Freedom of Information Manager

Ministry of Defence Police

Palmer Pavilion,

Building 666,

RAF Wyton, Huntingdon,
Cambs, PE28 2EA

[redacted]

E-mail: MDP-FOI-DP@mod.gov.uk

Our Ref: eCase: FOI 2024/08749

RFI: 093/24

Date: 15th July 2024

Dear [redacted]

FREEDOM OF INFORMATION ACT 2000: MINISTRY OF DEFENCE POLICE: INVESTIGATIVE SOFTWARE

We refer to your email dated 21 May 2024 to the Ministry of Defence Police (MDP), which was acknowledged on 21 May 2024.

We are treating your email as a request for information in accordance with the Freedom of Information Act 2000 (FOIA 2000).

In your email you requested the following information:

1. How many investigation departments are there within your police force (e.g. criminal, narcotics, traffic, cybercrime, etc)?
2. Is your third-party investigative software procured by a centralised IT team or by each investigation department?
3. What was your police forces overall spend on third-party investigative software last year? £…k
4. In percentage terms, approximately how much of this annual spend was:
a. One-off costs (e.g. installation): …%
b. Recurring software fees: …%
5. In percentage terms, approximately how has your overall spend, on an annual basis, changed over the past 3 years?
a. Why (e.g. increase in number of users within existing departments, increase in departments, adopting new software, price increases, etc.)?
6. Please populate the below table, specifying your police force's third-party investigative software spend by category and listing your current software provider(s).
Note that the total annual spend across the below categories should approximately sum to the overall annual spend on third-party investigative software, as per Q3.

Category of investigative software	Description	Approximate annual spend, £k, last available year	Name of your current software provider(s)
Case management software	**Software used as a central hub to manage cases (from incident to reporting), including to ingest and manage relevant evidence, track case progress, and prepare reports for court proceedings.**		
Financial investigation software	**Software designed for extracting, cleaning, analysing and / or visualising financial data and information to investigate financial crimes.**		
Covert operations software	**Software for planning, managing, and executing covert operations, including surveillance management, undercover operations, intelligence gathering and secure communication tools.**		
Critical incidents software	**Software designed specifically for managing and coordinating responses to crises and major incidents. This includes tools for resource allocation, situation analysis, incident tracking, and strategic decision-making during large-scale emergencies. Note that this does NOT include computer-aided dispatch and incident communication software that is used to address everyday 999 calls (see below).**		
Computer-aided dispatch software	**Software for real-time dispatching of emergency services and communication between dispatchers and field units. This category focuses on the operational aspects of dispatching resources, managing communication channels, and ensuring quick response to everyday incidents.**		
Open-source intelligence analysis software	**Software that aggregates and analyses data from multiple open sources (e.g. public records, social media, online forums, etc.) to identify patterns, relationships, etc that aid investigations.**		
Digital forensics software	**Software that enables data extraction from various digital devices (e.g. mobile, social media, cellular networks, etc) and performing detailed analysis on retrieved files.**		

Digital recording and transcription software	**Software used for taking notes, recording interviews, and transcribing recordings into text for analysis, reporting and archiving (can be used in fieldwork by police officers and on investigations).**		
Public evidence and appeals submission portal	**Software that enables members of the public (e.g. victims, witnesses, partners) to upload evidence and information that relates to a criminal incident(s).**		
Other investigative software	**Please provide a high-level summary of what other includes: […]**		

A search for information is complete and I can confirm that the MDP does hold some information in scope of your request. The information we can release is detailed below. Some exemptions apply in line with the FOIA 2000.

1. How many investigation departments are there within your police force (e.g. criminal, narcotics, traffic, cybercrime, etc)?

2

2. Is your third-party investigative software procured by a centralised IT team or by each investigation department?

Third-party investigative software is procured by each investigation department.

3. What was your police forces overall spend on third-party investigative software last year? £…k

£943.5k

4. In percentage terms, approximately how much of this annual spend was:
a. One-off costs (e.g. installation): …%

No information held.

b. Recurring software fees: …%

No information held.

5. In percentage terms, approximately how has your overall spend, on an annual basis, changed over the past 3 years?

Overall spend has remained static.

a. Why (e.g. increase in number of users within existing departments, increase in departments, adopting new software, price increases, etc.)?

No information held.

6. Please populate the below table, specifying your police force's third-party investigative software spend by category and listing your current software provider(s).

Note that the total annual spend across the below categories should approximately sum to the overall annual spend on third-party investigative software, as per Q3.

Category of investigative software	Description	Approximate annual spend, £k, last available year	Name of your current software provider(s)
Case management software	**Software used as a central hub to manage cases (from incident to reporting), including to ingest and manage relevant evidence, track case progress, and prepare reports for court proceedings.**	*Total NEC spend = £910k	NEC*
Financial investigation software	**Software designed for extracting, cleaning, analysing and / or visualising financial data and information to investigate financial crimes.**	£6.5k	Withheld under Section 24(1) and 31(1)
Covert operations software	**Software for planning, managing, and executing covert operations, including surveillance management, undercover operations, intelligence gathering and secure communication tools.**	Neither confirm nor deny under Section 24(2) & 31(3)	Neither confirm nor deny under Section 24(2) & 31(3)
Critical incidents software	**Software designed specifically for managing and coordinating responses to crises and major incidents. This includes tools for resource allocation, situation analysis, incident tracking, and strategic decision-making during large-scale emergencies.** **Note that this does NOT include computer-aided dispatch and incident communication software that is used to address everyday 999 calls (see below).**	No information held	No information held
Computer-aided dispatch software	**Software for real-time dispatching of emergency services and communication between dispatchers and field units. This category focuses on the operational aspects of dispatching resources, managing communication channels, and ensuring quick response to everyday incidents.**	*Total NEC spend = £910k	NEC*
Open-source intelligence analysis software	**Software that aggregates and analyses data from multiple open sources (e.g. public records, social media, online forums, etc.) to identify patterns, relationships, etc that aid investigations.**	No information held	No information held
Digital forensics software	**Software that enables data extraction from various digital devices (e.g. mobile, social media, cellular networks, etc) and performing detailed analysis on retrieved files.**	£27k	Withheld under Section 24(1) and 31(1)

Digital recording and transcription software	**Software used for taking notes, recording interviews, and transcribing recordings into text for analysis, reporting and archiving (can be used in fieldwork by police officers and on investigations).**	No information held	No information held
Public evidence and appeals submission portal	**Software that enables members of the public (e.g. victims, witnesses, partners) to upload evidence and information that relates to a criminal incident(s).**	No information held	No information held
Other investigative software	**Please provide a high-level summary of what other includes: […]**	No information held	No information held

Covert operations software

MDP can neither confirm nor deny that it holds any information relevant to your request as the duty in Section 1(1)(a) of the FOIA does not apply by virtue of the exemptions in Section 24 (2) – National Security and Section 31 (3) – Law Enforcement. These are prejudice based qualified exemptions and there is a requirement to articulate the harm that would be caused in confirming or denying that information is held by carrying out a public interest test.

The balance of this test strongly favours neither confirming or denying that the MDP holds any information. No inference can be taken from this response that information relating to your request does or does not exist.

Section 24 (2) is applied because confirming, or not, that information exists could compromise national security.

Section 31(3) is applied because confirming, or not, that information is held would risk undermining law enforcement.

Case management software / Digital forensics software

MDP are withholding the software provider for each of the above. The duty in Section 1(1)(a) of the FOIA does not apply by virtue of the exemptions in Section 24(1) – National Security, and 31(1) – Law Enforcement. These are prejudice based qualified exemptions and there is a requirement to articulate the harm that would be caused in releasing the information by carrying out a public interest test. On balance, the public interest favours maintaining the exemptions and withholding the information requested.

Section 24(1) is engaged as to release information would render national security measures less effective. This would lead to the compromise of ongoing or future operations to protect the security or infra-structure of the UK and increase the risk of harm to the public.

Section 31(1) is engaged as to release the information would have a detrimental impact on Law Enforcement and could be used to undermine operational policing.

If you are not satisfied with the handling of your request, or the content of this response, you can request an independent internal review by contacting the Information Rights

Compliance team, Ground Floor, MOD Main Building, Whitehall, SW1A 2HB (e-mail CIO-FOI-IR@mod.gov.uk). Please note that any request for an internal review should be made within 40 working days of the date of this response.

If you remain dissatisfied following an internal review, you may raise your complaint directly to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Please note that the Information Commissioner will not normally investigate your case until the MOD internal review process has been completed. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Further details of the role and powers of the Information Commissioner can be found on the Commissioner's website at https://ico.org.uk/.

Yours sincerely

MDP Secretariat and Freedom of Information Office