan Police premises situated on the outskirts of East London was required. This caused considerable delay.”⁷¹

“The Panel concluded eventually that it would have to continue with the existing arrangements of viewing sensitive documents at the Metropolitan Police premises in East London. This was far from satisfactory, and significant time continued to be wasted.”⁷²

Our terms of reference

Our second term of reference required us to assess whether the MPS responded appropriately to the Panel’s requests for disclosure and access to material. Therefore, we have considered the DMIP’s criticism of the MPS and the evidence on which that criticism is based.

Our conclusions

We have acknowledged elsewhere in this report that the MPS should not have attempted to prevent all the Panel members from seeing all unredacted material, and that the Panel’s access to HOLMES should not have been in doubt. However, we are satisfied that, ultimately, the DMIP wasn’t refused access to anything.

⁶⁶ As before, vol 3, p 1,236, paras 5 and 6

⁶⁷ As before, vol 3, p 1,235.

⁶⁸ As before, vol 1, p 13, para 78.

⁶⁹ As before, vol 1, p 14, para 79.

⁷⁰ As before, vol 3, p 1,132, para 70.

⁷¹ As before, vol 3, p 1,114, para 493.

⁷² As before, vol 3, p 1,136, para 92.

We find it difficult to understand why matters relating to the disclosure protocol, travelling to East London to view sensitive material, and access to HOLMES would – either individually or collectively – have extended the inquiry for seven years beyond an initial estimate of one year.

Potential reasons for the length of the inquiry

And so, we turn to other potential reasons for why the inquiry took so long. We consider there are two principal reasons: the DMIP’s terms of reference, and the volume of material. We assess each in turn.

The scope of the DMIP’s inquiry

We concluded that the main reason for the length of the inquiry was the scope of the DMIP’s inquiry, as defined in its terms of reference.

The terms of reference acknowledged that corruption had blighted the investigation. They directed the Panel to review its effect on that case:

“the Government is committed through the work of the Independent Panel to a full and effective review of corruption as it affected the handling of this case and of the treatment of the family by the police and other parts of the criminal justice system.”

More specifically, the Panel was asked to address questions relating to:

- “police involvement in the murder;
- the role played by police corruption in protecting those responsible for the murder from being brought to justice and the failure to confront that corruption; and
- the incidence of connections between private investigators, police officers and journalists at the News of the World and other parts of the media and alleged corruption involved in the linkages between them.”

Although not explicit, we consider that the reference to private investigators, journalists and the media generally related to their involvement in the Daniel Morgan case. The bullet point sat immediately below two others which were clearly directed at that investigation and no other, and followed a statement in the terms of reference about the Panel’s remit and purpose:

“The purpose and remit of the Independent Panel is to shine a light on the circumstances of Daniel Morgan’s murder, its background and the handling of the case over the whole period since March 1987.”⁷³

The Panel seemed to accept that its requirement to review the involvement of private investigators and the media was to be restricted to the Daniel Morgan case:

“The Terms of Reference have been interpreted as requiring the Panel to examine:

- whether or not there was any police involvement in the murder itself;
- whether there was any police corruption affecting the investigation of the murder and making it impossible to bring whoever was responsible to justice; and

⁷³ As before, vol 3, p 1,234.

- in the context of the murder and its investigation, what was the incidence of connections among private investigators, police officers and the media, and whether or not there was, as alleged, corruption in the linkages.”⁷⁴

Furthermore, the DMIP went on to say:

“It is not part of the Panel’s remit to examine corruption within the Metropolitan Police generally during the period in question but rather to focus on addressing specific issues related to it and to Daniel Morgan’s murder.”⁷⁵

However, having examined potential corruption during the various murder investigations, the Panel went on to consider other investigations into corruption, which “had not yet begun when the Panel was established”⁷⁶ in 2013. The DMIP set out its involvement:

“The Panel’s Report examines the sequence of events and issues arising before and after the murder and explores the allegations against different individuals who are said to have been involved. It considers all the investigations of the murder and linked investigations into corruption from 1987, including associated disciplinary and criminal investigations, the most recent of which ended in 2020.”⁷⁷

Therefore, in effect, rather than ‘drawing a line’ and looking back at events over the previous 26 years, the DMIP’s work was concurrent with ongoing MPS and IOPC corruption investigations. As the Panel reported, this meant that “the final documents were not received from the Metropolitan Police until March 2021”.⁷⁸

The Panel seemed to recognise that its approach greatly increased the duration of the inquiry but felt it was justified:

“The complexity and length of these investigations was not anticipated in 2013. It was necessary to examine them in order to fulfil the Panel’s Terms of Reference. The Panel could not properly complete its work and make its report to the Home Secretary while this was ongoing.”⁷⁹

The volume of material

Undoubtedly, the volume of material also contributed to the length of the inquiry. At the outset, it filled almost 600 crates. But, even after an assessment by two independent technology consultants appointed by the Home Office, the terms of reference stated:

“It is envisaged that the Panel will aim to complete its work within 12 months of the documentation being made available.”⁸⁰

⁷⁴ As before, vol 3, p 1,018, para 17.

⁷⁵ As before, vol 3, p 1,023, para 42.

⁷⁶ As before, vol 1, p 12, para 67.

⁷⁷ As before, vol 1, p 12, para 66.

⁷⁸ As before, vol 1, p 13, para 77.

⁷⁹ As before, vol 1, p 12, para 67.

⁸⁰ As before, vol 3, p 1,235.

We don't consider that was ever a realistic proposition. The DMIP appeared to agree and made a recommendation accordingly:

“Prior to the establishment of any future non-statutory inquiries or panel, there should be an honest and full discussion between the relevant police force(s) and the sponsoring Government department, to enable a realistic, informed assessment of the nature and volume of documentation in all its forms, and of the scope and depth of the work required. Framework procedures, capable of being customised, for the disclosure of material to such panels should be available, so as to avoid excessive delays in reaching agreement for access to material. Deadlines should only be established when the relevant inquiry or panel has had the opportunity to review the programme of work it is required to do. Any such deadline should be supported with an analysis explaining how the projected deadline has been identified, and why that is a reasonable time within which the work should be completed.”⁸¹

Despite the obvious amount of material, it is perhaps understandable that the task at hand was underestimated at the outset. But the potential timeframe might have become more apparent as time progressed. However, we found that when the DMIP considered the MPS's offer of a HOLMES terminal in 2015, the Panel told the MPS (in an email dated 8 October 2015): “We are to have completed our work by July next year.”

In January 2018, the DMIP realised that its “decision not to pursue the installation of a HOLMES terminal was premature”.⁸² This was because “significant new information and voluminous material about the investigations into the murder of Daniel Morgan continued to come to light”. Much of the material may have related to the ongoing investigations which the DMIP reviewed.

⁸¹ As before, vol 3, p 1,118, para 3.

⁸² As before, vol 3, p 1,130, para 62.

10. Vetting – an important line of defence against corruption

Vetting is required for anyone who wishes to become a police officer, a member of police staff or a volunteer. It is also used to ensure that those who have access to police equipment, information and premises through their job, such as contractors, have a suitable background and history. Checks carried out as part of the vetting process assist in establishing whether a person, their family or associates has a criminal background, whether they lack honesty and integrity or whether they are financially vulnerable.

The risk of criminal infiltration into policing is very real. Police information is an extremely valuable commodity to criminals. If an organised crime group can gain access to police buildings, equipment and information systems they can have almost unfettered access to the details of police operations and intelligence; it significantly improves their ability to commit crime and evade detection. Vetting is designed to minimise this and other risks.

In 2017, both the statutory *Vetting Code of Practice* and APP for vetting were introduced. The *Vetting Code of Practice* sets out the important principles of vetting and how they should be implemented. The APP sets out the necessary technical processes and procedures involved in vetting. The APP was updated in 2021. Together, these two documents aim to bring consistency to the application of vetting standards across forces.

Vetting decisions – either to accept or reject an applicant – can only be based on the information available to the vetting team at the time they perform the relevant checks; they are made at a snapshot in time. But individuals' circumstances change in ways that can affect their suitability to work in or alongside a police force. An effective vetting process should identify these changes and ensure they remain suitable to be employed by or work with police forces.

The different levels of vetting

Forces vet officers and staff to different levels depending on their role. The minimum level of force vetting required before they can join the police service is called 'recruitment vetting' (RV). Some roles need a higher level of vetting due to the postholders' access to more sensitive information. This is called 'management vetting' (MV).

The Vetting APP sets out the minimum checks and enquiries expected for each of these vetting levels. A list of these can be found at [Annex A](#).

Renewing vetting clearance

A person's vetting must be renewed periodically to ensure they are still suitable to work in policing. A full application must be completed for a person's vetting to be renewed and all the required checks must be completed again.

The APP states that vetting should be renewed every seven years for MV and ten years for RV. However, significant changes can occur in an individual's personal circumstances during this time. There is an onus on the individual to notify the force vetting unit (FVU) of any changes to their personal circumstances.

Vetting of transferees

APP sets out the process for the vetting of officers who want to transfer between forces. In cases where an officer seeking to transfer has been vetted within the previous year, it allows for the vetting clearance to be transferred to the receiving force. In such cases, the full vetting file should be passed to the receiving force. In all other cases, the APP requires a full re-vet before a decision is made whether to allow the officer to transfer.

The APP states that, in either case, the receiving force must request and review the full complaint and misconduct history and any counter-corruption intelligence from the parent force and from any other forces where they have served.

We believe individuals who transfer between forces should be fully re-vetted before acceptance. This is for the following reasons:

- officers' personal circumstances can change a lot in 12 months; their vetting clearance may no longer be appropriate; and
- there is a minimal difference between the time it takes to review a vetting file, compared with the time it takes to re-vet an individual.

We will comment on the vetting of transferees in more detail in our forthcoming thematic report.

The MPS vetting process for recruits

Once a candidate has passed the MPS recruitment selection process, the FVU undertakes a series of vetting checks (see [Annex A](#)). Vetting officers carry out these checks and make recommendations to the senior vetting officer (SVO), who makes the final decision as to whether clearance should be granted.

The MPS reports a massive reduction in the number of unvetted personnel

At the time of our [previous vetting inspection](#), in December 2018, we established that the force had approximately 16,000 personnel (about 37 percent of its entire workforce) who had either never been vetted or whose vetting had expired. We raised concerns about this and the force's management and understanding of the vetting status of the workforce.

During this inspection, the MPS reported that, as at 7 September 2021, its number of unvetted personnel stood at only 671. The force told us it had achieved such a massive reduction by increasing resourcing levels in the vetting unit and improving its working practices. This seems highly encouraging. We congratulate the force on its progress.

Data accuracy and the links between HR and vetting records need to improve

Although the MPS has approximately 44,000 personnel, the vetting database has over 61,000 records of personnel with current vetting. The MPS told us this was due to the presence of many duplicate records, which doesn't inspire confidence in the accuracy and reliability of the process. In response to our finding, the MPS said: "This is an IT system functionality matter, not a process accuracy and reliability shortcoming."

However, we understand that the MPS is preparing to implement a new vetting system. We were told that it should:

- link in with the HR system;
- remove duplicate records; and
- provide managers with improved information about the vetting of the workforce.

Review of vetting files against the APP's checklist

We reviewed 40 vetting files to see if the checks recommended by the APP had been completed. These checks are listed in [Annex A](#). We found that, in every case, they conducted all the necessary checks required by the Vetting APP.

Our inspection focused on whether the checks were being completed, not how the MPS interpreted the information obtained from them, and not whether the APP's recommended checks are sufficient. We will explore this latter point in our forthcoming thematic report.

Personnel in sensitive posts might not have enhanced vetting

The MPS told us that, in December 2020, they compiled a list of designated posts that needed an enhanced level of vetting. There are approximately 4,200 such posts on the MPS's list. These posts include child protection, major crime investigation, informant handling, and counter-corruption investigation. But the force couldn't tell us whether everyone in these posts had been vetted to the MV level.

The force's HR data shows the current location where someone is based but not the post they occupy. Therefore, the FVU was unable to say who occupied the designated posts and their current level of vetting. Until the new system is fully functional, the limitations in the current arrangements strike us as unprofessional. They create obvious risks. The MPS's practice is contrary to the Vetting APP's requirements on vetting for sensitive posts. It is not what we would expect to see in any police force that has fully effective and well-integrated vetting and HR functions.

This is not a new finding. In 2017 our national report [PEEL: Police legitimacy 2016](#) contained the following cause of concern:

“HMIC is concerned that some forces are failing to comply with current national vetting policy. This means that these forces are employing individuals who have not undergone even basic vetting checks, which represents a significant risk to the integrity of the organisation.”

To address this cause of concern we made the following recommendation:

- “Within six months, all forces not already complying with current national vetting policy should have started to implement a sufficient plan to do so; and
- Within two years, all members of the police workforce should have received at least the lowest level of vetting clearance for their roles.”

In our [2019 inspection report on the MPS](#), we made the following recommendation:

“The force should undertake work to ensure it fully understands the vetting status of staff where their current vetting status is currently unknown and vet staff who do not have current vetting. It should ensure that it has appropriate central governance over the number of staff who require enhanced vetting and re-vetting.”

In the same year we published our [Shining a light on betrayal](#) national report where we recommended:

“All forces that are not yet doing so should immediately comply with all elements of the national guidance on vetting. By July 2020, all forces that haven’t yet done so should vet all personnel to the appropriate standard. Forces should also have a clear understanding of the level of vetting required for all posts, and the level of vetting held by all their officers and staff. Forces should make sure all personnel have been vetted to a high enough level for the posts they hold.”

There are approximately 660 more personnel with enhanced vetting than there are sensitive posts that require it

As of 10 September 2021, the number of MPS personnel who had an enhanced level of vetting was 4,860. The MPS told us that the higher number of personnel with enhanced vetting than designated posts is because a person’s enhanced vetting isn’t automatically cancelled when they are no longer in these posts. They may therefore have two current vetting clearances, such as RV and MV.

Based on our findings in 2021, it is clear that the MPS has more to do. It is encouraging that the force has compiled the list of designated posts. But our findings are not reassuring – even after a specific recommendation three years ago – the force does not know whether those who occupy these posts have been vetted to MV level.

Recommendation 3

By 31 March 2023, the MPS should establish and begin operation of a process to:

- determine the vetting status of all personnel in designated posts; and as soon as possible thereafter;
- ensure that all designated postholders are vetted to the enhanced (management vetting) level; and
- provide continued assurance that designated postholders always have the requisite vetting level.

Operation Fortress and warrant cards

We found that the MPS has recently introduced Operation Fortress. This involves access to police buildings and systems being controlled through personal issue 'chipped' warrant cards. These are linked to the individual's vetting; their access rights expire at the same time as their vetting clearance. When an individual is approaching the expiry date of their vetting clearance, they are required to reapply. Should they fail to do this, there is an escalation process through their line managers and access to buildings and IT systems can be cancelled. This appears to be an excellent initiative which, in due course, should help to ensure that everyone in the MPS has current vetting clearance. It is proving highly effective in improving the timeliness of vetting renewals.

However, one worrying aspect that we heard was the MPS's apparent failure to retrieve warrant cards from some officers who had left the force. We were informed that approximately 2,000 such warrant cards are unaccounted for. This presents a significant operational security risk to the force. Furthermore, there are many examples (including one later in this report) of warrant card misuse, which may adversely affect public safety and confidence in policing. For that reason, if no other, we would have expected to see much greater concern and action to recover these warrant cards.

The Vetting APP is open to interpretation

Officers and staff are expected to "have regard to APP in discharging their responsibilities".⁸³

The Vetting APP states it should "form the basis of all vetting activity, including decision making".⁸⁴

When assessing the suitability of applicants, APP does not give a list of convictions or cautions that should lead to a vetting rejection.

⁸³ [About us: What is APP?](#), College of Policing, 26 January 2018.

⁸⁴ [APP on Vetting 2021](#), College of Policing, 25 March 2021, p 63.

“Each case must be considered on its own individual merits in relation to the role being undertaken and the assets being accessed, subject to the rejection criteria highlighted below.”⁸⁵

There are two clear rejection criteria:

- cases where an adult or juvenile committed an offence that resulted in a prison sentence, including suspended sentences: and
- where the applicant is or has been a registered sex offender or is subject to a registration requirement in respect of any other offence.

The APP states that offences where vulnerable people are targeted, offences motivated by hate or discrimination and offences of domestic abuse should result in rejection. It also contains a ‘rebuttable presumption’ that applicants to become a police officer who have other convictions and cautions should be rejected.

APP goes on to say that there should be a risk-based assessment of convictions and cautions which should consider circumstances such as the:

- seriousness of the offence;
- level of the applicant’s involvement in the offence;
- motivation leading to the offence;
- openness of the applicant;
- level of clearance required;
- length of time since the offence;
- presence of repeat offending;
- effect on public confidence in the police service;
- nature of the role applied for; and
- applicant’s behaviour since the conviction or caution.

This section of APP appears to give forces considerable latitude to set their own standards, in relation to the level of risk they are willing to accept when deciding on the suitability of applicants to become officers. This level of subjectivity brings with it an inevitability that decisions made by forces are not consistent.

As previously stated, we will comment on the Vetting APP in more detail in our forthcoming thematic report.

The vetting panel reviews all cases where vetting is refused

We were told the MPS reviews any vetting refusals and appeals at a monthly vetting panel (VP). The panel consists of representatives from the FVU, DPS, HR, staff associations, independent advisory group, and other community groups.

A commander, who is independent of the vetting process, chairs the panel. All cases are anonymised prior to the panel’s review. The VP considers each case on its merits and either ratifies the refusal, recommends the refusal is changed to a clearance, or asks the FVU to interview the applicant to obtain more information.

⁸⁵ As above, p 64.

If the VP recommends that a decision to refuse vetting is overturned, the rationale is communicated to the staff in the FVU. Regularly, we heard that this rationale amounted to the force's 'risk appetite'.

Risk appetite

Although there were few cases in which there was a recommendation to overturn, these cases may have a wider impact. We believe, the FVU – understandably – takes account of the VP's rationale when making decisions on subsequent cases. However, the FVU continues to assess each case on its own merits.

We examined the records from the VP meetings that were held in July, August and September 2021. In total, there were 57 cases heard at these meetings. Of these, the VP upheld the decision to refuse vetting clearance for 42 of the cases. They recommended that three refusals should be changed to clearances. For the remaining cases they either recommended a vetting interview is held to obtain further information, or they were waiting for further information.

In the Vetting APP, there is nothing specific on the use of vetting panels, and the Vetting APP certainly doesn't preclude their use. Nevertheless, based on our findings, we have concerns about the MPS's interpretation of the Vetting APP and that the force may have lowered its vetting clearance thresholds based on a heightened risk appetite. In other words, the Vetting APP provides scope for the MPS (and other forces) to lower the standards: too widely; too readily; and too far.

At least one senior officer told us that there is pressure to clear applicants so they can be recruited into the organisation. To us, this appeared to be an attempt to meet recruitment targets, but with insufficient focus on the inherent risks associated with clearing candidates whose backgrounds should present concerns.

Tension between recruitment and vetting objectives

We conclude that there is tension between HR objectives to meet recruitment targets and the FVU objectives to admit only those with sufficiently high levels of integrity.

We can see the benefits of the VP in achieving consistency of decision-making in borderline cases and in setting an appropriate level of risk in relation to vetting standards. However, the MPS's operation of the VP, its composition and potential (if not actual) effect on the FVU's decision-making, comes dangerously close to contravening the *Vetting Code of Practice*:

“Decision-making in respect of vetting clearance should be separate from, and independent of, recruitment and other human resources processes.”⁸⁶

In this context, we believe that the Code's reference to “decision-making” isn't just about the vetting decision in individual cases.

We will comment on the Vetting APP and code of practice in more detail in our forthcoming thematic report.

⁸⁶ [Vetting Code of Practice](#), College of Policing, 12 October 2017, p 13.

Managing the risk

Factors that may lead to forces wishing to manage some personnel who have passed vetting, but give cause for some concerns, fall into three broad categories:

- the integrity of the individual (for example, their previous criminal history);
- the integrity of close associates of the applicant (for example, their criminal history and/or intelligence on family members);⁸⁷ and
- other vulnerabilities (for example financial difficulties).

For cases where one or more of these factors is present, the Vetting APP states:

“consideration must be given to the risk that this information poses to the force, the individual and the public. Forces must consider these cases on their individual merits and take into account:

- the likelihood that the applicant’s performance of duty may be adversely affected, for example, through adverse pressure or a conflict of interests;
- the nature, number and seriousness of the offences or involvement in criminal activity, as well as the time period over which these took place;
- the likelihood of damage to the force’s operational capability;
- the potential for information leakage; and
- whether the circumstances are likely to bring discredit to, or embarrass, the police service or police force.”

In accepting that some recruits may pose a risk to the organisation, whether through previous convictions or declarable associations, the MPS should manage the risk.

Risk mitigation

The Vetting APP states that:

“Where a decision is made to grant clearance following assessment of identified potential risk, a risk mitigation strategy must be considered to determine whether clearance can be granted with reasonable, proportionate, measurable and manageable mitigations in place.”

The MPS’s approach to risk mitigation

In early 2021, the DPS conducted a PNC check of the entire workforce. It revealed that approximately 350 members of the workforce had a variety of offences recorded against them, including criminal convictions.

Of these, 205 were police officers. In the vast majority of cases, they committed their offences before joining the MPS. In three cases, officers had committed offences whilst serving with the force. The FVU hadn’t informed the DPS about many of the 205 cases. The DPS is the department where most, if not all, mitigation measures would be instigated.

⁸⁷ In the MPS these are referred to as ‘disclosable associations’.

We asked the FVU how many other officers and staff had been recruited with other items of adverse information, such as family members with criminal links, over the last three years. They were unable to answer this question. To do so would have required a review of approximately 18,000 vetting files.

After the PNC checks revealed information on personnel that the DPS was unaware of, the FVU started to provide the DPS with details of all new recruits with an identified risk. Prior to early 2021, the decision whether to pass on these details was based on the FVU's professional judgment. Therefore, there are officers with an identified risk who have not been appropriately assessed by the DPS. This is unprofessional: opportunities have been lost to put mitigation measures in place to prevent corruption.

The types of mitigation measures forces may use include: restrictions on where officers can work; restrictions on the types of roles they can undertake; limitations on systems access; monitoring of their systems access; placing them under greater levels of supervision; and regular reviews. We found that the MPS did not have sufficiently well-established and robust processes to implement such measures. This is not what we would expect to see in a well-run force.

Since the APP's introduction, there has been an increase in the number of MPS recruits with convictions and cautions

We established that, since 2018, there has been an increase in the number of people recruited with prior recordable offences. This coincided with the implementation of the Vetting APP and increases in recruitment under the police's [uplift programme](#). In 2018, the MPS recruited 12 police officers with prior recordable offences. In 2019, the number increased to 56. In 2020, it was 53.

Some of these offences were relatively trivial but many were not. They included handling stolen goods, drink driving, possession of controlled drugs, assault, and theft. Most of these cases were dealt with by way of cautions, fixed penalty notices, fines, and disqualifications from driving.

Because of limitations in the way in which its records are configured, the MPS was unable to tell us how many personnel with a declarable association had joined since 2018. The combination of recruits with recordable offences, those with declarable associations, and the DPS not having been made aware of these, paints a worrying picture.

There is, first, the question of whether the MPS has set its risk appetite at the right level. Second, we are far from assured that the vetting process is sufficiently effective in assuring the trustworthiness and reliability of new recruits. And third, it is clear to us that the DPS does not have anything approaching a satisfactory understanding of the risk posed by some of the MPS's officers and staff.

We will explore some of these matters in more detail in our thematic inspection of police vetting and counter-corruption arrangements in England and Wales.

Quality assurance processes in the FVU are good

We are pleased to see that the FVU is taking steps to promote learning and continuous improvement within the team. We were told that the FVU dip-checks 5 percent of vetting cases to see whether the enquiries have been carried out appropriately. Feedback is then given to the vetting officers involved in these cases. This is good practice.

Vetting for transferees to the MPS

We checked ten vetting files for officers who applied to transfer to the MPS. We found that all the vetting checks for these applications were carried out in accordance with the Vetting APP. We also found examples of vetting being refused for transferees based on information provided to the FVU by the officer's home force.

Given the public concerns raised by the murder of Sarah Everard by a serving police officer who was a transferee into the MPS, we will examine the arrangements for vetting of transferees in more depth during our thematic inspection.

Changes in circumstances are not being reported

MPS personnel are required to report any change in their circumstances to the FVU. The Vetting APP states:

“Vetting is based on a snapshot in time. Because an individual's circumstances can change, it is important that their ability to maintain their security clearance is assessed. A comprehensive aftercare regime allows such assessments to be made. Aftercare is therefore an important part of any vetting process and is the responsibility of both the vetting subject and the FVM.

All individuals who are subjected to the vetting process must report any changes in their personal circumstances. This can include changes in marital status or civil partnership, name or address, and financial status (such as a county court judgment or participation in a debt management plan). Failing to report such changes may result in an individual's vetting clearance being downgraded or withdrawn.”⁸⁸

Despite the availability of guidance on the force intranet, and a September 2020 force-wide intranet article reminding all personnel of their responsibilities, we found that some still didn't understand the requirement to update the FVU if their circumstances changed. Some officers told us they knew they needed to update HR in such cases but not the need to update the FVU. They informed the HR team by updating their personal file online, but we established that this information was not automatically passed to the FVU.

The FVU told us that, between January 2021 and September 2021, they had only received 48 change of circumstance forms. In a workforce of 44,000, it is extremely unlikely that this is a true reflection of changes during that period. If the right standards were being imposed, we would expect this figure to be very much higher.

⁸⁸ [APP on Vetting 2021](#), College of Policing, 25 March 2021, paras 8.48.1 and 8.48.2.

Recommendation 4

By 31 March 2023, the MPS should:

- ensure that all police officers and staff are made aware of the requirement to report any changes to their personal circumstances; and
- establish a process whereby all parts of the organisation that need to know about reported changes, particularly the force vetting unit, are always made aware of them.

Monitoring for disproportionality has improved

In [a previous inspection](#), we found that the MPS did not monitor its vetting decisions to identify disproportionality in decision-making concerning applicants from minority backgrounds. Both the *Vetting Code of Practice*⁸⁹ and the Vetting APP⁹⁰ require it to do so.

Encouragingly, we found that the MPS had introduced a process to identify any disproportionality in its vetting decisions. The FVU produces a ‘diversity pack’, which it sends to the force vetting board (FVB).⁹¹

The MPS identified that, between 1 March 2021 and 31 May 2021, applicants from some minority backgrounds were three times more likely to be refused vetting clearance. Often, this was because applicants hadn’t disclosed their associations with family members or other associates with criminal records, or on whom the police held criminal intelligence.

We were told that, in July 2021, the MPS established an ‘equality cell’ to reduce this disproportionality. The main aim of this cell is to improve potential applicants’ understanding of the vetting process. The MPS recognised that, in some ethnic minority groups, cultural differences and mistrust of public authorities could lead to applicants failing to disclose some of the information required during vetting.

Members of the equality cell told us they attend outreach and recruitment events with the public. They address concerns about the vetting process and how information provided during the process will be handled. Such information could include a person’s convictions or family history. The equality cell answers any questions potential applicants have about whether this may prevent them from joining the police.

We saw data that shows that, between 1 June 2021 and 31 August 2021, the disproportionality rates reduced. The MPS told us this was due to the work of the equality cell. It is commendable.

⁸⁹ *Vetting Code of Practice*, College of Policing, 12 October 2017, para 6.6.

⁹⁰ *APP on Vetting 2021*, College of Policing, 25 March 2021, para. 4.1

⁹¹ The force vetting board is chaired by an MPS chief officer to provide strategic direction to the vetting process.

Areas where the MPS does not comply with the Vetting APP

On 21 July 2021, [the Commissioner stated to the London Assembly's Police and Crime Committee](#):

“we do comply with or exceed all standards set by the College of Policing in APP.”

In some respects, the MPS does exceed the standards set by the Vetting APP. These include the MPS's practice of carrying out basic national security vetting checks for every member of its workforce, and, for some levels of vetting, its practice of allowing shorter periods of time than the APP allows between vetting and re-vetting.

However, as we described earlier in this chapter, we found three respects in which the MPS either doesn't comply with, or cannot be sure it complies with, the Vetting APP. These are:

1. the lack of certainty over the vetting levels of those in designated posts (and the possibility that a significant number of designated postholders haven't been vetted to MV level);
2. the absence of established, robust processes to implement risk mitigation measures in cases where such measures would be advisable (including high-risk cases); and
3. the remarkably few instances in which the FVU has been informed of changes of personal circumstances and, among the workforce, the lack of awareness of the requirement to report such changes (leading to a high probability that many changes of personal circumstances haven't been reported).

We also found a respect in which, in July 2021, the MPS didn't comply with a requirement of the Vetting APP but appears to do so now. The Vetting APP states that, if an officer or member of staff is issued with a written warning or final written warning following misconduct procedures, their vetting clearance should be reviewed.⁹² At the time of our inspection, the MPS told us they did not do this, but they have since told us that they started doing this after our visit to the FVU.

In making these observations about the extent of the MPS's compliance with the Vetting APP, we do not seek to imply that the MPS Commissioner deliberately misled the Police and Crime Committee. At our request, the MPS provided us with a copy of the briefing note prepared for the Commissioner's appearance before the committee. It was open to a degree of misinterpretation.

⁹² [APP on Vetting 2021](#), College of Policing, 25 March 2021, para. 8.50.1.

11. Policies designed to prevent corruption

Vetting can't identify all possible threats and vulnerabilities: "vetting will not be effective if used in isolation. It must form part of a wider protective security regime."⁹³

The Counter-Corruption (Prevention) APP outlines what policies forces are expected to have to prevent corruption and provides guidance as to their content. These policies are:

- **gifts and hospitality**, covering the circumstances in which police officers and staff should accept or reject offers of gifts and hospitality;
- **business interests**, covering when the force should allow or deny officers and staff the opportunity to hold 'second jobs' and how the force will manage the risks that arise when they are allowed to hold them;
- **notifiable associations**, covering how the force should manage the risks associated with officers and staff who may associate with, for example, private investigators, journalists, or criminals, and require the disclosure by officers and staff of such associations;
- **service confidence**, covering how the force should manage officers and staff whose integrity is in question;
- **debt management**, covering how the force should manage officers and staff who disclose unmanageable debts;
- **media**, covering how the force should define unauthorised disclosure of information and the boundaries of appropriate relationships with journalists and the media; and
- **social networking**, covering how the force should provide guidance as to what content is and is not acceptable to post on social networking sites.

Clear and concise corruption prevention policies help to guard against corrupt activity. Such policies do not guarantee to prevent corruption, or in themselves stop corrupt practice. They set parameters for how the workforce should behave. They also provide opportunities for forces to gather information on personnel who could be involved in corrupt activities. Policies should clearly state what is expected of the individual and what actions they should take to protect themselves and the organisation from corruption.⁹⁴

⁹³ *APP on Vetting 2021*, College of Policing, 25 March 2021, para. 1.4.

⁹⁴ *APP Professional Standards: Counter-Corruption (Prevention)*, College of Policing, 28 July 2015, p 31.

MPS counter-corruption policies mostly follow APP

We examined MPS policies in respect of gifts and hospitality, declarable associations (this is the MPS name for notifiable associations), business interests, press and media and social media. These policies mostly follow APP but, in some important respects, they didn't. Some appeared to be several years old and required updating. All the MPS's corruption policies are managed by the DPS.

We found no specific MPS policies relating to debt management or service confidence. It has overarching policies where these areas are mentioned.

The legal proceedings policy contains a reference to debt, unpaid fines, and bankruptcy. And it describes the procedures and requirements for personnel when they become subject to, or initiate, legal proceedings, or court orders. We were told that the integrity assurance policy acts as the service confidence policy, although 'service confidence' is not mentioned.

For the purposes of this inspection, we have focused primarily on the gifts and hospitality, business interest and notifiable (declarable) associations policies. These are the three main counter-corruption related policies that most commonly affect the workforce.

Inconsistent understanding of counter-corruption policies

Some personnel we spoke with had an awareness of the three main policies, but others' knowledge was extremely limited. Most personnel we spoke with relied on a common-sense approach to what they thought was expected of them, rather than the direction given by these policies.

We were told that the MPS provides new recruits with training in respect of the policies when they join. This is covered again when individuals are promoted to supervisory roles. We found no refresher training in place for those who joined several years ago but who have not pursued promotion.

The MPS holds local professional development days where it provides training and updates on a variety of subjects. We were told that some local professional standards units provide training sessions. But these were inconsistent in terms of frequency and content, as each local area operates differently. There is no consistent professional standards package that all local professional standards units are expected to provide. This approach was described as "not very organised". It is not based on corruption trends or risks. We found no evidence that corruption policies are covered during these training sessions.

Area for improvement 1

The MPS should provide a more consistent approach to counter-corruption training on local professional development days.

Interviewees told us that they knew how to find the policies in respect of corruption on the intranet, but very few had looked for them. Similarly, very few could recall any messaging from either the DPS or the local professional standards units in respect of corruption.

Failure to communicate and uphold clear standards is a high risk on the force risk register

The MPS is aware that improvement is needed regarding how standards are communicated to the workforce. Significant risks to the MPS are recorded on the force risk register.⁹⁵ We examined an extract from the register entitled ‘Risk 3 Standards’ which is the responsibility of the Assistant Commissioner – Professionalism. The risk is described as “Failure to communicate and uphold clear standards for our workforce undermines public confidence in the Met”. The extract has been risk assessed as red. This means ‘control is not in place or working or progress has slipped’.

The risk register specifies what action is required to bring this risk under control by April 2022. Action to address this risk includes appointing a chief inspector in each BCU to begin local ownership of establishing and raising standards and carrying out a review of standards-related policies and processes. We found there were newly appointed Professionalism chief inspectors in place throughout the force. It was too early for us to evaluate their impact.

Gifts and hospitality

The receiving of, or the offer of, gifts or hospitality is a regular occurrence in many organisations. Customers often like to reward good service with a gift or ‘tip’, which may be perfectly acceptable.

The situation in policing is very different. At the start of their careers, all police officers are required to swear, [on oath](#), that they will serve with:

“fairness, integrity, diligence and impartiality”.

If they then accept gifts or hospitality in the course of their duties, their impartiality may be justifiably called into question, or even compromised.

For these reasons, it is very important that forces have clear and robust policies in respect of how offers of gifts and hospitality are dealt with. It is not sufficient to allow individual members of the workforce to decide for themselves what is and isn’t acceptable. To provide consistency, the College of Policing has developed APP in respect of how forces should deal with such matters.

⁹⁵ A ‘risk register’ is a document for recording identified risks and the actions to be taken to manage each risk.

APP on gifts and hospitality

The Counter-Corruption (Prevention) APP states that receiving gifts and other forms of discounts, hospitality or gratuity can make staff vulnerable to corruption; it can compromise their actual or perceived independence and impartiality. The APP also states that police forces should have a policy which guides staff on how to respond to the offer of gifts and gratuities and promote a culture of non-acceptance.

The Counter-Corruption (Prevention) APP advises that forces should maintain a central record of all gifts offered, accepted, or refused. Most forces set a maximum threshold for the value of a gift that may be accepted. This can be as low as £10.

Where a gift is accepted, a senior officer, normally the operational commander or departmental head, should decide what happens to the item in question. The APP does not comment on the appropriateness of accepting alcohol or cash. However, we find in most forces that, in general, the acceptance of such items is precluded.

We find it difficult to envisage any circumstances in which it would be right and proper for police officers and staff to accept gifts of cash. Recognising the need to maintain public confidence in policing, we consider the safest position for the police service to adopt would be an unambiguous policy that precludes the acceptance of cash gifts.

Recommendation 5

By 31 March 2023, the College of Policing should amend the Counter-Corruption (Prevention) Authorised Professional Practice to make clear that gifts of cash should never be accepted.

The MPS Gifts and Hospitality Policy complies with APP

The MPS gifts and hospitality policy includes the process for managing gifts and hospitality offered to, or accepted by, members of the workforce and the actions they are required to take. Irrespective of whether the gift/hospitality is accepted, the policy states that the offer must be declared and recorded. The implications for those not declaring are also included.

The process involves the (intended or actual) recipient completing a declaration form and submitting it to a local single point of contact (SPOC). The SPOC determines whether the gift should be accepted or refused (if not already refused). The details should be entered onto a local register. A monthly report should be sent to the 'Business Group' SPOC who collates details of all the local declarations. These should be entered onto a single register and sent to the DPS.

The MPS gifts and hospitality policy does not set any maximum acceptable value for a gift that can be accepted or preclude the acceptance of cash or alcohol as gifts. Therefore, theoretically at least, in a case where an officer receives a substantial cash gift, enters it onto the register, and a supervisor approves its acceptance, there would be no breach of the MPS policy.

Gifts and hospitality record keeping is mostly poor

Each BCU/OCU should maintain a record of gifts and hospitality. In the BCUs/OCUs we visited we found that responsibility for maintaining the records varied between the BCU/OCU commander's staff office and the local professional standards unit.

In one BCU, we found that this record-keeping element of the MPS gifts and hospitality policy hadn't been implemented with any appreciable degree of care. There was confusion as to who maintained the record. Despite asking several senior members of staff, we did not get to review their gifts and hospitality register. Our inspectors were contacted several hours after we had left the BCU. We were told a register had finally been located but we were told there were very few entries on it. All the entries predated the restructure of the BCU in February 2019.

We found registers in other BCUs/OCUs were often under-used. In one, there were only five entries recorded and these were undated. On that BCU, officers told us that gifts are often offered but not accepted, which leads us to conclude they weren't completing the register properly. The MPS policy states *all* offers of gifts and hospitality should be recorded whether accepted or refused.

In another BCU, we examined a register that contained 15 entries in relation to gifts received since 2018. There were no entries for hospitality and no entries outlining gifts that had been refused. A third BCU had only one entry recorded in the last 18 months. This was a gift of theatre tickets, which were distributed to members of the local community. A fourth BCU had a register containing the only entry we saw where a gift had been refused.

Record keeping within specialist departments was significantly better than on BCUs. For example, the Royalty and Specialist Protection Command's register contained 30 entries for 2021, comprising mainly gifts from foreign governments and royal families. These were accepted so as not to cause offence and were subsequently donated to charitable causes.

An unusual entry

We found one instance where a member of personnel had been bequeathed many thousands of pounds, following the death of a member of the public. As a bequest rather than a 'gift' in the strictest sense of the policy, it perhaps didn't require an entry in the register or the approval of a senior officer before its acceptance. Nevertheless, the entry was there.

We reviewed an email that suggested the beneficiary had made the entry at a supervisor's request. Having made such a request, we would have expected to see from those handling the matter a greater degree of professional curiosity than we actually found. It appeared to us that their enquiries didn't extend beyond speaking with the beneficiary. This was even though there were obvious enquiries that could have been made with the solicitor handling the estate, or perhaps the bereaved family, to seek independent confirmation of the facts as reported by the beneficiary.

In the documents we reviewed, we saw nothing to suggest impropriety on the part of the beneficiary.

Recommendation 6

By 31 March 2023, the MPS should review and update its gifts and hospitality policy and associated processes to:

- make clear that gifts of cash to individual officers and staff are unacceptable;
- ensure the registers to record gifts and hospitality are accessible, used and maintained;
- ensure that officers and staff are made aware of the policy and their individual responsibilities; and
- ensure that appropriate oversight is maintained of the process and registers, including dip sampling.

Business interests

Legislation and APP relating to business interests

Police forces have a responsibility to avoid any conflict between the business interests of their officers and staff and their roles within policing. This is covered by legislation, i.e. Police Regulations, and force policy which should follow the Counter-Corruption (Prevention) APP.

For police officers and their relatives, business interests are defined in Regulations 6 to 9 of the [Police Regulations 2003](#). For the purposes of this report, this can be summarised as:

- being a member of a police force, the person holds any office or employment for hire or gain (otherwise than as a member of the force) or carries on any business; or
- being a member of a police force or a relative of a member, the person holds or possesses a pecuniary interest in a licence or permit granted in pursuance of the law relating to alcohol licensing, refreshment houses or betting and gaming or regulating places of entertainment in the area of the police force in question.

Where an officer or their relative has a business interest, the officer is required by law to declare it. A senior officer should then decide whether it is compatible with the officer's role. Where a force considers the business interest incompatible, the request can be refused. But where the individual is determined to pursue the interest, they may not be allowed to continue to be a police officer. Where an interest gives a cause for concern, but a force does not wish to refuse the application, it may be managed through restrictions or conditions; for example, a condition covering where the business may be conducted. It is not always possible to manage business interests this way.

For police staff members, their contracts of employment usually include similar provisions concerning business interests.

The Counter-Corruption (Prevention) APP states that business interest policies should specify:

- the requirement for authorisation;
- factors to be considered before approval;
- the application process;
- the monitoring and review process; and
- how to manage subsequent appeals.

The MPS business interest policy reflects the legislation and complies with the APP

We found the MPS has a detailed business interest policy. It is based on [Police Regulations](#) and APP. It highlights the importance of transparency, impartiality, and the effect a business interest may have in “discrediting the police force or undermining confidence in the police service”.

The policy covers officers, staff and other persons working for, or on contract to, the [Mayor’s Office for Policing and Crime \(MOPAC\)](#). It includes relevant family members. Interests such as political activities, additional employment, voluntary activities, commercial arrangements, and contracts are also included. It also outlines the implications for members of the workforce if they fail to notify the force of a business interest. There is an annual review process, a risk management process, and an appeals process. The annual review should be undertaken during the performance development review (PDR) meeting (as we stated earlier, these meetings don’t always take place). Regardless of whether there have been any changes to the business interest or not, an annual review form should still be completed and submitted (but, often, they aren’t).

When someone wants to have a business interest approved, the BCU or OCU will indicate if it wishes to support the application or not and forward it to the DPS. The DPS then decides whether to approve the application. They can approve an application with conditions.

The DPS approves the vast majority of business interest applications it receives. In 2019/20, it received 583 applications; it declined 10 of them. In 2020/21, it received 701 applications; it declined 8 of them.

We were told that personnel often seek informal advice as to the likelihood of their business interest application being approved. We were also told that, where the advice is that it would probably not be approved, many don’t bother submitting an application. Therefore, in such instances, no records would be generated. We are concerned that a lack of formal records of informally refused oral applications might hinder the MPS’s ability to check whether officers who enquire about, but don’t formally apply for approval of a business interest, pursue their interest anyway.

In cases involving a formal application, the individual and the BCU/OCU are notified of the decision. There is no further monitoring of the application by the DPS. The records are held by the BCU/OCU in a format that isn’t easily searchable. The DPS cannot access the locally held records.

Local professional standards units need a better understanding of the business interests held by the personnel they are responsible for

In all the local professional standards units we visited, we asked personnel there about the business interests of the officers and staff for whom they are responsible. Without manually searching a series of individual electronic folders, they could not tell us:

- how many officers and staff on their BCU/OCU had a business interest;
- how many had been approved with conditions and/or what the conditions were;
- how many had been refused; and
- the review dates for the recurring reconsideration of business interest approvals.

Neither the DPS nor local professional standards units monitor compliance with MPS decisions to refuse, or conditions attached to the approval of, business interests

Personnel within the local professional standards unit and the DPS told us they do not have the resources to monitor compliance. We consider that such monitoring is particularly important in cases in which the application was refused on the grounds of incompatibility with policing, and those in which the application could only be approved with conditions.

The risks associated with business interests, identified by the DMIP, are still prevalent

The DMIP reported that in 1987, at least three MPS officers involved in the murder investigation were ‘moonlighting’ for a private detective agency called Southern Investigations. This included providing security for a car auction company. The company became the victim of an alleged robbery, implicating the owner of Southern Investigations and, by association, the serving police officers.⁹⁶

This highlights the need for scrutiny of business interests and officers who undertake additional employment, either with or without authority. The APP is clear that this type of employment outside of their official police duties should be declined, if such a business application were to be made today. We examined the MPS’s business interest policy and found that it explicitly precluded employment as a private investigator or security guard.

Having a clear policy is one thing; robustly implementing it is another. Because of the absence of monitoring that we found, we cannot offer assurance that the MPS’s systems and processes do enough to minimise the risk of corrupt police officers pursuing inappropriate business interests. This is disturbing; officers having inappropriate secondary employment was a significant feature in the Daniel Morgan case.

⁹⁶ [The report of the Daniel Morgan Independent Panel](#), 15 June 2021, vol 3, p 1,032, paras 83–86.

Recommendation 7

By 31 March 2023, the MPS should strengthen its business interests monitoring procedures to ensure that:

- records of business interests are managed in accordance with the business interests policy;
- records are easily accessible to enable reviews to be carried out effectively;
- all personnel are made aware of the policy and their individual responsibilities;
- the force actively monitors personnel compliance with decisions to refuse, or conditions attached to the approval of, business interests; and
- appropriate oversight is maintained of the process and records, including dip sampling.

Notifiable associations

APP guidance on notifiable (declarable) associations

The purpose of this policy is to protect officers, staff and the force from people who may, or may be perceived to, compromise their integrity. The Counter-Corruption (Prevention) APP advises that officers and staff should declare specific associations with people who, for instance:

- may have unspent criminal convictions;
- are under investigation or awaiting trial; or
- are the subject of criminal intelligence.

In this context, 'association' is any relationship or connection with another individual. This can include via social media. The types of people the APP suggests who could be potential corruptors includes family, friends, partners, private investigators, journalists, and members of extremist groups.

In cases where the association presents a significant risk, conditions and restrictions may be applied. These should be subject of regular review and monitoring.

Between January 2018 and October 2021, the MPS received 3,855 declarable association reports. Of these: 3,558 were deemed low risk; 249 medium risk; and 48 high risk (we discuss deficiencies in the risk assessment process later in this report).

At the time of our inspection, 5,293 officers and staff (more than one tenth of the workforce) had at least one declarable association.

The MPS Declarable Associations Policy is seriously out of date

We examined the Declarable Associations Policy the MPS sent us as part of this inspection. It was so outdated that we thought they had sent us an old version. They hadn't.

The policy we saw referred to the [National Policing Improvement Agency](#), an organisation that hasn't existed since 2013. It also referred to a 'professional standards champion', a role that no longer exists in the MPS.⁹⁷

Two surprising omissions from the Declarable Associations Policy

The policy does not include requirements for personnel to disclose their relationships with journalists or extremist groups. These are surprising omissions.

The following examples highlight the importance of having a clearly defined and robust policy that requires personnel to disclose their relationships.

- The DMIP report clearly shows there were continued inappropriate associations by officers with journalists throughout the various stages of the Daniel Morgan investigations and subsequent reviews. This included a huge amount of sensitive information being leaked by a then senior officer involved in the Abelard Two murder investigation, who was subsequently subject of criminal investigation.
- On 7 July 2011, [The Guardian reported](#) that the MPS was trying to identify up to five officers who had allegedly received at least £100,000 in bribes from the News of the World.
- On 1 April 2021, [BBC News](#) and [Sky News](#) reported that the MPS had dismissed an officer who was convicted of being a member of a banned neo-Nazi terror group. The individual was the first British police officer to be convicted of such an offence. The officer was also convicted of lying in respect of the information he provided on his police vetting application.

This prompted further discussion between us and the MPS, during which the force referred us to its media policy. We were advised that the media policy contained a requirement for the disclosure of relationships between MPS personnel and journalists. We examined the media policy, which said:

"If you have a relationship with a journalist on a personal basis outside of your role as a police officer or police staff – such as a relative or close friend – *this is not classed as a declarable association* [our emphasis]. However, you should follow the MPS Professional Standards Policy in the same way that you would in other areas. Therefore, if that relationship with that individual could be seen to impact either on a job that you are involved in or your role, then you should highlight this to your line management so that they are aware."

We compared this with the Counter-Corruption (Prevention) APP, which states:

"a notifiable [declarable] association policy would be expected to contain information on ... television, print and online journalists [and] individuals who are members of or have associations with extremist groups."⁹⁸

⁹⁷ After our fieldwork ended, the MPS informed us that the policy had been revised and was awaiting sign-off.

⁹⁸ *APP Professional Standards: Counter-Corruption (Prevention)*, College of Policing, 28 July 2015, p 32.

and:

“Association has its normal everyday meaning in this context, ie, meeting or uniting for a common purpose, keeping company or being familiar with, being an ally, confederate, partner or colleague, having a friendship, intimacy or connection, being a member of a group, organisation or society which is formed for the promotion of a common objective or aims. This also includes association via social media. Notifiable associations should not include individuals with whom the officer or staff member has a purely professional, on-duty relationship.”⁹⁹

We considered this aspect of the APP to be clear and unambiguous. The MPS’s media policy is incompatible with it. Furthermore, the media policy contains two limitations:

Firstly, it places the onus on the individual to decide whether to disclose an association with a journalist.

Secondly, even in instances where the individual does make such a disclosure, it is only to make their line manager aware. The media policy doesn’t require formal notification along the lines set out in the MPS’s Declarable Associations Policy. As a result, the DPS is unlikely to be told, is unlikely to be able to carry out a risk assessment and is therefore unlikely to put in place any necessary mitigation measures.

The risk assessment process is deficient

The policy states that declarations will be assessed as high, medium or low risk. All risk assessment decisions are made in local professional standards units. There are three deficiencies in the process:

1. these units don’t have any access to the DPS’s corruption-related intelligence system, so they may not be in possession of all the relevant information;
2. most of the decision-makers haven’t been trained in how to assess risk when dealing with counter-corruption intelligence; and
3. there is no ‘scoring matrix’ by which they can ascribe numerical values (weighted or otherwise) to specific factors or considerations, so the assessment is wholly subjective and open to individual interpretation. In other forces, we have seen such matrices in use. While we haven’t evaluated their effectiveness, it is clear that they bring a degree of objectivity to the risk assessment process.

The risk-assessed declarable association is then sent to the DPS, which checks that those graded medium and high risk have been appropriately graded. High-risk associations are recorded and maintained in the DPS. The responsibility for managing low-risk and medium-risk associations is retained by the local professional standards unit.

This process is of concern to us. This is because the DPS, which can see all the relevant information, does not get involved in the assessment of low-risk cases. These cases form the majority.

⁹⁹ As before, p 33.

Under current arrangements, it is entirely conceivable that a declared association is graded as low risk, when the DPS holds intelligence that, if known to the risk assessor, would have resulted in a higher grading.

Recommendation 8

By 31 March 2023, the MPS should ensure that the risk assessment process in respect of declarable associations:

- is always carried out by suitably trained assessors who have access to all relevant information and intelligence; and
- includes an element of objectivity by, for example, the use of a numerical risk matrix.

Monitoring of declarable associations by the MPS needs to improve

The MPS Declarable Associations policy states that high-risk associations are to be managed by the DPS; medium and low-risk associations are to be managed locally. The policy also states that action plans relating to medium and low-risk cases should be reviewed upon any substantial change and at least annually.

In all the local professional standards units we visited, we asked staff about declarable associations. In common with the response we received when we asked similar questions concerning business interests, they said that answering these questions would require them to manually open and read the contents of documents in multiple electronic folders. Without doing this, they couldn't tell us how many of the personnel on their BCU/OCU:

- had a declarable association;
- were medium risk;
- were low risk; and
- had conditions attached to them and what the conditions were.

In all the local professional standards units we visited, personnel told us that, due to their volume of work, they had no time to monitor their low and medium-risk declarable associations. This means that officers' compliance with any conditions that may have been imposed goes unchecked.

Since 2018, the DPS has sent 249 medium-risk and 3558 low-risk declarable associations to the local professional standards units to manage. Local professional standards unit personnel told us that, unless other factors arise, medium and low-risk associations are also not reviewed. This is contrary to force policy. The absence of reviews and monitoring in these cases (especially those that are not low-risk cases) was unacceptable.

In one BCU, we examined three low-risk cases. None had any restrictions applied to them. In one case, an officer was sharing a flat with a drug user. We were surprised that a police officer living with a criminal was graded as low risk. The case was reported in August 2021. The officer was due to move out in September 2021. When we visited the local professional standards unit, on 5 October 2021, our review

found no updated information. It was unclear as to whether the officer had moved out or not. We had concerns that the local professional standards unit was not actively managing this situation.¹⁰⁰

Recommendation 9

By 31 March 2023, the MPS should revise its declarable association policy and associated procedures to:

- place firm obligations on all personnel to disclose to the DPS any relationships with journalists, and any relationships with extremist groups;
- remove outdated references in the policy to the National Policing Improvement Agency and professional standards champions;
- ensure the records are accessible, used and maintained;
- ensure personnel are made aware of the policy and their individual responsibilities;
- maintain effective oversight of the process and registers, including the use of dip sampling (or other similar measures) for assurance purposes; and
- in future, keep the policy up to date.

Ineffective, inconsistent, and fragmented processes to ensure compliance with force counter-corruption policies

MPS compliance processes rely heavily upon:

- effective supervisory oversight;
- an annual PDR process;
- the workforce following gifts and hospitality, business interests and declarable association policies;
- oversight by the DPS and local professional standards units;
- the effective dissemination of intelligence; and
- early intervention.

We found the processes in the MPS to ensure compliance with counter-corruption policies were, in the main, ineffective, inconsistent and fragmented. Compliance checking of force policy within the DPS and local professional standards unit was also hindered by a lack of resources.

Supervisors find it hard to manage corruption risks

Many supervisors told us that they were not provided with sufficient information to manage corruption risks posed by their staff, including those risks that had been formally declared and recorded. They often didn't know about any business interests or declarable associations unless the individual told them.

¹⁰⁰ After our inspection ended, the MPS informed us that the officer had moved out.

They told us that, commonly, staff turnover, the remote location of supervisors and differing shift patterns between constables and sergeants meant that supervisors often don't get to know their staff as well as they would wish. This also hinders their ability to identify welfare, performance, or corruption concerns.

During new recruits' first two years of service, they are usually redeployed four times. This gives them valuable experience of working in different police stations and teams, but it results in them consecutively having four different supervisors. The situation has been exacerbated by remote working because of the pandemic.

Recommendation 10

By 31 March 2023, the MPS should establish and begin operation of a process to ensure that all supervisors are properly briefed on the business interests and declarable associations of all those whom they are expected to supervise.

Annual performance development reviews are inconsistent and ineffective

Performance development reviews (PDRs) are undertaken in many organisations. Their purpose is to assess an individual's performance against corporate values, aims and objectives. Such reviews can have an important role in reinforcing and maintaining the standards of the organisation, but only if they are undertaken correctly. If PDRs are not carried out properly, their purpose is undermined and an important opportunity to reinforce standards and deal with underperformance is lost.

Officers and staff in the MPS should have an annual PDR, where individuals and their supervisors can record evidence of their performance and development needs. As part of the PDR process there is a checklist for supervisors to complete. The checklist is extensive and prompts the supervisor to ask about any business interests or declarable associations the individual may have. It also covers numerous other topics including the current vetting status of the individual.

But we found completion of the PDR and associated checklist was inconsistent. We spoke to many officers who did not have a current PDR and therefore no checklist. In many other cases, officers had a PDR, but their supervisors had not completed the checklist.

Officers in one specialist team told us that they all had up-to-date PDRs and all the checklists had been completed. This was rare. In other areas, officers told us they had not had a PDR for years. The examples given included twelve, seven and five years. Some supervisors told us that they are too busy to deal with all the PDRs of their team. Those applying for promotion or newly promoted were prioritised.

The checklist, which is not mandatory, is not completed for most officers. This is a lost opportunity for the force to capture up-to-date information about important aspects of its workforce, and to check that force counter-corruption policies are being complied with.

Area for improvement 2

The MPS should ensure that its annual professional development review checklist is completed for all officers and staff.

The local professional standards units' role in ensuring compliance with counter-corruption policies is limited

The personnel in the local professional standards unit are not managed by the DPS. The DPS conducts some training for them, but this is generally in respect of the handling of complaints. We were not made aware of any training or inputs for personnel in these units, relating to the role they should take in managing the threats posed by potential corruption.

In the local professional standards units we visited, some staff had less than two years' service and some staff were on recuperative duties. Their primary focus was dealing with public complaints.

Due to the volume of work in local professional standards units, some were experiencing significant backlogs in complaints handling. Consequently, they were not able to undertake any work in relation to counter-corruption activities.

There did not appear to be any oversight by the DPS of local counter-corruption work, such as reviews of registers or dip sampling of how medium-risk cases were being monitored. Given the lack of counter-corruption training and expertise, this is also worrying.

Integrity assurance unit – a valuable resource with not enough staff

The integrity assurance unit (IAU) is responsible for managing individuals in the MPS who have been identified as posing a high corruption risk (including all those with declarable associations assessed as high risk). However, despite the presence of dedicated, hard-working personnel in this unit (as we found elsewhere in the MPS during this inspection), the IAU's capacity is insufficient. The unit comprises only a sergeant and three constables.

The IAU considers whether management meetings are necessary with personnel considered to be high risk. At the meetings, conditions can be placed on the individual to manage the risk. Due to the limited numbers of personnel in the IAU, officers and staff representing a high risk are only reviewed on an annual basis. In the interim, any other action taken is usually because the IAU has received intelligence about the individual. This approach creates a significant risk to the force.

At the time of our inspection, the IAU was attempting to maintain an overview of 495 officers and staff with circumstances that were of concern. Of those 495, they were actively profiling 48 high-risk individuals to assess how to manage the risk they pose.

There were 88 other officers and staff who were subject to risk management measures, such as postings to locations away from the source of the risk. Due to the volume of work in the IAU, 40 (nearly half) of these cases were overdue an annual review.

Where new cases are graded as high risk, the IAU records the relevant information and decides whether a management meeting is required. The meetings involve representatives from the local professional standards unit and the IAU, and the DPS's head of intelligence. Over recent years, the number of individuals assessed as high risk and requiring management meetings has increased: 15 in 2019; 20 in 2020; and, between January and October 2021, 28.

Cause of concern 4

The MPS's lack of monitoring and oversight of declarable associations, business interests and gifts and hospitality is a cause of concern.

Recommendation 11

By 31 March 2023, the MPS should take steps to ensure that:

- the integrity assurance unit (or another unit or units) is sufficiently resourced for the effective monitoring and reviewing of all MPS personnel assessed as presenting a high risk of corruption; and
- any counter corruption-related conditions the MPS places on personnel so assessed are effective in mitigating the risks those personnel present.

The absence of people intelligence meetings is a missed opportunity to prevent corruption

The purpose of 'people intelligence meetings' (in use in many police forces but not the MPS) is to identify individuals who may pose a corruption threat prior to them committing any corrupt acts. They bring together representatives from different parts of the force, to exchange information on those officers and staff who are of concern as described in the Counter-Corruption (Intelligence) APP. This can include, but is not limited to, those who have:

- unsatisfactory performance management;
- sickness management and absenteeism;
- public complaints;
- counter-corruption intelligence;
- internal misconduct cases;
- internet usage;
- high overtime and expense earners;
- business interests;
- debt management problems;
- inappropriate usage of force-issue credit cards; and
- excessive use of force phones, including SMS messages.

Personnel discussed in these meetings can often appear in more than one category. Because relevant information is often held by several departments, corruption risks

can easily be missed. On rare occasions, information exchanged at people intelligence meetings highlights an individual who is already involved in corruption.

We found that the MPS does not hold such meetings. The force holds ‘strategic people management’ meetings to discuss issues such as sickness and attendance, but these do not include the presentation or exchange of corruption-related intelligence or information. Other bespoke meetings may be held to discuss officers of concern. These were described as “ad hoc” and of “limited structure”.

Recommendation 12

By 31 March 2023, the MPS should:

- convene, and hold on a regular and continuing basis, people intelligence meetings; or
- establish and begin operation of an alternative process to facilitate the presentation and exchange of corruption-related intelligence, to identify officers and staff who may present a corruption risk.

12. Information security

Lawful business monitoring

Lawful business monitoring (LBM) is a legitimate activity for forces to monitor their information systems and methods of communication.

LBM is governed by the [Investigatory Powers \(Interception by Businesses etc. for Monitoring and Record-keeping Purposes\) Regulations 2018](#), which authorises public authorities to monitor and record internal business communications.

The use of LBM helps ensure that access to police systems and use of communication devices is for a lawful policing purpose. By using LBM, forces seek to identify unlawful access to police records, wrongful disclosure of police data, computer misuse and inappropriate use of communication devices

The use of IT monitoring

The use of IT monitoring is covered by LBM legislation. This can be used to automate proactive checks on the access to all a force's IT systems and communication devices.

Most forces proactively use IT monitoring to enhance their ability to identify corrupt individuals; for instance, those providing information to organised crime groups, targeting vulnerable people for sexual abuse and accessing police information unlawfully.

It is particularly useful when identifying irregular use or focusing on the systems accessed by the workforce. Automated checks can be used:

- when investigating individuals where there are integrity concerns;
- in cases where mitigations are required because of declarable associations;
- where concerns are raised through the vetting process; and
- to ensure that access to force data is for a lawful policing purpose.

APP guidance on IT monitoring

The Counter-Corruption (Intelligence) APP states that the use of monitoring and auditing software has significant prevention, intelligence gathering and enforcement advantages. This APP lists these as:

- ensuring the integrity and security of personal data and operational information held by forces;
- deterring computer misuse;

- enhancing operational security of serious and complex investigations; and
- providing a reactive and proactive investigative capability.

The use of such systems allows alerts to be created which immediately inform investigating officers when a specific file has been accessed or printed.¹⁰¹

Despite a series of warnings, the MPS still lacks IT monitoring capability

In January 2017, we stated in our national police legitimacy report that:

“the ability of a force to prevent and detect misuse of the information held on its computer systems is an important means of preventing corruption. Protecting this information is vital to integrity and operational effectiveness. Forces must therefore be able to monitor and audit all their information technology (IT) systems to help identify individuals who misuse them for corrupt activity. For example, this could include inappropriate access to personal information, passing on information to organised crime gangs or using systems to identify vulnerable victims for sexual abuse.”¹⁰²

The MPS used to have a form of IT monitoring, known as SpectreSoft, which it purchased in 2009. This product is no longer in use. It is not fit for purpose due to upgrades in software and the types of devices used. Therefore, for the MPS to be able to proactively monitor its workforce’s use of IT, it needs a new IT monitoring system.

In 2017, the force started to evaluate IT monitoring systems that are used by many other UK forces. A demonstration of the systems was planned for early 2018. In April 2018, the force considered a business case but decided not to progress it, due to other priorities.

At that time, the MPS estimated that the cost of procuring and operating an IT monitoring system over a three-year period would have been approximately £1.3 million. Over five years, it was just under £2 million.

On 27 September 2019, we published our [Police effectiveness, efficiency and legitimacy 2018/19 report in respect of the MPS](#). In that report we commented that the MPS “should invest in suitable software to proactively monitor its IT systems”. The report contained a description of an area for improvement in the MPS. It read:

“The force should ensure it has full [IT] monitoring to effectively protect the information contained within its systems.”

Despite this area for improvement being identified, the MPS still does not have the capability to proactively monitor its IT systems. The MPS is – by a substantial margin – the largest force in the UK yet is one of only a tiny number that does not have proactive IT monitoring capability.

¹⁰¹ *APP Professional Standards: Counter-Corruption (Intelligence)*, College of Policing, 28 July 2015, p 20.

¹⁰² [PEEL: Police legitimacy 2016 – A national overview](#), HMICFRS, 8 December 2016, p 28.

The introduction of Connect will not solve this problem

The introduction of Connect, a new MPS IT system, was originally planned for 2021. Connect has been delayed but is now scheduled to go live in two phases: the first phase in November 2022, and the second phase in May 2023. The MPS procured the Connect system without including a full auditing function (which some other forces have done). When implemented, it will provide the MPS with even less auditing capability than it has on its current systems.

The DPS still has concerns about the lack of progress

In 2020, the DPS continued to raise concerns over the auditing and monitoring capability of Connect. As a result, the MPS began to reconsider the purchase of an IT monitoring system. Once again, this work did not progress. Concerns were raised about the effect on the IT network. We were told by senior IT staff that they want to undertake “proof of concept” work to assess the system’s suitability. But this cannot be progressed until a project and appropriate funding has been approved. At the time of our inspection, neither had been approved.

In the meantime, the digital policing department is working with the DPS to enable it to use a cyber security suite of tools for monitoring and auditing. This is still work in progress and will not give the DPS the full capability it needs. The cyber security suite will be insufficient to meet the guidance in the Counter-Corruption (Intelligence) APP, or to resolve our 2018 area for improvement. The fact that the MPS does not have this enhanced capability creates a significant risk for the force.

It is high time that the force took the matter much more seriously, learned from other forces that have done so, and resolved to deal with the material threat of the abuse of its IT systems by corrupt officers and staff. Any suggestion that the force’s size and complexity present too great a hurdle is unconvincing. By their very nature, IT solutions are designed to be scalable. And the MPS has few IT-related policing systems and functions that other forces don’t.

Recommendation 13

By 31 March 2023, the MPS should ensure that it has full IT monitoring capability, to effectively protect the information contained within its systems and help it to identify potentially corrupt officers and staff.

Random checks of the access to national systems are conducted

The MPS carries out some random checks on the use of certain systems, such as PNC and PND. Such checks act as a deterrent to corruption. When contacted, officers and staff are asked to justify why they have searched the database. We spoke to many officers who confirmed that they had been the subject of such a check.

Poor digital device management hinders counter-corruption capability

Management of mobile devices is important when protecting information. It is essential the force has accurate records of who has each device so that they can be held accountable for its use. The workforce must also understand the restrictions on the use of force-supplied devices to ensure they are not used for unauthorised purposes.

We were told that the digital policing department of the MPS has started to improve its management of mobile devices. Despite this, record keeping in respect of such devices was still poor. It is still – indefensibly – unable with any certainty to state to whom each phone or tablet is allocated. At the time of our inspection, there were 45,000 SIM cards in use in the MPS, which emphasises the scale of the problem.

The MPS is planning to introduce a new telephony system, Intune. If successful, this should enable better control of these assets. Through this programme, the force intends to establish who each device has been issued to and what SIM is linked to it. The new system should also bring new auditing capabilities.

Recommendation 14

By 31 March 2023, the MPS should establish and begin operation of an improved system of digital device management, with accurate record keeping concerning:

- for each digital device, the identity of the officer or staff member to whom the device is allocated; and
- the uses to which each device is put.

Guidance on the use of mobile devices is not understood

Many officers and staff told us that, whilst there is guidance on the use of phones, it is confusing and the instructions, for instance in respect of personal use, are unclear. Some stated that the devices were purely for work purposes; others believed that personal calls were allowed. A third group stated they had to 'opt in' to a force scheme prior to making personal calls.

We were told that there is an MPS policy that states individuals wishing to use a force-issued phone for personal use must pay an annual contribution of £50. The policy predates the introduction of smartphones and was designed only to cover the making of personal calls, not communication via social media or internet usage. The MPS intends to review this outdated policy.

Allowing officers and staff use of force-issued mobile devices for personal use may create a false expectation of privacy and impede the force's future attempts to monitor activity on these devices.

In 2020, South Wales Police, on behalf of the National Police Counter-Corruption Advisory Group, prepared *The National Anti-Corruption Monitoring Gap Analysis Report*. The report discussed the problems of allowing personal use of force-issued mobile devices, stating:

“the mixing of personal and business data has significant potential repercussions where private data was obtained through work devices”; and

“that stating employees should have ‘No expectation of privacy’ is insufficient”.

The report contained a recommendation which read:

“Forces are recommended to evaluate the potential cost/benefits of maintaining a Business Use Only policy and ensure their rationales are detailed within their DPIA and local policies.”

We have similar concerns. The MPS has not taken action to implement this recommendation.

Recommendation 15

By 31 March 2023, the MPS should update its policy on the use of mobile devices to include clear explanations of:

- the expectation that force-issued devices are for official police use only; and
- what the force considers to be acceptable and unacceptable use of force-issued devices.

Encrypted apps are a risk to information security

The use of encrypted apps, such as WhatsApp, on mobile phones makes the monitoring of what officers and staff are sharing on their work phones very difficult. We were pleased to see that the MPS does not allow encrypted apps on its force mobiles as a matter of routine. Personnel requiring such apps for operational purposes must apply, providing appropriate rationale.

However, many officers and staff told us they do not have a force-issue mobile phone. They therefore use their private mobile phones, including encrypted apps, for operational purposes. Whilst in some cases this may be being done with the best of intentions it is a risk to: information security; vulnerable members of the public; the workforce; data protection and subsequent disclosure in criminal cases.

In using their personal device, individuals also risk divulging their personal details. Joint guidance from the College of Policing and the NPCC¹⁰³ states:

“Use of (or providing) personal social media, email, telephone or contact details to contact a member of the public you meet during the course of current work or duties is usually inappropriate.”

¹⁰³ [Maintaining a professional boundary between police and members of the public](#), College of Policing and NPCC, undated, para 14.

The MPS Engaging with the Media Policy is misunderstood

The MPS has an 'Engaging with the media policy', which sets out the principles underpinning the way the force should communicate with the media. The policy states officers and staff:

“are encouraged to provide factual information to the media regarding operational incidents or investigations for which they have responsibility.”

The policy also outlines that the directorate of media and communications (DMC) is available for advice and guidance.

Despite the policy, most officers and staff told us they believed they were not allowed to speak with the media and were required to leave such matters to the DMC.

13. Corruption-related intelligence

Sources of corruption-related intelligence

The MPS obtains corruption-related intelligence from a wide range of sources. These include a significant number of reports raised by the workforce through confidential methods of reporting. Other methods of receiving intelligence include: line managers; colleagues directly reporting concerns; investigations into serious and organised crime; other law enforcement agencies and from members of the public.

However, almost all the cases we saw involved the force reacting to items of intelligence that had been referred to the DPS. We believe the MPS is missing opportunities to proactively gather corruption-related intelligence. Earlier in the report, we wrote about the counter-corruption policies, and the opportunities provided by IT monitoring. These can be used to prevent corruption and provide opportunities for forces to gather information on potentially corrupt individuals. We found very little evidence of the MPS using information from these sources to identify potential risks. The MPS is also missing other opportunities to proactively gather counter-corruption intelligence, such as people intelligence meetings.

Certain organisations that work with vulnerable people can be another valuable source of intelligence to help identify officers and staff who abuse their position for a sexual purpose. When their staff are speaking to clients, they may become aware of officers and staff who are becoming overly familiar with the client, which may be a precursor to grooming or sexual abuse.

We explained this in 2017, when we published our [national legitimacy report](#). The report contained the following recommendation:

“Within six months, all forces should have started to implement a plan to achieve the capability and capacity required to seek intelligence on potential abuse of authority for sexual gain. These plans should include consideration of the technology and resources required to monitor IT systems actively and to build relationships with the individuals and organisations that support vulnerable people.”

Following this recommendation, in 2017, we asked all forces to submit their plans to achieve this recommendation. Regrettably, the MPS did not supply sufficient information to allow us to assess its plan. Subsequently the force assured us that it was addressing this recommendation.

We then published a [national report](#) detailing the progress all forces had made, encouraging those with outstanding actions to complete them as soon as possible.

In 2018 we inspected the MPS again, when we found that this recommendation was still outstanding. In our [MPS 2019 PEEL](#) report, we raised this in the form of an area for improvement.

In our 2019 report [Shining a light on betrayal](#), we recommended that all forces that hadn't yet done so should establish regular links between their counter-corruption units and those agencies and organisations that support vulnerable people.

During this inspection we found, three years later, still no evidence that the MPS was doing this.

Cause of concern 2

The MPS's lack of any concerted effort to establish relationships between the directorate of professional standards and organisations supporting vulnerable people is a cause of concern.

Recommendation 16

By 31 March 2023, the directorate of professional standards should establish relationships with external bodies that support vulnerable people. This is to:

- encourage the disclosure by such bodies, to the DPS, of corruption-related intelligence regarding the sexual abuse of vulnerable people by police officers and staff;
- help these bodies' personnel to understand the warning signs to look for; and
- ensure they are made aware of how such information should be disclosed to the directorate of professional standards.

Proactive intelligence development is very infrequent

The MPS often reacts to intelligence concerning potential corruption by its officers but, in some respects, it should do more to proactively generate such intelligence.

In our [2016 national legitimacy report](#) we recommended that, within six months, forces should improve their capability and capacity to seek corruption-related intelligence on potential abuse of authority for sexual gain.

In our 2019 report [Shining a light on betrayal](#) we further recommended:

“By April 2020, all forces that haven't yet done so should make sure they have enough people with the right skills to look proactively for intelligence about those abusing their position for a sexual purpose, and to successfully complete their investigations into those identified.”

We also raised this in the [MPS 2019 PEEL](#) report, in the form of an area for improvement, which stated the force should ensure that it:

“has sufficient capability and capacity in its counter-corruption unit to be effective in its proactive approach to counter corruption.”

Other forms of proactive intelligence development we would have wished to find more of in the MPS, but often didn't, included:

- closer monitoring of IT systems;
- identification of financial irregularities, such as inappropriate or excessive overtime claims and abuse of MPS-provided credit cards;
- analysis of communications data;
- identification and assessment of officers with a propensity to attend certain kinds of incidents (usually those involving vulnerable people); and
- monitoring compliance with counter-corruption policies.

During this inspection, we reviewed 175 items of intelligence and we found only one item was the product of proactive intelligence development. This was a check of who had accessed the custody record of a high-profile individual who was under arrest.

Based upon our previous recommendations, described above, and our experience of other forces, we would expect the MPS's proportion and use of proactive intelligence development to be significantly higher. The lack of IT monitoring capability undoubtedly also has a detrimental impact on the MPS's ability to be proactive.

Despite our clear recommendation in the 2016 national report, our further recommendation in the 2019 spotlight report, and the area for improvement described in our 2019 PEEL report, it appeared to us that the MPS had not made any progress whatsoever. Its absence of attention to this matter prompts us to escalate it accordingly.

Cause of concern 3

The MPS's lack of proactive work to gather counter-corruption intelligence is a cause of concern.

Strong internal processes enable reports of suspected wrongdoing

An effective way to prevent and identify corruption in an organisation is for the workforce to recognise and report wrongdoing. The [Code of Ethics](#) places a duty on officers and staff to challenge and report improper conduct. This means that an officer or a member of staff would be in breach of the standards of professional behaviour and at risk of misconduct procedures if they didn't report wrongdoing.

In July 2021, the MPS introduced a Raising Concerns policy. This policy lists several ways the workforce can raise a concern or report wrongdoing. These include:

- overtly telling a supervisor or colleague;
- reporting directly to the DPS or IOPC;
- covertly reporting wrongdoing using an internal confidential system either on the phone or online; and
- contacting [CrimeStoppers](#), either on the phone or online.

The policy states that the MPS will support anyone who raises a genuine concern.

All officers and staff we spoke to were aware of their responsibility to report wrongdoing and told us of their willingness to do so.

The MPS has a confidential reporting system that is managed by the DPS. This is called the 'Right Line'. The Right Line can be accessed by the workforce either on the phone or online. The phone lines are staffed by officers from the DPS twenty-four hours a day and seven days a week. Officers and staff can choose whether to give their name when they use this system. If they use the online system, they can choose not to give their name but still stay in contact with the DPS by using an anonymous, password protected mailbox system.

If personnel do not feel confident contacting the DPS through either of the Right Line methods, they can contact the CrimeStoppers integrity line. The details of this line are widely circulated across the MPS. It is staffed by non-MPS personnel. Any information provided is passed to the MPS for it to deal with.

The workforce is confident to use confidential reporting systems

We found most of our interviewees were aware of the Right Line and how to use it. Those who told us they had used the system were positive about their experience.

For the year ending 31 March 2021, officers and staff contacted Right Line, either by phone or online, on 296 occasions and CrimeStoppers on 222 occasions.

Of the 175 counter-corruption intelligence files we reviewed, 44 originated from Right Line and CrimeStoppers.

Some told us about the potential consequences of reporting wrongdoing. They feared being ostracised by their team or labelled as a troublemaker if they were identified as having made such a report. One individual told us "You get a name for yourself for being a grass, so you keep things under wraps". Such fears were disturbing to hear and said something very unsettling about the culture within sections of the force.

The leadership of the MPS should be doing more to inculcate a culture in which concerns such as this do not exist.

During our file review we saw two (unrelated) cases, reported through the Right Line, where personnel made allegations against their supervisors. We were concerned that:

- the local professional standards units merely approached the two supervisors on behalf of the DPS and asked for explanations, without carrying any background enquiries; and
- the DPS accepted the explanations without further investigation.

Such a response does little to enhance confidence in personnel that the information they provide via Right Line will be handled in a way that protects their identity.

The MPS definition of a ‘whistle-blower’

The Raising Concerns policy describes who would be considered to be a ‘whistle-blower’ under the Public Interest Disclosure Act 1998 and how such a person will be dealt with. Encouragingly, the DPS has a small team that supports such individuals. The whistle-blower team supports members of the workforce who give ‘protected disclosures’ that are made in the public interest and provide information about:

- the commission of a criminal offence;
- health and safety being endangered;
- damage to the environment;
- a miscarriage of justice;
- failure to comply with a legal obligation; or
- the deliberate concealment of any of the above.

The policy states that individuals who provide such information should not be subject to any detriment at work or lose their job due to ‘blowing the whistle’.

The MPS is the only force in which we have seen a dedicated team to support such ‘whistle-blowers’. The whistle-blower team told us that, between January and September 2021, they received 21 referrals. Two of these had been given official whistleblowing status under the above policy. Anyone who is given ‘whistle-blower’ status will have a point of contact within the whistle-blower team throughout their career.

Where time allows, the team also supports those who provide information but do not fall within the statutory whistleblowing criteria.

The categorisation of corruption-related intelligence still needs to improve

The Counter-Corruption (Intelligence) APP lists 12 categories of corruption-related intelligence. It is good practice for forces to use these categories when recording intelligence. All forces should do this consistently to help them understand the threats they face. The National Crime Agency (NCA) combines local and regional counter-corruption threat assessments (discussed later) to produce a national assessment. Forces should compare their local assessment to the national document and identify any gaps in their understanding. This should be addressed in their control strategy. Use of the Counter-Corruption (Intelligence) APP categories is essential if forces are to play their part in this process.

The Counter-Corruption (Intelligence) APP states that only those behaviours that meet the definition of police corruption should be reported as such. The categories are:

- infiltration;
- disclosure of information;
- perverting the course of justice;
- sexual misconduct;
- controlled drug use and supply;

- theft and fraud;
- misusing force systems;
- abuse of authority;
- inappropriate association;
- vulnerability;
- commit, incite, aid and abet, assist an offender in the commission of a crime; and
- other [corruption-related intelligence not categorised elsewhere].

In 2019, in our [PEEL report](#) we identified an area for improvement as the MPS was not using the Counter-Corruption (Intelligence) APP corruption categories. Similarly, this area was also highlighted in our 2019 report [Shining a light on betrayal](#).

At the time of our inspection, the MPS was one of a very small number of forces still not recording corruption-related intelligence in line with these categories. It was using its own bespoke corruption intelligence categories. To address the difference in recording, it had designed its own IT fix. This selects intelligence based on the MPS codes and electronically aligns them with the national categories. The accuracy of this depends upon a quality assurance process that has been introduced within the DPS intelligence bureau (IB).

During our counter-corruption file review, we found 21 cases which had not been categorised in accordance with the APP categories. We are unclear as to why this should be the case but the MPS still needs to ensure its corruption-related intelligence is categorised in accordance with the Counter-Corruption (Intelligence) APP.¹⁰⁴

Recommendation 17

By 31 March 2023, the MPS should ensure all its corruption-related intelligence is categorised in accordance with the NPCC counter-corruption categories (and any revised version thereof).

Multiple systems for recording corruption-related intelligence presents a risk

The MPS records its corruption-related intelligence on multiple IT systems. This presents a risk as not all those who analyse corruption-related intelligence have access to all the information they need. In several instances, the officers who were assisting us struggled to find the outcome of concluded cases. This was partly due to the number of systems in use and each individual's level of access.

The systems where corruption-related intelligence is held include:

- a database within the DPS IB;
- Centurion (a national system that forces use to record police misconduct and public complaints); and
- a system used solely by the anti-corruption command.

¹⁰⁴ After our inspection ended, the MPS informed us that work was underway to adopt the national categories.

Only the anti-corruption command and a few individuals in the IB have access to all these systems. Others involved in the management of intelligence and risk assessment processes do not. These include personnel based in local areas, departments, and the majority of those within the DPS IB.

We found the MPS's management and storage of corruption-related intelligence to be confusing and disjointed. The MPS would benefit from storing all its corruption-related intelligence in a way that can be accessed by everyone who needs it for their role (for security purposes, a necessarily small group mainly within the DPS).

Access to force systems restricts effective intelligence development

The anti-corruption command focuses almost entirely on the investigation of corruption. The management of corruption-related intelligence is separate from the anti-corruption command; its personnel do not process all items of corruption-related intelligence.

The intelligence bureau (IB) is split into several different units, not all of which have access to all the corruption-related intelligence. The IB is unable to see intelligence relating to anti-corruption command live cases and relies on relevant information being provided to it.

Those involved in the management of corruption-related intelligence outside the IB, including local professional standards units, can't see any of the corruption-related intelligence systems. However, they will still be expected to make risk-based decisions such as the grading of declarable associations.

The development of lower-level corruption-related intelligence should be improved

Most of the intelligence the DPS handles relates to lower-level risks of police corruption. This intelligence is routed through the IB core desk. The core desk deals with a substantial volume of information: approximately 2,000 items of intelligence and enquiries per month. This places a high demand on the IB personnel involved in this work and undoubtedly affects the quality of the intelligence development¹⁰⁵ that can take place. This is not in any way a reflection of the performance of those in the unit.

The core desk seeks to develop corruption-related intelligence to determine if further investigation is required. To do this, it uses other units. These are the dedicated source unit (DSU), integrity assurance unit (IAU), the financial investigation unit (FIU), the research desk and the local professional standards units.

The core desk also sends cases which can be linked to public complaints or certain types of misconduct, such as abuse of position for a sexual purpose, to other units. These include the specialist investigation unit (SIU), complaint support team (CST) and the local professional standards units.

We examined 175 items of corruption-related intelligence handled by the core desk. We found 33 where opportunities to develop the intelligence had been missed.

¹⁰⁵ In this context, intelligence development is the making of further enquiries to clarify the accuracy of the intelligence or obtain further information.

An example of a missed opportunity is a case where there was an allegation of sexual assault against an officer. The allegation was allocated to the local professional standards unit, who contacted the victim, who after some delay decided not to pursue the allegations. This was not communicated to the DPS and the case was closed. As a result, no research was undertaken to establish if the alleged offending was more widespread.

Of the 175 files, we found that 63 progressed to a criminal or misconduct investigation. When a decision was made to investigate an item of corruption-related intelligence, we found that these had been completed to a good standard.

The development of sensitive corruption-related intelligence is good

On occasions, the core desk receives intelligence which is extremely sensitive. The core desk allocates such cases to the tactical team (TAC) or intelligence management unit (IMU) in the DPS for further intelligence development. The TAC team has access to a wide range of covert tactics. Once developed, the TAC allocates the case to the anti-corruption command if further investigation is needed.

In addition to our intelligence file review, we reviewed ten intelligence development files being dealt with by the TAC team. We found that the standard of these files was good and there were no development opportunities missed.

The anti-corruption command deals with highly sensitive and high-risk corruption-related investigations. It does not get involved in the development of lower-level corruption intelligence.

Unstructured arrangements for the development of lower-level corruption-related intelligence

The core desk allocates lower-level corruption-related intelligence to local professional standards units to conduct enquiries. The DPS and the local professional standards units have no standardised method of recording or managing this intelligence. There was also no apparent method of following up these allocated cases once they had been sent to the local professional standards units. This creates a risk that the necessary actions aren't completed. This was evident in our intelligence file review and our visit to local professional standards units.

The types of cases that had been allocated to local professional standards units for further enquiries included suspicions of: theft from police stations (including property stores); misuse of police vehicles; improper recording of duty hours; fraudulent overtime claims; and sexual misconduct. We were surprised to find that the DPS allocated cases of suspected sexual misconduct to the local professional standards units for further enquiries; we do not consider these to be low-level matters.

Recommendation 18

By 31 March 2023, the MPS should develop an effective and auditable process to ensure that all corruption-related intelligence the directorate of professional standards allocates to other units is handled effectively.

Strategic counter-corruption threat assessments

All forces should produce an annual strategic counter-corruption threat assessment detailing the corruption threats they face. They should then use this assessment to:

- identify corruption threats and emerging issues;
- identify locations for corruptors and corrupt activity;
- profile potentially corrupt officers and corruptors; and
- highlight individual and organisational vulnerabilities.

Forces should also use the NCA's national threat assessment to identify any intelligence gaps. A control strategy should then be produced which identifies the action the force will take to better tackle corruption. This is usually achieved through a 'delivery plan' with nominated individuals who are responsible for implementing the actions and providing timely updates as progress is made.

The threat assessment often contains sensitive information which is unsuitable for disclosure to the entire workforce. For example, it may identify vulnerabilities, enforcement tactics and details of operational security. The Counter-Corruption (Intelligence) APP advises that a sanitised version, with these details removed, can be used to convey the main points to the whole workforce. They are then better informed and equipped to identify potential signs of corrupt activities amongst the workforce.

The MPS counter-corruption strategic threat assessment lacks analysis

At the time of our inspection the MPS had a current counter-corruption strategic threat assessment. The MPS assessment is an overview of the volume of corruption-related intelligence received in the DPS. It includes information on whether certain types of reports such as sexual misconduct, including abuse of position for a sexual purpose, are increasing.

It contains six priorities which are:

- sexual misconduct/abuse of position for a sexual purpose;
- theft and fraud;
- unauthorised disclosure of law enforcement information;
- drug use and supply;
- inappropriate and notifiable associations; and
- organised crime – threat of corruption (including infiltration and hostile state actors).

In addition, social media has been identified as an underlying risk area for all of these priorities.

The MPS assessment contains an overview of the volume of corruption-related intelligence received in the DPS. We saw little evidence of any in-depth analysis of this information to identify the current threats. There was no information about the locations of corruptors or corrupt activity. There were no profiles of potentially corrupt officers and staff, or potential corruptors. Furthermore, there was no analysis of where types of corrupt behaviour may be more prevalent. This lack of analysis made

it unclear whether previous preventative activity has worked in trying to address corrupt behaviours.

The MPS counter-corruption control strategy and its implementation are poor

The control strategy associated with the counter-corruption strategic threat assessment is based on the national 4P (Prevent, Prepare, Pursue, Protect) approach. It followed the six priorities identified in their threat assessment, which mirrored those in the national assessment. Each of the priorities was described and several control measures for each threat were identified, together with known gaps in the DPS's capability to tackle corruption.

We found an abundance of control measures but a lack of meaningful detail on how they will be achieved. There was a clear lack of governance and direction. For example, one of the control measures involved consultation with partners who supported vulnerable people. As previously discussed, no appreciable progress has been made on this. Similarly, the strategy should have included a clear intelligence requirement that set out the information needed to fully understand corrupt activities. It didn't.

The MPS does not have a 'delivery plan' or any clear or apparent strategic lead overseeing it. The overall approach is ad hoc with no named individual with responsibility for the identified priorities in the threat assessment, or a method to track progress against the control measures.

We found a lack of awareness and knowledge of the strategic threat assessment and control strategy, not only in OCUs and BCUs, but also within the DPS. This means there are insufficient levels of understanding within the workforce of the threats the force faces and the pivotal role they can play in countering corruption. More encouragingly, we learned that the MPS had established a counter-corruption board, the first meeting of which was due to take place in December 2021 (after our fieldwork had ended).

Recommendation 19

By 31 March 2023, the MPS should revise its counter-corruption strategic threat assessment and control strategy, to include:

- analysis and an evidence base to support the reasons why particular forms of corruption are identified as current threats;
- a clear intelligence requirement;
- a plan in which named individuals are allocated responsibility for the actions set out in the control strategy, and held to account for carrying them out; and
- a communication process to increase the workforce's understanding of the threats the force faces.

14. Capacity and capability to investigate corruption

The anti-corruption command

The anti-corruption command is highly capable

The anti-corruption command's role is to investigate MPS officers and staff where intelligence indicates they may be involved in serious criminality or other forms of police corruption. In some investigations this unit is supported by the intelligence bureau (through the TAC team and the IMU). This support can include executing search warrants, making arrests and undertaking other aspects of the investigation where appropriate.

We found a high level of capability within the anti-corruption command. We were told that all officers and staff have the skills, training, and expertise to undertake complex counter-corruption investigations. The anti-corruption command uses cutting-edge technology, seldom seen elsewhere. We were impressed by the standard of the anti-corruption command investigations that we examined.

Many other forces regularly turn to the MPS anti-corruption command for advice, guidance, and investigative support.

Anti-corruption command personnel are well trained

We were told anti-corruption command detective sergeants attend the College of Policing national counter-corruption bronze course; anti-corruption command detective inspectors and above attend the counter-corruption silver course. A detective inspector leads every corruption investigation. The detective inspectors are also trained to PIP level 3.

It is a mark of the anti-corruption command's expertise that it assists with the College of Policing counter-corruption training by allowing officers with specialist knowledge and experience to provide inputs on these courses.

All the anti-corruption command detective constables are accredited to PIP level 2 and attend an in-house counter-corruption training course.

In addition, the anti-corruption command undertakes a high degree of other specialist training, including covert investigation.

Anti-corruption command – Senior officer resilience

However, there are significant levels of risk being managed in the anti-corruption command, with limited resilience at senior level. We were told the unit head has submitted a business case to increase the number of senior officers by one detective chief inspector (DCI). As of 15 September 2021, one DCI was responsible for 28 investigations, in addition to other supervisory matters.

Anti-corruption command – Detective resilience

At the time of this inspection, the MPS planned to transfer the existing detectives on the anti-corruption command Surveillance Unit to other roles. We were told that all the posts on the anti-corruption command surveillance teams were filled by accredited detectives. Due to a shortage of detectives elsewhere in the MPS, they will be redeployed into other investigative roles. They will be replaced by other officers, trained in surveillance techniques.

At present, the surveillance detectives are accredited to [Professionalising Investigations Programme](#) (PIP) level 2, which provides additional resilience to investigations and allows senior leaders to better manage their resources. Should the MPS continue with its plans to transfer detectives from the unit, the process will need to be managed carefully to maintain the anti-corruption command's capabilities.

Case study: anti-Corruption Command – Operation Carleton

Operation Carleton was focused on the activities of a police constable and a criminal associate. The investigation identified several incidents in which they acted as if engaged in legitimate police business and stopped and detained persons engaged in money laundering, to seize the money for themselves. They both wore police uniform and used marked and unmarked police vehicles. In total, it is believed they acquired more than £2m.

The officer committed offences both on and off duty. Many of these were committed whilst he was on long-term sick leave.

The anti-corruption command undertook a complex covert investigation involving surveillance and other sophisticated tactics. It resulted in the arrest of six suspects, including the serving officer. They were charged with offences including misconduct in a public office, supplying controlled drugs and money laundering.

The officer and five other members of the organised crime group pleaded guilty to all offences. On 13 May 2021, they were collectively sentenced to a total of 64 years imprisonment. The officer was sentenced to 8 years.

The specialist investigations unit

The specialist investigations unit is carrying too many vacancies

The SIU's role is to overtly investigate incidents that involve death or serious injury to members of the public, following direct or indirect contact with the police. This could include road traffic collisions involving a police vehicle, fatal or non-fatal police shootings and deaths in police custody. The SIU also overtly investigates:

- public complaints which are assessed as potentially involving gross misconduct;
- allegations of serious corruption (for example, abuse of position for a sexual purpose); and
- other matters that could be of high risk to the MPS.

Later in 2022, we will report on the findings of our thematic inspection. We will examine the MPS's SIU investigations as part of that inspection.

At the time of this inspection, the SIU establishment was 128 posts. But only 95 were occupied, with most vacancies being at the detective constable level.

Senior officers in the SIU told us that investigators become "overwhelmed", that "the existing establishment is insufficient to deal with the workload", and that "staff are working ridiculous amounts of overtime, doing double the work they should".

Local professional standards units

The local professional standards units lack capacity

In many cases, the local professional standards unit did not have the capacity to undertake all the work they were allocated. Therefore, some complaint investigations were allocated to other, already busy, police inspectors within the BCU/OCU.

Many local professional standards units have huge backlogs. Officers told us that, in one BCU, this led to delays of up to a year before the professional standards unit could appoint an investigating officer, let alone complete the investigation. We were also told that "the standard of investigations they deliver, the volume of work and the nature of that work is disparate and inconsistent".

We were told that none of the local professional standards units had any proactive capability or capacity. Officers and staff told us they had insufficient resources and skills to undertake proactive counter-corruption work. We were told that 90 percent of the workload is complaint investigation and 10 percent low-level misconduct.

The capability of the local professional standards units to investigate corruption is also lacking

Local professional standards units mainly consist of uniformed officers. The force does not allow officers who are detectives or who hold response driver permits to work on these units as their specialist skills are required elsewhere. We were told that in some professional standards units there were not enough applicants to fill vacancies and other teams were instructed to nominate individuals to work there. Some officers on recuperative duties were placed in local professional standards units on a short-term basis. These practices could lead to unsuitable individuals being posted into these roles.

The restriction on recruiting detectives into the local professional standards units significantly limits their investigative expertise. As a result, they have limited capability to undertake anything other than straightforward low-level complaint and misconduct investigations.

They have one training day that is scheduled every quarter and provided by the DPS. These tend to be focused on dealing with complaints. We were told that regular information bulletins are also provided.

Despite not being trained to investigate corruption, on occasions the DPS allocates lower-level corruption investigations to the local professional standards units. We understand that this is primarily to obtain additional facts or information prior to referring the matter back to the DPS. As a result of our findings, it was suggested to us that, sometimes, local professional standards units refer cases to BCU-based detective managers for “early stage fact finding”. The MPS should ensure that personnel in the local professional standards units are only allocated cases for which they are appropriately trained.

We are aware of the transformation project (see next section) which includes a review of the professional standards units. As part of this, the MPS should examine the role, capacity, and training of the personnel in the units, with a view to these units’ roles being extended, to additionally include formal responsibilities for lower-level counter-corruption work. This would include monitoring compliance with counter-corruption related policies, managing the risks associated with declarable associations and business interests, and investigation of lower-level allegations of corruption.

Cause of concern 5

The current professional standards operating model within the MPS is a cause of concern.

The future

A transformation project started in July 2021, focused on making improvements in the DPS. The project's aim is to improve public confidence and satisfaction and reduce demand. It is due for completion at the end of 2022. At the time of our inspection, it was too early to comment on its progress.

The project is led by a detective superintendent. It has four objectives:

1. establish a complaints resolution unit (by January 2022);
2. review the professional standards units;
3. review the IT systems within the DPS; and
4. design a 'target operating model' for the DPS.

The project is expected to secure an additional 32 personnel to form a complaints resolution unit (CRU) and to streamline the way complaints within the MPS are handled. The MPS currently receives approximately 8,000 complaints a year.

The force recently piloted the proposed CRU operating process in one BCU, where they found most of the complaints could be dealt with by a phone call, rather than a personal visit. The aim was to try to resolve most complaints without the need for further investigation. We have not seen a formal evaluation of this, nor are we aware of the complainants' views in respect of the service they received. However, the DPS intends to implement a routine complainant satisfaction survey process.

We are encouraged that the MPS is reviewing the DPS and the local professional standards units.

15. The institutional corruption label

There are various definitions of corruption. In the DMIP report, the Panel identified their definition of police corruption and several features which, in their opinion, amounted to institutional corruption. When the Chair addressed the [London Assembly Police and Crime Committee on 21 July 2021](#), she was unequivocal:

“We have found the [MPS] to be institutionally corrupt.”

This echoes the report, which stated “these cumulative failures amount to institutional corruption on the part of [the MPS, Hampshire Constabulary and the Police Complaints Authority]”.¹⁰⁶

The finding was widely reported; one journalist described it as a “[headline-grabbing epithet](#)”. Examples are easy to find across all aspects of the media, including [newspaper reports](#) and [television coverage](#). But it is perhaps an easier claim to make than to prove – or disprove – in the absence of a universally recognisable and accepted definition.

In this chapter, we consider not only the DMIP’s findings about institutional corruption but other definitions of corruption. Finally, we provide our conclusions.

The DMIP definition of police corruption

The DMIP decided on a broad definition for its work during the inquiry:

“The improper behaviour by action or omission:

- i. by a person or persons in a position of power or exercising powers, such as police officers;
- ii. acting individually or collectively;
- iii. with or without the involvement of other actors who are not in a position of power or exercising powers;

for direct or indirect benefit:

- iv. of the individual(s) involved; or
- v. for a cause or organisation valued by them; or
- vi. for the benefit or detriment of others;

such that a reasonable person would not expect the powers to be exercised for the purpose of achieving that benefit or detriment.”¹⁰⁷

¹⁰⁶ [The Report of the Daniel Morgan Independent Panel](#), 15 June 2021, vol 3, p 1,071, para 293.

¹⁰⁷ As before, vol 3, p 1,020, para 25.

The DMIP definition of institutional corruption

The concept of institutional corruption is not a new one. It has been applied to many areas of public and private life, including the political world. But we found no recognised definition.

In essence, the Panel, in its final report, defined this type of corruption as one where an organisation protects its reputation, rather than where any individual benefits from a corrupt act. The Panel identified the following nine behaviours, actions and omissions, which, *if not the result of professional incompetence or poor management*, should be considered institutional corruption:

1. “failing to identify corruption;
2. failing to confront corruption;
3. failing to manage investigations and ensure proper oversight;
4. failing to take a fresh look at past mistakes and failures;
5. failing to learn from past mistakes and failures;
6. failing to admit past mistakes and failures promptly and specifically;
7. giving unjustified assurances;
8. failing to make a voluntarily commitment to candour; and
9. failing to be open and transparent.”

On this basis, the DMIP concluded that the MPS is institutionally corrupt. The Panel based its finding not only on historical events, but recent ones too:

“The Metropolitan Police’s lack of candour manifested itself in the hurdles placed in the path of the Panel [in relation to HOLMES access, limitations concerning access to sensitive material and the MPS’s response during the fairness process]”.¹⁰⁸

The NPCC definition of police corruption

The College of Policing published its original Counter-Corruption (Intelligence) APP in 2015. It included a definition of police corruption which was designed to assist the police in categorising corrupt actions and behaviours. This standardised approach helped the police service and the Government to identify and assess the nature of corrupt activity and the threats it posed.

¹⁰⁸ As before, p 1,060, para 243.

The APP stated that police corruption occurred when:

“A law enforcement official commits an unlawful act or deliberately fails to fulfil their role, arising out of an abuse of their position, for personal or perceived organisational advantage, having the potential to affect a member of the public.”¹⁰⁹

‘Perceived organisational advantage’ was intended to include instances where individuals acted with the intention of manipulating the perceived performance or standing of the organisation. For example, this included, but was not limited to, manipulating crime figures or detection rates. The DMIP definition of institutional corruption would also fall under this category.

However, the Criminal Justice and Courts Act 2015 introduced a new offence of police corruption, which can only be committed by police officers.

In response to the new offence, the NPCC’s National Counter-Corruption Advisory Group (NCCAG) reviewed its definition of police corruption. In 2018, the NCCAG adopted an amended version:

“Improper exercise of a power or privilege for the purpose of achieving a personal benefit, or a benefit or detriment for another person.”

Corrupt behaviour can be committed by both police officers and police staff. Not all corrupt behaviour constitutes a criminal offence and it often must be dealt with under police misconduct regulations, or police staff regulations.

Therefore, it is necessary that all corrupt behaviours are categorised and recorded.

There are 12 national corruption categories for recording corruption-related intelligence and incidents:

- infiltration;
- disclosure of information;
- perverting the course of justice;
- sexual misconduct;
- controlled drug use and supply;
- theft and fraud;
- misusing force systems;
- abuse of authority;
- inappropriate association;

¹⁰⁹ Although there appears to have been no direct judicial consideration of the term ‘institutional corruption’, the APP definition is similar to the approach summarised in *R v Crook* [2003] EWCA Crim 1272, and in *R v Foran* [2014] EWCA Crim 2407, that the credibility of the evidence of a police officer in a criminal trial may be tainted where, although the officer themselves had not been the subject of any adverse disciplinary or other finding, they were part of a team against which substantial findings had been made. That taint may properly be attributed to those found guilty of misconduct and those who turned a blind eye to the misconduct of other officers of which they were aware. In the context of the specific legal rules about the weight to be attributed to evidence in a criminal trial, it is understandable why a narrower approach to the relevance of institutional corruption concerns has been adopted.

- vulnerability;
- commit, incite, aid and abet, assist an offender in commission of a crime; and
- any other.

We examined these categories and the guidance provided to forces when using them. In their current format, they would not encompass the concerns raised by the DMIP within the nine points they state could constitute institutional corruption.

We also failed to see how the revised NCCAG definition covers all aspects of corruption that need categorising and recording. The new definition appears to focus on the individual and their behaviours. It is our view that the definition and categories need to be amended to accurately reflect the types of incidents which concerned the DMIP and the wider behaviours that can constitute corruption.

Recommendation 20

By 31 March 2023, the NPCC, in consultation with the College of Policing, should amend its definition of police corruption and amend its national corruption categories. This is to ensure that:

- both become more useful to those recording, categorising and analysing corrupt behaviour; and
- the concept of institutional corruption is included in the definition and the categories.

Our views on the DMIP's finding of institutional corruption

Our views must be considered within the context of our terms of reference. We were asked to examine the MPS's organisational learning, its response to the DMIP's requests for information and how well it now tackles the threat of corruption. We were not asked to conduct a criminal investigation; that is not our role. And it was not our intention, nor were we asked, to review the DMIP's work, which it conducted over an eight-year period.

When we considered the institutional corruption label that has – in effect – been attached to the MPS, we did so through the prism of the DMIP's explanation of the concept. We applied the concept to our findings and our interactions with the MPS during this inspection, in terms of the documentation and data we reviewed, and the interviews and reality tests we conducted.

We have considered the nine behaviours the DMIP specified. For the purposes of this exercise, we have aggregated the nine behaviours under five broad headings:

1. Failing to identify or confront corruption

We found shortcomings in the MPS's counter-corruption strategic threat assessment and control strategy. These included a lack of information about the current threats and what the force was doing to mitigate them. Across the force, we also found a lack of awareness and knowledge of these documents and insufficient levels of understanding of the threats the force faces.

Furthermore, the workforce should have a sound understanding of the policies designed to prevent corruption. We found levels of knowledge of these policies was inconsistent and the processes to ensure compliance with the policies were, in the main, ineffective, inconsistent and fragmented.

We also identified shortcomings in the management of corruption-related intelligence. They included failure, despite previous HMICFRS recommendations, to fully record this intelligence in accordance with the NPCC's national categories. Once recorded, we found the investigation of lower-level corruption was too often ineffective. The DPS has insufficient resources to investigate these cases fully and the local professional standards units, to which the DPS allocates some of these cases, also lack sufficient resources and expertise.

These matters amount to a failure to effectively identify and confront some forms of corruption, particularly those at the lower levels of seriousness.

2. Failing to manage investigations and ensure proper oversight

We agree with the DMIP's finding that the management of the initial investigation into Daniel Morgan's murder was poor. Failings from the outset meant that opportunities to gather evidence were lost. Undoubtedly this has had a significant debilitating effect on subsequent efforts to solve the case.

There have been several investigations and reviews into Mr Morgan's death, none of which has led to a conviction for his murder. Regardless of their quality, the MPS has invested heavily in the investigations and reviews. And we saw that, over the years, the MPS tried different approaches, used various methods of investigation (covert and overt) and tried to exploit opportunities provided by new legislation. The MPS's failure to solve the case wasn't because of a shortage of resources to investigate it.

We would need to conduct a separate homicide inspection to consider in depth how the MPS now investigates crimes of this nature. That said, we recognise that the MPS solves the vast majority of the homicides it investigates. This is, no doubt, due in some measure to the changes it has made over the years, which include: the introduction of a specialist crime command, which provides a consolidated approach with appropriate levels of governance; the provision of a wide range of investigation training courses; considerable investment in family liaison; and the introduction of a structured case review process, with a dedicated team of detectives.

3. Failing to examine, admit and learn from past mistakes and failures

We assessed the MPS's appetite for learning. On several occasions, it reviewed – or caused to be reviewed – the investigations into Daniel Morgan's murder. We found lessons that should have been learned over the years had been disregarded and mistakes repeated. We were particularly concerned about the MPS's approach to property and exhibits; our findings painted a dismal picture. Given the lessons of Daniel Morgan's case, this is inexplicable, and indefensible.

The MPS is now taking organisational learning more seriously, although we considered its approach confusing. Much was also still 'work in progress'. Nevertheless, it was encouraging to find that a senior officer is providing leadership and direction in this regard.

We also found that, eight days after its publication, the MPS established Operation Drayfurn to respond to the DMIP report. A deputy assistant commissioner (DAC) has overall charge of the operation and is answerable to the force's deputy commissioner. This commitment should be maintained.

We concluded that, at least until recently, the MPS has often shown a reluctance to examine, admit and learn from past mistakes and failures.

4. Giving unjustified assurances

During our inspection, we found several instances where the MPS provided assurances which did not stand up to scrutiny. We cite two specific examples.

Firstly, in 2019, we published two reports in which we identified that the MPS was not using the national Counter-Corruption (Intelligence) APP corruption categories; we recommended that it should. In response, and instead of fully adopting the national categories, the MPS continued to use its own bespoke categories and designed an IT fix to align the two. The MPS assured us that it had met the requirements of our recommendations and was – in effect – using the national categories. However, during our file review, we found 21 cases that had not been correctly categorised. The MPS's assurance was unjustified.

Secondly, our inspection found that there were two surprising omissions from the Declarable Associations Policy: the requirement for personnel to disclose their relationships with journalists, and similarly, with extremist groups. On being advised of our findings, the MPS referred us to its media policy. We were assured the media policy contained a requirement for the disclosure of relationships between MPS personnel and journalists. Whilst the policy did contain a reference to relationships with journalists, it didn't conform to the counter-corruption APP and, in one respect, opposed it. Again, the assurance was unjustified.

5. Failing to make a voluntary commitment to candour, and failing to be open and transparent

As the Panel found, corrupt police officers obstructed the investigation into Daniel Morgan's murder, or otherwise prevented the interests of justice from being served. At times, the MPS has tried to conceal its failings. Moreover, we conclude that the MPS should not have tried to prevent the full Panel having access to all material in unredacted form; nor should it have even considered refusing the DMIP access to the HOLMES system.

The MPS should have made more of a commitment to assist the DMIP with its work and – from the outset – should have provided more resources to meet the Panel's needs.

The working arrangements between the MPS and the DMIP became adversarial at times. Some important matters weren't resolved quickly enough, required solicitors' correspondence and, on occasion, the Home Office's help. Some of this may have been inevitable, but a greater degree of openness from the MPS would probably have reduced the friction that ensued.

The Home Secretary was clear from the outset that the MPS was expected to co-operate fully with the Panel. However, the MPS's mindset over access to sensitive material and HOLMES belied a lack of openness. Nevertheless, we are satisfied – and the Panel accepts – that the MPS did not ultimately deny them access to any material.

We also found that the MPS was open and honest with us during our inspection. It readily provided any material or information we asked for, and even volunteered additional material which it thought might be helpful.

Conclusion

In respect of its findings concerning the nine behaviours, the DMIP stated the following:

“These failings do not all automatically fall within the definition of corruption.

Some may result from professional incompetence or poor management. However, when the failures *cannot reasonably be explained as genuine error and indicate dishonesty* [our emphasis] for the benefit of the organisation, in the Panel's view they amount to institutional corruption. A lack of candour on the part of the Metropolitan Police in respect of its failings is shown by a lack of transparency, as well as prevarication and obfuscation.”

For our purposes, we viewed this statement as creating a test to be applied when considering the question of institutional corruption. We concluded that the adverse matters we described in our report (and summarised above) bore the hallmarks of limited resources allocated to the maintenance of professional standards, professional incompetence, a lack of understanding of important concepts, poor management or genuine error, rather than dishonesty (other than in the conduct of some individual officers in the context of specific investigations into Mr Morgan's murder). Importantly, we found no evidence of any deliberate or co-ordinated campaign to intentionally frustrate the Panel's work. It follows that we would not describe the MPS as institutionally corrupt based upon the evidence we have seen.

This should not for a moment be understood to be a finding that there are not serious areas of concern which have been, and continue to be, present in the MPS. As this report explains, we conclude that there are multiple serious areas of concern, including in relation to the ways in which the MPS responds to allegations of corruption, which must be addressed to secure public confidence in the MPS. It is essential that the MPS should be more open to criticism and prepared to change where necessary, including by implementing our recommendations. A further failure to do so (without good reason) may well justify the label of institutional corruption in due course.

In a [letter to the Home Secretary dated 29 July 2021](#), the Commissioner set out the MPS's “initial reflections” on the DMIP report and how it intended to proceed with its findings. The Commissioner reiterated that she did not accept the accusation of institutional corruption but made an important statement about the MPS's defensive attitude:

“As an organisation we are proud of the men and women who work for us and the work they do every day serving the public. We do acknowledge that occasionally

this can lead to an overly defensive attitude. We accept that as an organisation we could listen more. We could do even more to be – and to show ourselves to be – open and transparent, to explain what we do and why we do it. This is a vital part of gaining and retaining public confidence and trust.”

Actions speak louder than words, but we consider this a step in the right direction. It is essential that this direction be maintained.

Annex A: Vetting checks

Minimum checks

Recruitment vetting: police officer, police staff, special constables

On applicant, partner, all family (aged 10 years old and over), associates and co-residents:

- Police National Computer (PNC)
- all force databases (including non-conviction databases)
- Counter Terrorism Unit
- Police National Database (PND) and other force checks.

On applicant only:

- record management system check
- crime report allegations
- voters' records
- check of vetting database
- credit reference check and consideration of financial position
- open-source enquiries (for example, search engines and social networking sites)
- professional standards check where necessary
- Ministry of Defence (MOD) checks where relevant
- Criminal Records Office (ACRO) check where appropriate
- Counter Terrorist Check (CTC) may be applied where appropriate.

Management vetting (MV): individuals identified as working in a post assessed as meeting the criteria for MV

On applicant, partner, all family (aged 10 years old and over), associates and co-residents:

- Police National Computer (PNC)
- local intelligence checks
- PND and other force checks
- all force databases (including non-conviction databases)
- Counter Terrorism Unit.

On applicant only:

- voters records
- checking of vetting database
- Ministry of Defence (MOD) checks where relevant
- professional standards checks
- personal finances (including financial questionnaire, force credit reference check and assessment of information returned)
- business interest and secondary employment check (where relevant)
- liaison with occupational health (where relevant)
- open-source enquiries (for example, search engines and social networking sites)
- enquiries relating to vulnerability to pressure or inducements (including the indiscriminate use of alcohol or drugs and/or gambling), where relevant
- appraisals from current and/ or former supervisors to cover a minimum 12-month period (where applicants are existing staff)
- interviews with current and former supervisors at the discretion of the Force Vetting Manager (FVM)
- interviews with the person subjected to the vetting procedure at the discretion of the FVM
- line manager endorsement (reference)
- aftercare must be carried out for MV clearances
- Criminal Records Office (ACRO) check where appropriate
- Security Check (SC) and Developed Vetting (DV) may be applied where appropriate.

March 2022 | © HMICFRS 2022

www.justiceinspectorates.gov.uk/hmicfrs