National Audit Office

REPORT

The Ministry of Defence's management of its losses from fraud and other economic crime

Ministry of Defence

SESSION 2024–2026
30 JANUARY 2026
HC 1596

The National Audit Office (NAO) scrutinises public spending for Parliament and is independent of government and the civil service. We help Parliament hold government to account and we use our insights to help people who manage and govern public bodies improve public services.

The Comptroller and Auditor General (C&AG), Gareth Davies, is an Officer of the House of Commons and leads the NAO. We audit the financial accounts of departments and other public bodies. We also examine and report on the value for money of how public money has been spent.

In 2024, the NAO's work led to a positive financial impact through reduced costs, improved service delivery, or other benefits to citizens, of £5.3 billion. This represents around £53 for every pound of our net expenditure.

National Audit Office

The Ministry of Defence's management of its losses from fraud and other economic crime

Ministry of Defence

Report by the Comptroller and Auditor General

Ordered by the House of Commons
to be printed on 28 January 2026

This report has been prepared under Section 6 of the National Audit Act 1983 for presentation to the House of Commons in accordance with Section 9 of the Act

Gareth Davies
Comptroller and Auditor General
National Audit Office

22 January 2026

HC 1596 | £10.00

Investigations

We conduct investigations to establish the underlying facts in circumstances where concerns have been raised with us, or in response to intelligence that we have gathered through our wider work.

016946 01/26 NAO

Contents

This report can be found on the National Audit Office website at www.nao.org.uk

If you need a version of this report in an alternative format for accessibility reasons, or any of the figures in a different format, contact the NAO at enquiries@nao.org.uk

The National Audit Office study team consisted of:

James Ball, Christopher Barrett, Tabitha Beer and Holly Glenister, under the direction of Joshua Reddaway.

For further information about the National Audit Office please contact:

National Audit Office
Press Office
157–197 Buckingham Palace Road
Victoria
London
SW1W 9SP

020 7798 7400

www.nao.org.uk

@NAOorguk

What this investigation is about

1 The Ministry of Defence (MoD) is, like all parts of government, vulnerable to various types of economic crime and misconduct including fraud, bribery and corruption. The MoD faces particular challenges in safeguarding public expenditure, with high expenditure, complex procurement and supply chains, and a workforce split between the Civil Service and Armed Forces. To tackle these challenges, it has both a counter-fraud team and several Defence police authorities, which span both the criminal and service justice systems, involved in responding to such threats. These comprise the following teams.

- **Fraud Defence:** The MoD's central counter-fraud team, accountable for leading on tackling fraud. Fraud Defence houses its own investigation, risk analysis and fraud awareness teams. It also operates the 'Confidential Hotline', where allegations of fraud and economic crime should be reported, and which is designed to act as a central repository of allegations and investigations across the department.
- **The MoD Police Crime Command (MDP):** A civilian (as opposed to military) police unit tasked with protecting the UK's defence assets. Its remit, amongst other things, includes combating the threat and risk of major fraud, theft of key Defence equipment and assets, bribery and corruption. MDP investigates criminal, or potentially criminal cases involving civilians and military personnel under the criminal justice system, as opposed to the service justice system.
- **Royal Military Police (RMP), Royal Navy Police (RNP) and the Royal Air Force Police (RAFP) – collectively the 'service police':** The service police primarily conduct criminal and non-criminal investigations into people subject to service law and discipline, with potential fraud or economic crime making up a small portion of their work. The service police share a Financial Investigations Team. In 2022 the MoD set up the Defence Serious Crime Command (DSCC) to bring together some of the investigative capability of RMP, RNP and RAFP. DSCC investigates the more complex and serious crime relating to service personnel, including fraud.

2 We have received whistleblowing disclosures over recent years indicating that individual allegations can take a long time to resolve or do not reach a satisfactory resolution, and that overall the MoD could manage fraud and economic crime far more effectively. This report investigates and provides transparency over the MoD's management of its losses from fraud and economic crime. It covers:

- how the MoD is set up to make savings by tackling fraud;
- the MoD's understanding of its fraud risks;
- how the MoD handles fraud investigations, and the outcomes of its work; and
- areas the MoD could improve to realise greater savings from its counter-fraud work.

3 The report does not provide details of individual fraud investigations.

Summary

Key findings

4 The Ministry of Defence (MoD) could potentially make significantly greater savings through its counter-fraud work. The MoD reports what it calls its 'potential fraud risk exposure', which in recent years has peaked at up to £1.5 billion a year, mostly from procurement. The MoD believes this to be only a broad estimate of its potential loss to fraud, which does not take into account its controls. The MoD also receives hundreds of allegations of suspected fraud or economic crime each year, but relatively few result in detection, disruption and recovery. The MoD does not have full sight of all savings made by detecting and disrupting fraud in its other business areas. Cabinet Office and HM Treasury expect that public bodies should save £3 for every £1 spent on counter-fraud work. Between 2021-22 and 2024-25, the MoD reported to Cabinet Office that it spent an average of £5.7 million a year on counter-fraud work and prevented and recovered an average of £2.8 million, of which half was fraud and half was error. This is a return of 48p for every £1 spent. In 2024-25 the MoD's prevention and recovery improved to £6.4 million largely due to the production and application of new data analytics to analyse procurement spend. This resulted in a return of £1.34 for every £1 spent but does not include the cost of developing the new technology (paragraphs 2.2 to 2.10 and Figures 3, 4 and 6).

5 The MoD has been subject to several reviews of Defence policing that highlighted issues relevant to how it manages fraud and economic crime. The reviews have reported siloed working between different teams, inefficiencies and duplication, and relatively few criminal investigations, which tend not to be complex or serious. We heard a strong consensus among officials involved in counter-fraud that the MoD's operating model for managing potential fraud and economic crime needs to improve and have more senior attention across the organisation (paragraphs 1.4, 1.5, 4.5 and Figure 11).

6 The MoD has worked to improve its understanding of where its key fraud risks lie. In line with a general increased focus across government since the COVID-19 pandemic, the MoD has improved its understanding of its fraud risk through an increased and improved use of fraud risk assessments. But the MoD could not demonstrate that it consistently uses this understanding to estimate fraud losses in different areas, prioritise resources or mitigate potential losses (paragraph 2.11). The MoD's main fraud risks are as follows.

- **Procurement:** The MoD spends around £40 billion a year on procurement. While its commercial controls mitigate its exposure to procurement fraud, the MoD recognises procurement remains its biggest fraud risk and acknowledges that there is more it can do to fully understand the extent of the residual risk. For example, it does not know the extent to which its commercial assurance work designed to prevent overpayments stops fraud, because it does not register these overpayments as potential fraud (paragraphs 2.9 and 2.13 to 2.15).

- **Theft of assets:** The MoD recognises theft of assets as a key fraud and security risk. In 2024, the MoD received around 2,500 'security incident' reports about missing assets. Around two-thirds of these reports related to lost assets, with theft making up only 13%. The MoD does not record information on the financial value of assets reported as lost or stolen and only knows indicative figures on this topic. Some police officers we spoke to told us it is possible that some stolen items are reported as lost because it is easier to make a report for lost assets than stolen assets (paragraph 2.16).

- **Personnel management issues and information exploitation:** The MoD recognises separate key risks around personnel management, which include failure to follow gifts and hospitality rules, abuse of flexible working time, and deceit and misrepresentation for financial advantage. It also recognises risks around the exploitation of information and intellectual property, such as misuse of assets for personal use, and unlawfully obtaining or disclosing official documentation (Figure 5).

7 The majority of the MoD's recoveries and prevention savings over the past five years have come from payments to compensate service personnel for harm. According to data from the MoD's Confidential Hotline, between 2020-21 and 2024-25, the MoD made 65% of its prevention and recovery savings from investigation of such compensation, mostly from a single prevention case where an individual unsuccessfully sought to sue the MoD for injuries incurred in service. This kind of personal injury compensation claim against the MoD costs it around £125 million a year. Separately, the MoD spent around £820 million in 2024-25 on 'War Pension Scheme' benefits and the 'Armed Forces Compensation Scheme' to compensate for service-related harm to veterans. After accounting for the one-off case where a large saving was made, the MoD does not assess these areas as high fraud risk or estimate its loss from them (paragraph 2.17).

8 The MoD refers around 60% of reports of potential fraud made to its Confidential Hotline to the business areas outside its counter-fraud and police teams and has limited assurance that these are handled appropriately. The MoD had 1,037 fraud cases outside of Fraud Defence or its police teams open at some point during 2024-25, mostly with either the relevant team for controlling that area of expenditure or the appropriate line manager. The MoD's records state that for most of the allegations closed in 2024-25 no further action was taken, but Fraud Defence does not have complete records for every case and does not assure the quality of the investigations. The MoD's network of 'Fraud Focal Points', who act as a liaison point between business areas and Fraud Defence, spend varying amounts of time in the role and are not always confident about how to progress some fraud cases (paragraphs 3.4 to 3.6 and Figure 7).

9 The MoD does not always know and record how its police services investigate fraud where the department is the victim. We found mismatches between the data held by Fraud Defence and the police authorities on ongoing investigations. The MoD told us its police can receive reports direct from the public, and MoD's case management processes are very manual, with a number of hand-offs. This makes reconciliation of case details difficult. The MoD refers around 40% of reports made to its Confidential Hotline (603 cases in 2024-25) to the MoD's various police teams, with a small proportion handled by Fraud Defence itself. Although cases referred to the police had already been triaged by Fraud Defence, the police often treated them as 'intelligence' rather than reported crimes. In practice, the police investigated 363 cases, many of which Fraud Defence, who are meant to have oversight of all counter-fraud activity, had no knowledge. Where the police did investigate referrals from the Confidential Hotline, they did not always update Fraud Defence on progress with the case. Where the police did provide updates, Fraud Defence did not always record this on the Confidential Hotline case management system. Overall, the MoD's data suggest that investigations result in few outcomes that might serve as a deterrent to future fraud and economic crime, such as formal or informal action, or criminal or service justice action (paragraphs 3.4, 3.7 and 3.8 and Figures 7 to 9).

10 We have identified eight areas where the MoD needs to strengthen its response to fraud and economic crime if it is to achieve better results.

- **Objectives:** Although the MoD Counter Fraud and Corruption Strategy sets out an objective to achieve 'maximum impact' and 'harm reduction', the MoD has not articulated a cross-organisational shared objective of minimising fraud losses and protecting defence capability. Such an objective would assist Fraud Defence and police teams to better prioritise their counter-fraud work (paragraph 4.2).

- **Structure:** The MoD's counter-fraud resources are split between Fraud Defence, the service police and the Ministry of Defence Police Crime Command (MDP), making it hard for any to have economies of scale or the specialist resources to effectively investigate fraud and economic crime (paragraphs 4.3 and 4.4).

- **Culture:** Previous internal reviews have highlighted a lack of trust between counter-fraud and police teams, and noted unclear lines of reporting, duplication and missed investigative opportunities. While the MoD told us that there have been recent improvements, it was clear during our audit that collaboration could be further strengthened. Officials told us that some areas of the MoD do not consider fraud to be a major risk and can be reluctant to engage with counter-fraud officials or the police (paragraphs 4.5 and 4.6).
- **Case triage:** The way the MoD triages cases out of the Confidential Hotline means that it may allocate investigations to the police before exhausting potentially more proportionate, cost-effective and faster options to disrupt and recover losses (paragraphs 4.7 to 4.9).
- **Focus on prevention:** The MoD has significantly increased its number of fraud risk assessments in recent years. But these are not completed across the whole department, are of varying quality, and are not used consistently to identify how fraud gets past controls and to prevent future fraud (paragraphs 2.11, 4.10 and 4.11).
- **Data analytics:** The MoD has attempted several data analytics projects in recent years to help it flag risky transactions and identify areas where preventative controls would be useful, but has reported internally that some business areas lacked the capacity to investigate transactions flagged as suspicious (paragraph 4.12).
- **Intelligence-based prioritisation:** The MoD's many fraud risk assessments have also not been translated into a comprehensive, 'ground-up' estimate of its fraud loss which could inform where it should prioritise its counter-fraud resources (paragraph 4.13).
- **Case management and data:** The MoD's Confidential Hotline, overseen by Fraud Defence, is intended to be a central repository of all allegations of potential fraud across the department. But MDP and the service police have separate case management systems. These systems have incomplete data, use different definitions for key fields, and cannot be used to extract meaningful management information (paragraph 4.14 and Figure 10).

11 The MoD has taken steps over the past year to address some of the issues arising in this report. The MoD told us it is close to producing an enterprise-level fraud risk assessment and is adding an organisation-level shared objective to its next counter-fraud strategy; it has embedded police staff to work alongside Fraud Defence officials in the Confidential Hotline team; and Fraud Defence and the police are also working jointly on a new investigative model for fraud and economic crime – which could include joining police and Fraud Defence case management systems. Fraud Defence told us it is refocusing its resources on recovery, intelligence and analytics, particularly around commercial leakage and exploring the use of artificial intelligence (paragraph 4.15).

Conclusion

12 The MoD has an opportunity to save money through better coordination and management of its counter-fraud and economic crime activity. It is still improving its understanding of its fraud risk, but it is highly likely that the amount it investigates, recovers and prevents is considerably less than the loss it incurs. The MoD also reports a much lower financial return than other departments that invest a similar amount in counter-fraud activity. This is despite having stronger enforcement powers with its own in-house police services. Using this resource more effectively will require the MoD to reform the way it goes about tackling fraud and other economic crime, which would enable it to achieve real savings that could be used to enhance its defence capability.

Recommendations

13 We have discussed with the MoD the steps it has already taken to improve how it manages fraud and economic crime, and its future plans in this space. As it progresses these in the context of its wider Defence Reform activity, we recommend that it:

a **sets a department-wide objective to bring down the MoD's overall level of estimated financial loss due to fraud and economic crime.** This should involve setting out that the key aims of counter-fraud investigation are to maximise the return from prevention, disruption and recovery, to protect Defence capability, and to provide a deterrent against future threats. This objective should also make clear that business areas and functions (for example, commercial) across the MoD should work to reduce their respective levels of fraud and economic crime;

b **empowers a senior official, such as the Director General Finance, to bring together the different parts of the MoD to reduce its losses and to represent the department as the single victim of fraud and economic crime.** The police should report to this official in alignment with the Victim Code on case progress where the MoD is potentially the victim of economic loss. This official should also seek to improve collaboration between the police and Fraud Defence and hold individual business areas to account for how well they manage their fraud risk and cases referred to them;

c **establishes an accountable multi-disciplinary team that brings together the Fraud Defence, service police and MDP staff that investigate fraud and economic crime.** This 'fusion team' should pool resources for fighting fraud and economic crime and look to prioritise those resources to reduce the MoD's economic and defence capability loss. The team should have a clear goal to maximise its return on investment and should bring the right skills, jurisdictions and powers to each case;

d **improves the triaging of cases.** This process should include a more robust initial assessment of how the objective of minimising losses can be most efficiently achieved, whether through criminal investigation, HR action or another intervention. It should also include ongoing reassessment of how best to handle cases that the police have determined do not meet a criminal threshold;

e **continues to develop its understanding of its fraud and economic crime risks** and uses this to improve its counter-fraud performance by:

- **extending its understanding of its fraud controls and savings to include intelligence from across the MoD:** For example, the MoD should gain a better understanding of the financial impact of fraud risks in its commercial activity and the extent to which commercial colleagues are, or could be, employing counter-fraud techniques to disrupt and prevent losses to fraud. It should also improve the information recorded in 'security incident' reports to include an assessment of the financial value of items reported as lost or stolen, and use this as part of its risk assessments;
- **continuing to build its understanding of fraud risk:** The MoD should require all business areas to have their own fraud risk assessment that identifies any significant potential financial loss to fraud. Where such losses are identified, they should be prioritised and regularly updated and monitored to ensure the risk is being suitably mitigated in line with the MoD's risk appetite; and
- **publishing a robust estimate of its total fraud losses, broken down by significant area:** This estimate should be built from its understanding of fraud risks and be broken down to display the financial losses the MoD believes arise from different activities and, potentially, key supplier contracts. The MoD should set out its confidence level for different elements of the estimate, in a similar way to the NHS Counter Fraud Authority's annual 'Strategic Intelligence Assessment'. Where the MoD believes there is a significant fraud risk in a significant area of its expenditure it should also report an estimate of its loss to fraud in its Annual Report and Accounts;

f **gathers consistent, timely and complete information on fraud incidents either through a single case management system or aligning its case management systems.** This should provide the MoD with a 'single version of the truth' on how it is handling its fraud incidents; and

g **identifies where counter-fraud analytics would be most helpful for the MoD in tackling fraud and economic crime and resource these analytics in a way that maximises return on investment.** The MoD should use case data to identify areas or activities where improved controls or data analytics could prevent fraud and economic crime before it occurs. The MoD should also review its data analytics projects from recent years to determine whether investigating fraud flags from this work could bring an improved return, and to identify where preventative controls should be introduced.

Part One

How the Ministry of Defence is set up to make savings by tackling fraud

1.1 In this part we set out:

- how the Ministry of Defence (MoD) is set up to respond to allegations of fraud and economic crime; and
- the MoD's plans for managing fraud and economic crime in the future.

How the MoD is set up to respond to allegations of fraud

1.2 Each area of the MoD is responsible for managing its own fraud risks. To support these areas, the MoD has the following teams (**Figure 1** on pages 13 and 14).

- **Fraud Defence:** a central counter-fraud team which leads the MoD counter-fraud function.
- **The MoD Police Crime Command (MDP):** a police team which focuses on serious crime by civilians or military personnel under the criminal justice system, as opposed to the service justice system.
- **The 'service police' (the Royal Military Police, Royal Navy Police and Royal Air Force Police):** police teams which focus on crime by personnel subject to the service justice system. In 2022 the MoD established a Defence Serious Crime Command to handle the most serious and complex crimes alleged to have been committed by service personnel, including fraud.

The Defence police authorities' primary duties are around discipline and security, though they are sometimes involved in responding to instances of fraud or economic crime.

Figure 1

The Ministry of Defence (MoD) teams that respond to fraud and economic threats

There are several teams in the MoD that respond to fraud and economic threats, but these function mostly independently

	Fraud Defence	MoD Police Crime Command (MDP)	Service police
Involvement in tackling fraud and economic crime	Leads the MoD's counter-fraud function and reports to the Director General Finance.	Operationally independent civilian police service.	Operationally independent military police.
Consisting of	The 'Confidential Hotline' for reporting fraud and economic crime allegations. Teams that do investigation, risk analysis and fraud awareness.	Crime Command as the investigative, intelligence and counter terrorism branch of MDP.	Royal Military Police, Royal Navy Police, Royal Air Force Police and the Defence Serious Crime Command for more complex and serious cases.
Examples of fraud and economic crime handled	Pay related, personnel related, procurement fraud.	Civilian theft of assets, procurement, pension, pay related fraud.	Theft of assets, service pay related, service personnel related.
Investigations			
Types of investigations	Non-criminal	Criminal	Criminal
Persons investigated	MoD civil servants and service personnel.	Civilians and service personnel.	Service personnel and civilians who are subject to service law.
Charge for prosecution by	n/a – no powers to charge for crimes.[1]	The Crown Prosecution Service.	The Service Prosecuting Authority.
Powers			
Investigatory Powers Act 2016[2]	Limited	Yes	Yes, subject to Armed Forces Act 2006
Armed Forces Act 2006[3]	No	No	Yes
Ministry of Defence Police Act 1987[4]	No	Yes	No
Proceeds of Crime Act 2002[5]	No	Yes	No
Resources as at December 2025[6]			
Full-time equivalent (FTE) staff	22	46[7]	247[8]
FTE staff dedicated to investigating fraud and economic crime	5	7	0[9]

Figure 1 *continued*
The Ministry of Defence (MoD) teams that respond to fraud and economic threats

Notes

1 Fraud Defence can investigate service personnel and civilian staff equally but does not have powers to charge for crimes.

2 The Investigatory Powers Act 2016 enables investigation bodies to obtain communications and data about communications.

3 The Armed Forces Act 2006 provides the service police with powers to take disciplinary or criminal action against service personnel.

4 The Ministry of Defence Police Act 1987 provides MDP officers with full constabulary powers, identical to other civil police officers in the UK.

5 The Proceeds of Crime Act 2002 provides investigation bodies with the power to recover criminal assets including the confiscation of assets, search and seizure, and "restraint" or "freezing" of assets.

6 The resourcing shown here is the resourcing information that the MoD provided for this study. We have not sought to reconcile this to the MoD's reporting to Cabinet Office on the cost of its counter-fraud resource.

7 The FTE stated is for the MDP Crime Command, which is the part of MDP most likely to handle serious fraud and economic crime and makes up a small portion of the overall MDP workforce.

8 The FTE stated is for the Defence Serious Crime Command, which is the part of the service police most likely to handle serious fraud and economic crime and makes up a small portion of the overall service police workforce.

9 There are no service police personnel dedicated to investigating only fraud and economic crime. The service police share a Financial Investigation Team which consists of five personnel who provide support to investigations that have a financial element.

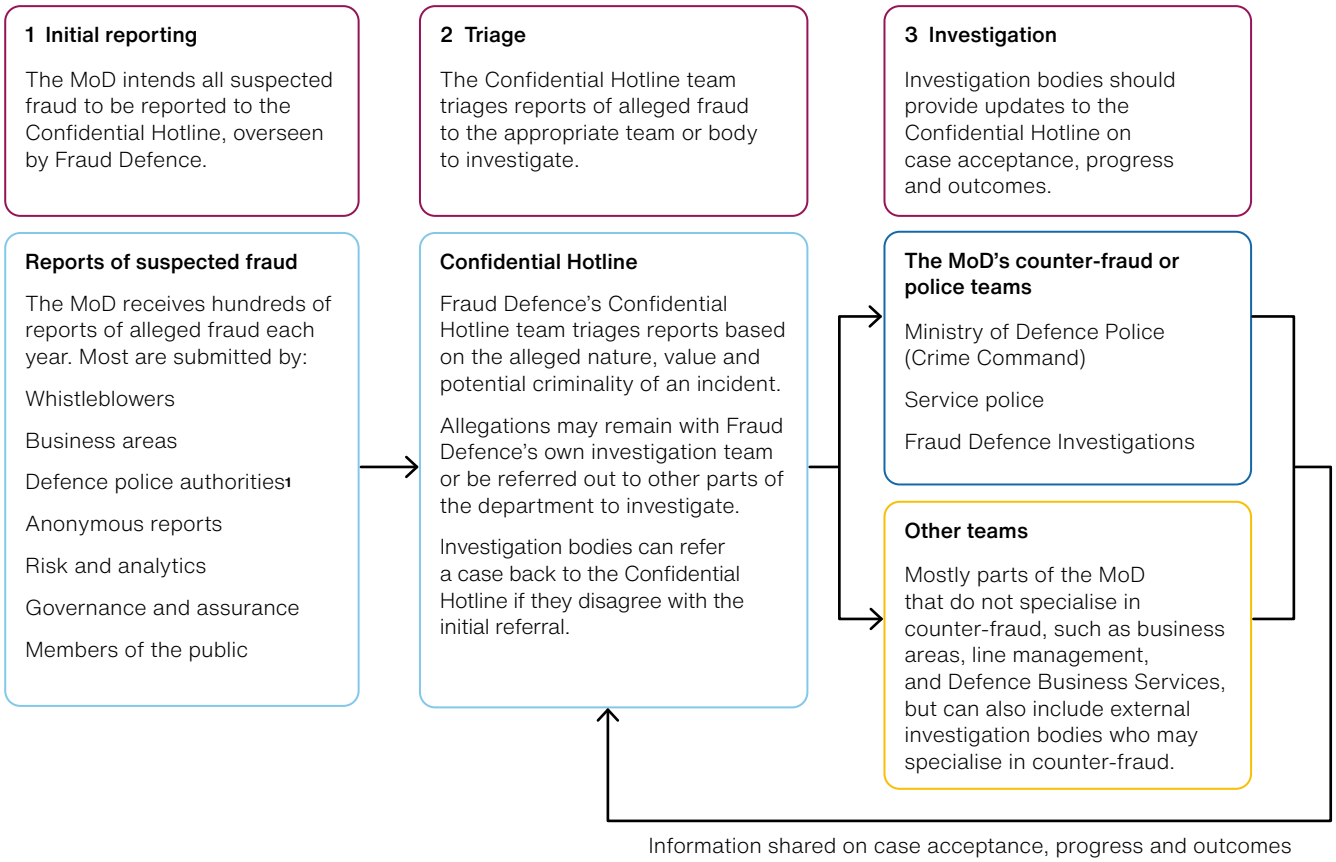
Source: National Audit Office interviews with officials and review of documents

1.3 The MoD asks armed forces personnel, staff, contractors and the public to report potential fraud and economic crime through its Confidential Hotline (**Figure 2**). This is operated by Fraud Defence, which triages cases out to appropriate teams, and logs progress and outcomes from fraud investigations across the department. The Confidential Hotline is intended to be the central repository of all fraud and economic crime investigations across the MoD.

Figure 2

The role of the Confidential Hotline in how the Ministry of Defence (MoD) manages fraud

The MoD intends for the Confidential Hotline to act as a central repository for all alleged fraud incidents – with Fraud Defence conducting initial triage and case development



- Process / system
- The MoD's counter-fraud or police teams
- Other teams

Notes

1 The Defence police authorities consists of the Ministry of Defence Police, Royal Military Police, Royal Navy Police, Royal Air Force Police and the Defence Serious Crime Command.

2 This figure illustrates how the MoD believes the Confidential Hotline should operate; however, in practice, the Confidential Hotline does not contain information about all counter-fraud activity occurring across the MoD.

Source: National Audit Office review of Fraud Defence Operations Standard Operating Procedures 2025

The MoD's future plans for managing fraud and economic crime

1.4 We heard a strong consensus among officials involved in counter-fraud that the MoD's operating model for managing potential fraud and economic crime needs to improve and have more senior attention across the organisation. The MoD has been subject to several reviews of Defence policing in recent years, which have highlighted siloed working between different teams, inefficiencies and duplication, and relatively few criminal investigations and these tend not to be complex or serious. The findings from these reviews are set out in Appendix One.

1.5 The MoD is making major changes to its structure and governance as part of its Defence Reform programme. As part of this, the MoD is undertaking two reviews that relate to Defence policing – one focusing on the governance of service policing and another on options for the most effective delivery of Defence policing. The MoD aims for these reviews to resolve the long-standing issues raised by past reviews and expects to provide recommendations during 2026. It is not yet clear whether there will be direct implications for the MoD's counter-fraud activity, but the reviews will examine the potential *"benefits from cohering the criminal investigation and intelligence abilities of Defence policing (including MDP)"*. Officials within Fraud Defence and MDP told us that uncertainty around the structure and governance of Defence policing regarding fraud and economic crime has hindered other efforts to make change.

1.6 Alongside this, Fraud Defence is completing work to understand the problems faced by the MoD's counter-fraud function and has proposed a new operating model for how the MoD could be set up to tackle fraud and economic crime. Officials in Fraud Defence told us they believe any new operating model for fraud and economic crime within the MoD should include:

- collective use of the MoD's overall counter-fraud resources;
- the creation of a common case management system and definitions;
- clearer adoption criteria and triage of cases to appropriate investigation bodies;
- clearer accountability for counter-fraud at senior levels across the MoD; and
- counter-fraud key performance indicators that the MoD can measure, are routinely used, and are helpful in its management of fraud and economic crime.

Part Two

The Ministry of Defence's understanding of its fraud risks

2.1 In this part we set out:

- the Ministry of Defence's (MoD's) understanding of its fraud risks;
- the fraud that the MoD prevents, detects and recovers; and
- the MoD's fraud risk assessment.

The MoD's understanding of its fraud risks

2.2 The MoD faces particular challenges in safeguarding public expenditure, with high expenditure, complex procurement and supply chains, and a workforce split between the Civil Service and Armed Forces.

2.3 In assessing the challenges it faces, the MoD does not have an accurate estimate of its fraud loss that is built from fraud loss measurement exercises or risk assessments. It produces annually what it calls a 'potential fraud risk exposure' estimate, based on what it detects and external benchmarks. The MoD calculates the minimum 'at risk' fraud value by assuming that it detected 10% of the average fraud that occurred in previous years. It calculates the maximum 'at risk' fraud value by assuming there is 4.57% fraud in its procurement and 1.7% fraud in its payroll spend. The MoD takes these benchmarks from the 2023 Annual Fraud Indicator published by Crowe, Peters & Peters and the University of Portsmouth but they are not specific to the MoD's activity or experience. Since 2020-21, the MoD has estimated the lowest minimum value 'at risk' was £1.1 billion, while the highest maximum was £1.5 billion, which is mostly from procurement.

2.4 The MoD acknowledges that these figures are only useful as a broad estimate of its potential loss to fraud and notes that they do not take into account the effectiveness of its controls. The MoD believes the estimates should only be seen as accurate to the order of magnitude. The real level of loss could be significantly higher or lower. For example, the MoD has historically calculated its maximum 'at risk' estimate using several specific areas of expenditure from its annual report and accounts, which for 2024-25 totalled £28.5 billion. The MoD told us in future it plans to calculate its maximum 'at risk' estimate using the total procurement spend of around £40 billion drawn from HM Treasury's 2025 Public Expenditure Statistical Analyses dataset, which would imply that the maximum 'at risk' estimate would be up to around £2 billion if not mitigated.

2.5 As well as financial risk, fraud and economic crime such as stolen equipment, product substitution, or fraudulent goods and services pose a risk to defence capability. The MoD has not attempted to estimate the impact of fraud and economic crime on its capability.

2.6 The MoD's exposure to fraud risk will increase as defence spending rises. The June 2025 Spending Review detailed plans for the MoD to increase its spending from £53.9 billion in 2023-24 to £73.5 billion in 2028-29. These plans reflect an increase in the MoD's predictable areas of spending but do not cover unpredictable or demand-led spending (which would be in addition to the amount stated). The government has committed to increase defence spending to 2.5% of GDP by 2027.

The fraud that the MoD prevents, detects and recovers

2.7 Cabinet Office's Public Sector Fraud Authority (PSFA) collects information from all government departments about their counter-fraud resourcing and levels of detected, prevented and recovered fraud. Although the MoD's estimate of its exposure to potential fraud loss is high, it only reports to Cabinet Office low levels of detected, prevented and recovered fraud losses (**Figure 3**).

2.8 Cabinet Office and HM Treasury expect government departments to target a saving of £3 for every £1 they spend on counter-fraud. Between 2021-22 and 2024-25, the MoD reported to Cabinet Office that it spent an average of £5.7 million a year on counter-fraud and prevented and recovered an average of £2.8 million a year, of which half was fraud and half was error. This meant it achieved savings of 48p for every £1 spent. In 2024-25 the MoD reported to Cabinet Office that it saved £6.4 million by preventing or recovering fraud – a return of £1.34 for every £1 it spent (**Figure 4** on page 20). This is an increase on previous years due to a one-off recovery of £3.8 million. This was the result of a review of commercial leakage completed in 2023, that identified £17.5 million of potentially recoverable overpayments.

Figure 3

Fraud that the Ministry of Defence (MoD) prevented, detected and recovered in 2024-25, compared with its 'potential fraud risk exposure' estimate

The MoD detected, prevented and recovered a small amount of fraud compared with its 'potential fraud risk exposure' estimate for the scale of fraud that may be occurring

Category	Value
	(£mn)
The MoD's 'potential fraud risk exposure' estimate[1]	Up to 1,500
Alleged fraud that the MoD reported to Cabinet Office	253
Detected fraud that the MoD reported to Cabinet Office	2.3
Prevented fraud that the MoD reported to Cabinet Office	2.1
Recovered fraud that the MoD reported to Cabinet Office	0.3

Notes

1 The MoD's estimate relies on benchmarks rather than fraud loss measurement or risk assessment of specific spend areas and has peaked at £1.5 billion in recent years. But the MoD believes the estimate is still a helpful indicator of the potential order of magnitude of the loss to economic crime. The MoD has told us it plans to revise this estimate using an updated procurement spend, which would imply that the estimate would be up to £2 billion, if not mitigated.

2 The alleged, detected, prevented and recovered fraud amounts are those which the MoD rewported to Cabinet Office for the period 1 April 2024 to 31 March 2025. The amounts shown do not include those that the MoD reported to Cabinet Office relating to error.

3 Cabinet Office defines 'alleged' fraud as "the suspected fraud allegations received through organisational reporting routes", 'detected' fraud as "fraud that was detected after it happened", 'prevented' fraud as "fraud that was prevented before it happened", and 'recovered' fraud as "fraud where funds have been recovered".

4 The MoD believes that significantly more activity to prevent and recover fraud occurs across the department than it measures and records, which means this activity does not get reported to Cabinet Office.

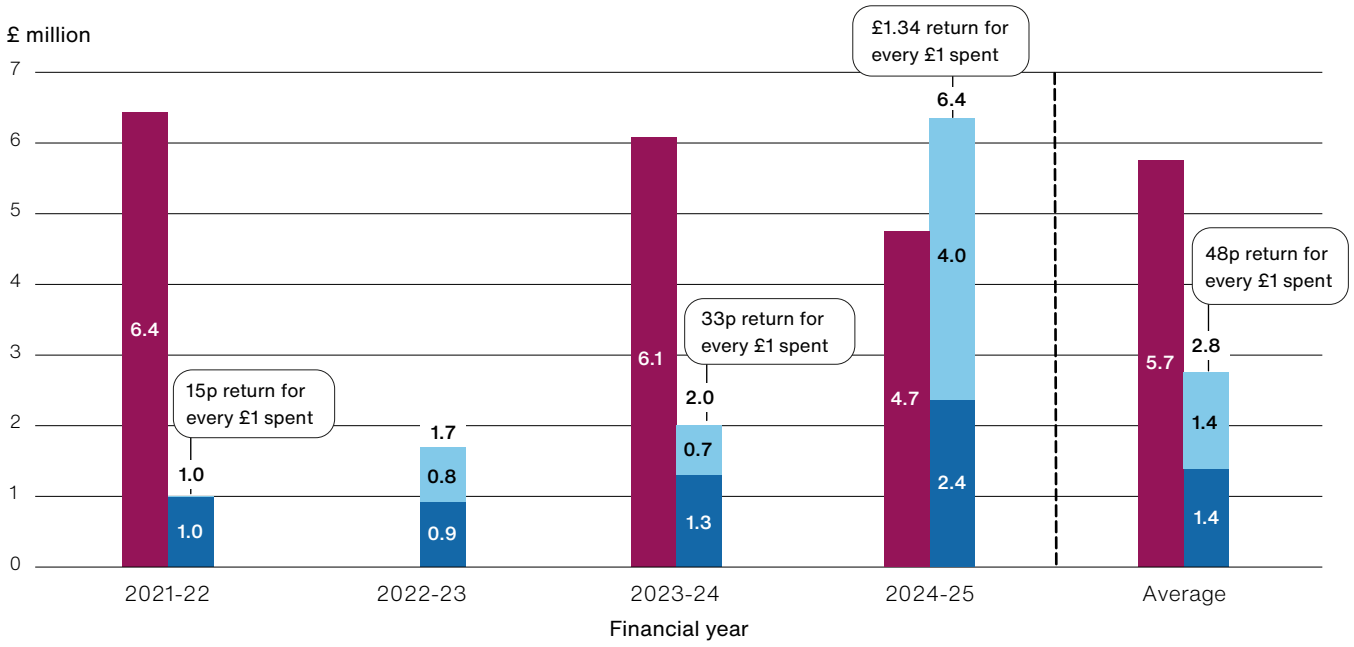
5 Cabinet Office data showing the MoD's counter-fraud submissions did not align exactly to the information we saw on the Confidential Hotline, the MoD's central reporting repository. But the two data sources suggested a broadly consistent level of performance and differences may have been a result of timing differences or other adjustments.

Source: National Audit Office review of the Ministry of Defence Audit Committee papers and Cabinet Office data on the Ministry of Defence's counter-fraud returns

Figure 4

The Ministry of Defence's (MoD's) counter-fraud spend and its prevented and recovered fraud and error, 2021-22 to 2024-25

Over the past four years, the MoD has reported that it returned on average 48p for every £1 it spent on counter-fraud activities; in 2024-25 it reported an improved performance on previous years of £1.34 for every £1 spent, largely due to a significant saving from a one-off exercise



Notes

1 The values used in this figure have been rounded, so specific returns for every £1 spent do not always match the values that would be calculated using amounts on the face of the figure.

2 The value for error prevented or recovered in 2021-22 was £1,700.

3 Cabinet Office did not collect data from the MoD about its counter-fraud budget in 2022-23.

4 The counter-fraud budget is the amount the MoD reported to Cabinet Office as being its overall budget for all counter-fraud, bribery and corruption activity.

5 Cabinet Office data showing the MoD's counter-fraud submissions did not align exactly to the information we saw on the Confidential Hotline, the MoD's central reporting repository. But the two data sources suggested a broadly consistent level of performance and differences may have been a result of timing differences or other adjustments.

6 The MoD believes it is preventing and recovering more fraud and error than it is currently able to identify and report.

7 The costs presented are only those incurred directly by the police and Fraud Defence on counter-fraud activities. Of the savings reported for 2024-25, £3.8 million related to recoveries following a review of 'commercial leakage' commissioned by the MoD and completed in December 2023, which identified £17.5 million of potentially recoverable overpayments. The MoD told us this review cost £5 million, mostly relating to the development of data analytics technology to analyse contract and spend data for identification and recovery of overpayments. The MoD has told us it intends to use an improved version of this technology in the future, and did not include the cost of this review in the costs of counter-fraud activities that it reported to Cabinet Office.

Source: National Audit Office analysis of Cabinet Office data on the Ministry of Defence's counter-fraud returns

2.9 The MoD's reporting to Cabinet Office may not accurately reflect its return on investment, for the following reasons.

- **It generally only captures fraud prevented and recovered directly by its counter-fraud work.** The MoD believes that significantly more activity to prevent and recover fraud occurs across the department than it measures and records, which means this activity does not get reported to Cabinet Office. For example, the MoD's single-source contracting has controls in place, including the Cost Assurance and Analysis Service (CAAS), to verify costs and resolve potential overpayments. This may prevent some fraud, without identifying it as such.
- **It excludes costs incurred on counter-fraud work outside of the police and Fraud Defence.** For example, the MoD told us the review of commercial leakage (paragraph 2.8) cost £5 million, mostly relating to the development of data analytics technology to analyse contract and spend data for identification and recovery of overpayments. The MoD told us it intends to use an improved version of this technology in the future. The MoD did not include the costs of this review or the total value of potentially recoverable overpayments in its reporting to Cabinet Office.
- **The MoD told us it finds it difficult to identify and record counter-fraud resourcing.** The MoD reported that it spent £4.7 million in 2024-25, which was lower than the £6.1 million it reported in 2023-24. It told us that this probably reflects a change in what it was counting as counter-fraud staff, rather than a reduction in resourcing.
- **The information in the returns does not reconcile to the data on the Confidential Hotline about prevented, detected and recovered money, or the recovery information provided to the NAO by police.** However, the different data sets were broadly similar, and differences may be due to timing or other amendments made during the production of the statistics for Cabinet Office.

2.10 Even if the MoD's return on investment on its counter-fraud work is significantly understated, we believe the MoD could achieve more from its existing level of counter-fraud resources. The level of resources the MoD has reported to Cabinet Office is similar to that of other departments that achieve a far greater return on investment.

The MoD's economic crime and fraud risk assessment

2.11 The MoD has worked to improve its understanding of the risk it faces from fraud and economic crime. This activity aligns with recent efforts from the Cabinet Office and the PSFA to promote better risk assessment across government since the COVID-19 pandemic. The MoD's Fraud Defence team has developed 130 bespoke risk registers and brought these together to give a single view of the scale of the MoD's fraud risks, and the mitigations it has in place to address them. Properly identifying the risks is a vital first step to manage those risks. However, the MoD has not finished this process, and we found it could better manage fraud risk by doing the following.

- **Completing fraud risk assessments to cover all areas of the MoD:** officials told us that some business areas have not fully engaged with the risk assessment process. The PSFA assessed in 2023-24 that, at that time, the MoD's fraud risk assessment did not meet the minimum requirements of the Counter Fraud Functional Standard, including that Initial Fraud Impact Assessments were not always completed on major new projects that meet the mandatory criteria. The PSFA wrote to the MoD in December 2025 highlighting areas of progress, including the standard of Initial Fraud Impact Assessments. But its letter also noted that "the department needs to hold to account the projects not engaging in this process and be clear of the need to progress this work". The MoD told us that it has now completed 21 of the 22 Initial Fraud Impact Assessments that it is expected by the PSFA to have completed.

- **Effective prioritisation:** The MoD's risk register shows around 1,500 active risks, of which about half have a current mitigated impact score of 'severe' or 'critical', the two highest levels of risk. These range from significant procurement fraud risks to items such as abuse of flexible working time (**Figure 5** on pages 23 and 24).

- **Quantifying the financial impact:** The MoD's risk scores are heavily based on the expected 'impact' of the risk, but it has not assigned financial values to its risks, even where they have been categorised as 'severe' or 'critical'. We would expect areas that are significant to the MoD, and which carry a significant fraud risk, to be estimated and reported on in its annual report and accounts.

- **Stating the risk appetite:** The MoD's risk register does not include risk appetites that it could use to decide how it should respond to the identified risks (for example, a certain level of risk might be accepted, mitigated, or avoided).

- **Measuring whether mitigations are working:** Some 'severe' or 'critical' active risks in the register had not been updated for up to five years, and there is no assessment of how well existing controls are operating.

Figure 5

Most commonly recorded fraud risks in the Ministry of Defence's (MoD's) central fraud risk register as at August 2025

The MoD records fraud risks in a central register but rates around half as having a 'severe' or 'critical' impact, with no assessment of financial impact, which limits its usefulness for prioritising counter-fraud activity that could minimise losses

Most commonly listed fraud categories	Most common types of fraud risk listed within category	Number of active fraud risks listed	Percentage rated as having a 'severe' or critical' potential impact[1,2]
			(%)
Procurement	Misuse of electronic purchasing cards	74	39
	Fraudulent invoicing for goods or services	53	58
	Pre-contract award fraud or irregularity	50	64
	Inappropriate asset disposal	33	36
	All other risk types	196	59
Personnel management related	Failure to follow gifts and hospitality policy and procedures	65	54
	Abuse of flexible working time	64	27
	Deceit and misrepresentation for advantage	42	26
	Misuse of official time	28	36
	All other risk types	57	32
Theft of assets	Theft of other Defence assets	69	39
	Theft of IT/telecoms	37	54
	Theft of intellectual property rights	34	65
	Theft of cash	33	58
	All other risk types	61	56
Exploiting assets and information	Misuse of assets for personal use	53	28
	Using official vehicles for personal use	28	39
	Unlawful obtaining and/or disclosure of other official documentation	16	81
	Unlawful obtaining and/or disclosure of personal data	7	57
	All other risk types	18	61

Figure 5 *continued*
Most commonly recorded fraud risks in the Ministry of Defence's (MoD) central fraud risk register at August 2025

Most commonly listed fraud categories	Most common types of fraud risk listed within category	Number of active fraud risks listed	Percentage rated as having a 'severe' or critical' potential impact[1,2]
			(%)
Pay related	False claims for overtime and other taxable allowances	33	33
	Creation of fictitious employees	17	29
	Actual or attempted corruption of an official	14	71
	Abuse of position or authority	11	55
	All other risk types	26	27
Sub-total		**1,119**	**47**
Other categories[3]		349	48
Total		**1,468**	**47**

Notes

1 The MoD defines 'severe' risks as those with possible impacts of "potential to significantly impact the business or programme" and "widespread media interest". 'Critical' risks have possible impacts of "potential for catastrophic impact to the business or programme" and "full public enquiry, national media interest, major loss of public confidence".

2 The figure shows potential risk impacts that are rated 'severe' or 'critical' after any mitigations to the potential impact that the MoD has in place, and does not consider how likely the risk is to occur. The MoD uses the impact score, and a separate score relating to how likely a risk is to happen, to generate an overall risk score.

3 Other fraud categories include civilian and service expenses, payment processes, civilian and service allowances, cyber and communication, recruiting, civilian and service pay, civilian and service compensation schemes, departmental income related, and pension fraud.

Source: National Audit Office analysis of the Ministry of Defence's central fraud risk register as at August 2025

2.12 The MoD's work to improve its understanding of its fraud and economic crime risk has identified five significant risks (Figure 5): procurement, theft of assets, personnel management, exploiting assets and information, and pay related risks. Together these constitute around three-quarters of the MoD's active fraud risks in its central register and are also the areas on which the MoD receives the majority of allegations to its Confidential Hotline. Our work suggests fraud may be underreported against the MoD's two biggest risks: procurement and theft of assets.

Procurement

2.13 The MoD spent around £40 billion on procurement in 2024-25. While its commercial controls will mitigate some of its exposure to procurement fraud, the MoD recognises procurement as its biggest fraud risk. It told us that, although it is challenging to understand the full extent of the residual risk, there is further work it could do to improve its view of this, and of how much fraud its commercial controls stop.

2.14 Our discussions with MoD officials working in counter-fraud and assurance suggest that the MoD's commercial teams do not routinely consider supplier relationships from a counter-fraud perspective. For example, there are no clear criteria for commercial staff to refer commercial disputes where fraud may have occurred to Fraud Defence or the police and the MoD. Commercial staff, seeking to maintain strong working relationships with suppliers, may be reluctant to consider whether overpayments require investigation, and may not employ contract management counter-fraud techniques to help improve value for money.

2.15 The MoD has recently sought to better align its commercial and counter-fraud functions. It told us that its commercial function works closely with Fraud Defence, CAAS and other stakeholders to respond to whistleblowing concerns requiring investigation. For each case, it will appoint a commercial professional with no conflict of interest or prior involvement to conduct an impartial review. As part of work on the Single Source Contract Regulations, the MoD also told us it is considering how it might better use the Single Source Regulations Office to monitor and address monopoly behaviours. Additionally, the MoD told us that there are clauses and contract provisions that highlight fraud prevention, and strategic suppliers have annual reviews that include scrutiny of their ethics, whistleblowing, and supply chain risks approaches. In 2023, the MoD commissioned a review of 'commercial leakage' to identify areas of non-compliance within existing MoD digital procurement contracts, which identified £17.5 million of potentially recoverable overpayments (see paragraph 2.8).

Theft of assets

2.16 Defence personnel, including industry partners, are expected to file 'security incident' reports about missing assets. The 'security incident' reporting form does not request information on the financial value of these assets. It does request the number of individual assets but the MoD does not routinely compile this into a total number of missing items or assess the financial value. In 2024, the MoD received around 2,500 'security incident' reports about missing assets (excluding ID cards). Around 40% of these reports related to IT assets and 30% related to assets 'attractive to criminal and terrorist organisations' (e.g. weaponry, protective equipment and communications devices). The rest related mostly to information and personal data. Around two-thirds of the 'security incident' reports related to lost items (1,649), with theft making up only 13% of the reports (324). The Confidential Hotline received only 151 allegations of stolen assets in 2024, and the police data showed that they received only 74 cases of theft. Some police officers told us it is possible that some theft in the MoD does not get reported. They said this was partly because it is easier to report items as lost rather than stolen.

Other risks

2.17 According to the MoD's Confidential Hotline, between 2020-21 and 2024-25, the MoD made 65% of its fraud prevention and recovery savings from payments to compensate service personnel for harm. The savings mostly came from a single prevention case where an individual unsuccessfully sought to sue the MoD for injuries incurred in service. On top of around £125 million payments a year for such personal injury compensation payments, the MoD also made payments of around £820 million in 2024-25 to compensate for service-related harm to veterans through the 'War Pension Scheme' and the 'Armed Forces Compensation Scheme'. After accounting for the one-off case where a large saving was made, the MoD does not assess these areas as high fraud risk. The MoD also does not have estimates of the level of fraud in the payments it makes that relate to pensions and compensation. It may be able to adapt methodologies used by other government departments to estimate fraud and error.

Part Three

How the Ministry of Defence handles fraud investigations, and the outcomes of its work

3.1 In this part, we set out:

- the types of fraud and economic crime allegations that the Ministry of Defence (MoD) receives;
- how the MoD triages reports of potential fraud that are made to the Confidential Hotline; and
- outcomes from investigations.

Fraud and economic crime allegations that the MoD receives

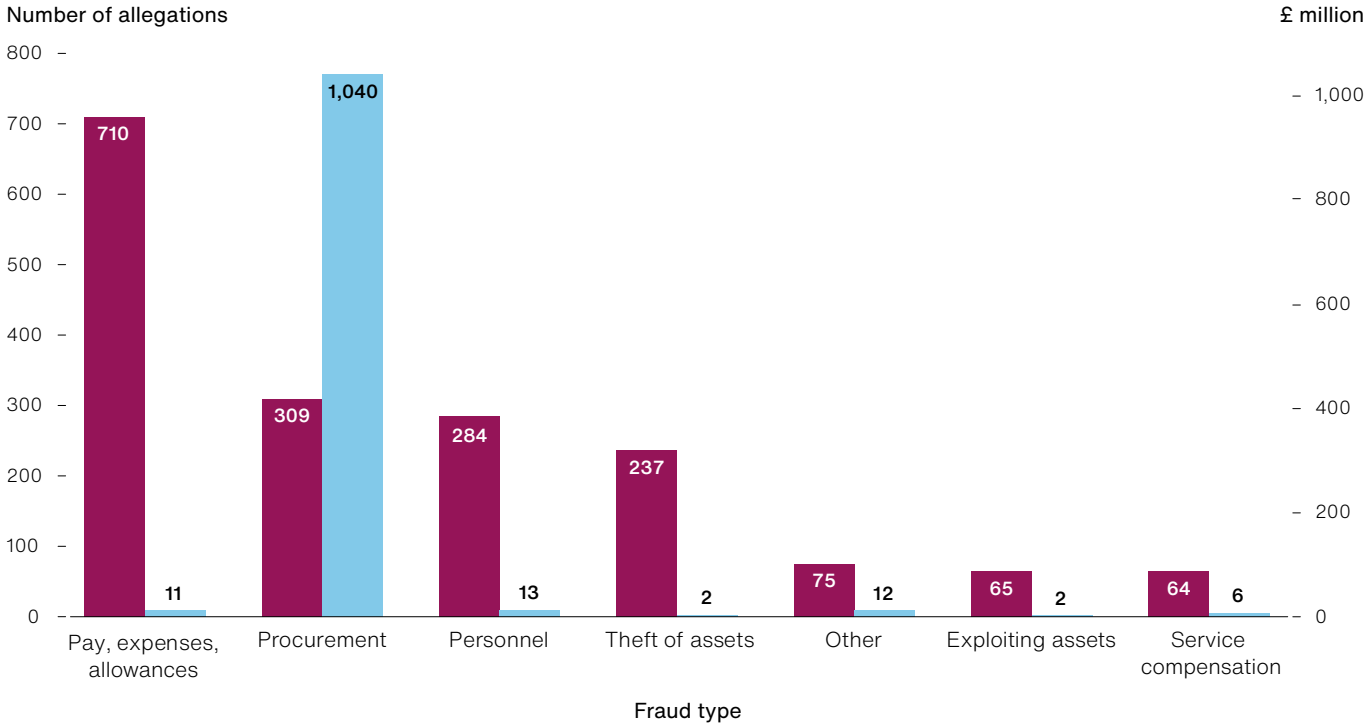
3.2 The MoD has a 'Confidential Hotline' which is run by Fraud Defence, its main counter-fraud team. The Confidential Hotline is intended to be a central database for all allegations and investigations of fraud and economic crime across the department. The MoD considered around 1,700 allegations in 2024-25, comprising allegations both reported to the Confidential Hotline in year and allegations that remained open from previous years (**Figure 6** overleaf). The Confidential Hotline data indicates that these allegations related to £1.1 billion of loss in 2024-25. This value is calculated by taking in order of priority: the actual fraud loss discovered on investigation; the suspected fraud loss reported by the person making the allegation; or a 'nominal' value based on broad historical benchmarks where a more informed value was not available.

3.3 Most of the allegations relate to issues with a low value that might be better dealt with through preventative controls rather than criminal investigation. Around 60% of the allegations relate to pay, expenses and allowances, and personnel issues like abuse of flexible working. However, these allegations represent only 2% of the estimated value of alleged crime. Procurement fraud constitutes 18% of the allegations on the Confidential Hotline and represents over 95% of the value of alleged fraud loss.

Figure 6

Fraud and economic crime allegations received by or at some point active on the Ministry of Defence's (MoD's) Confidential Hotline during 2024-25

Allegations were most commonly about pay, expenses and allowances, but nearly all the alleged financial loss related to procurement



Notes

1 We have grouped information on 'fraud types' from the Confidential Hotline into broader categories. Some items on the Confidential Hotline had more than one fraud type, in such instances all fraud types have been counted.

2 Twenty-two items on the Confidential Hotline recorded 'whistleblower' as the only fraud type. 'Whistleblower' is a method of reporting as opposed to a type of fraud, and so these items have been excluded. These items did not have an associated financial value.

3 Two items did not have a fraud type assigned. They did not have an associated financial value and have also been excluded from this figure.

4 The 'sum of financial value' shown is a combination of actual offence values, alleged offence values and nominal offence values. Where available, the actual offence value is used, as this is the value discovered on investigation. Where there was no actual offence value, the alleged value of the specific fraud case has been used, as this is the amount reported by the person making the allegation. If neither of these were available, the 'nominal value' recorded by the MoD has been used. Nominal values are based on broad historical benchmarks where a better estimate is not available. The financial values in the figure relate to the potential fraud loss for an offence and do not include amounts recorded as 'prevention' savings.

5 Fraud types in the 'other' category include categories such as cyber and communication, recruiting, health and safety, signposting, breaches of policy such as travel and subsistence and items recorded on the Confidential Hotline as 'other'.

6 The 'Service compensation' category includes fraud in payments to compensate service personnel for harm, 'War Pension Scheme' benefits and the 'Armed Forces Compensation Scheme'.

Source: National Audit Office analysis of data from the Ministry of Defence's Confidential Hotline

How the MoD triages reports of potential fraud that are made to the Confidential Hotline

3.4 Fraud Defence triages reports of potential fraud sent to the Confidential Hotline and normally refers them on for investigation by others (**Figure 7** overleaf). It has a standard operating procedure that sets out at a high level how triage should occur, but this does not detail the specific adoption thresholds for the various investigation bodies that could respond to a case. Fraud Defence officials told us that in practice they typically use their knowledge and experience to determine which team they should refer the case on to. This usually involves considering the nature of the case, alleged value and potential criminality. Of the fraud cases that were active at some point on the Confidential Hotline in 2024-25, the MoD had referred 1,037 (around 60%) outside of its counter-fraud or police teams, mostly to the relevant team for controlling the area of expenditure or the appropriate line manager. The other 40% of fraud cases were mostly referred to police teams (603 cases), with a small portion handled by Fraud Defence (12 cases) or yet to be referred to an investigation body (48 cases).

Cases handled outside of the MoD's counter-fraud or police teams

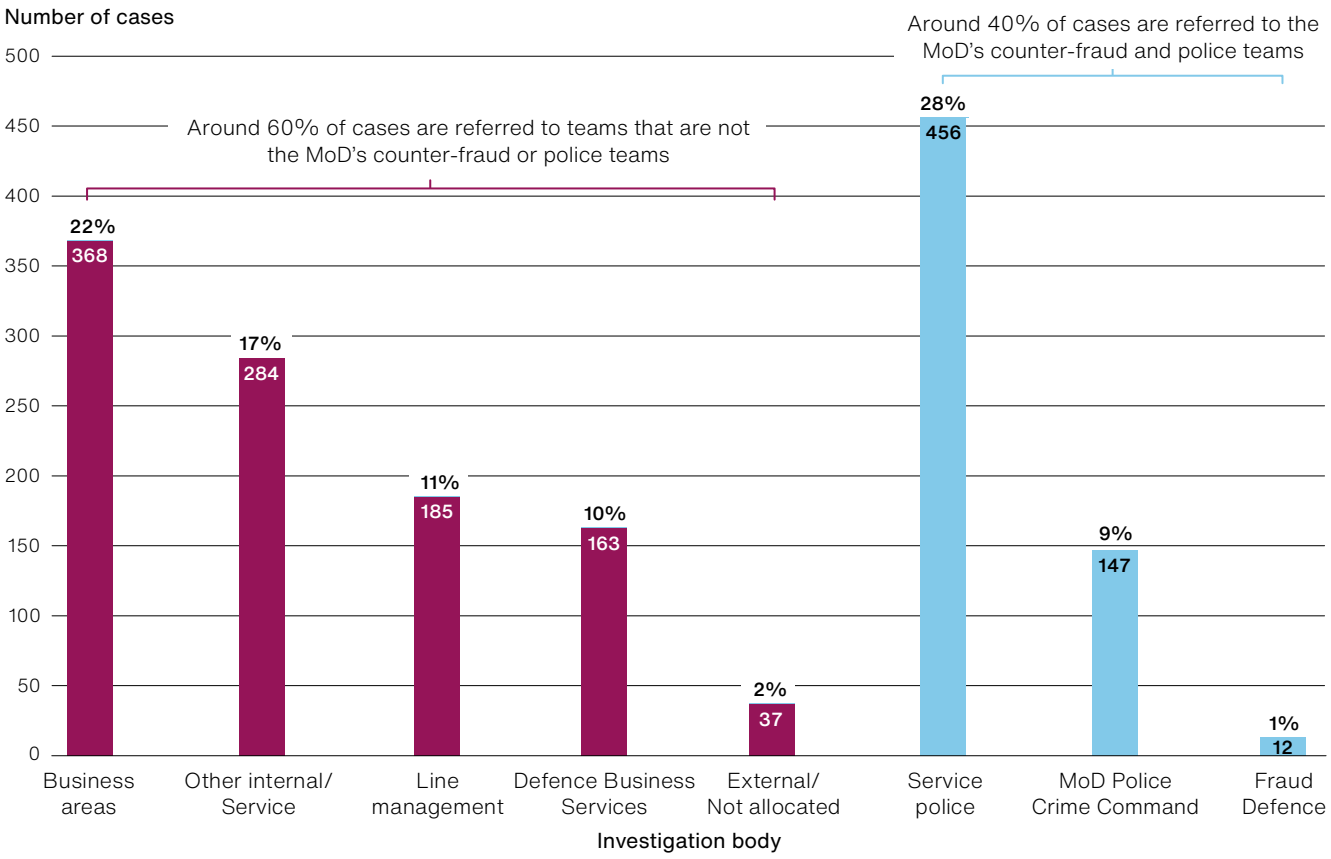
3.5 We found variation in the ability of different parts of the MoD to investigate reports of fraud. The MoD's network of 'Fraud Focal Points' is intended to act as a liaison point and to assist in the identification, prevention and investigation of suspected fraud. We found large differences in the amount of time Fraud Focal Points could dedicate to the role, and the impact they felt they could have. Several told us they spend very little time on their role as Fraud Focal Point, often because the role is taken on in addition to their usual duties. In addition, some Fraud Focal Points told us they were not always confident about how to progress some fraud cases.

3.6 Most of the 1,037 cases that had been referred to teams outside of the MoD's counter-fraud or police teams and that the Confidential Hotline records show as closed, were closed with no further action, mostly because no issue was identified or the MoD lacked evidence to pursue a case. But the MoD has limited assurance that the case had been properly investigated by the business unit and that closing the case was the appropriate outcome. Fraud Defence asks those it refers cases to for updates about the investigation, but does not assure the quality of those investigations. We selected a sample of 12 items from the Confidential Hotline that had been referred outside of the MoD's counter-fraud or police teams, and asked to be put in touch with the people who had investigated these cases, so that we could understand what investigations had taken place. In the majority of cases, updates were provided to Fraud Defence and the Confidential Hotline both during and at the conclusion of the investigation. However, a few of the contacts told us that it was not their role to update the Confidential Hotline with the outcome of the case because they did not consider them to be fraud cases.

Figure 7

Confidential Hotline data on cases that were referred to or at some point active with investigation bodies during 2024-25

The Confidential Hotline refers around 40% of cases to the Ministry of Defence's (MoD's) counter-fraud and police teams, and the rest to other teams such as business areas and line management



Notes

1 'Other internal/Service' investigation bodies include corporate governance, Defence Intellectual Property Rights, Defence Intelligence, Defence Internal Audit, Director of Resources, Directorate of Judicial Engagement Policy, Internal Regulator, Joint Personnel Administration auditor, Nominated Officer, Professional Standards Department – the Ministry of Defence Police, Professional Standards Department – Service, Chain of Command, Royal Marines, and Veterans UK.

2 'Service police' comprises the Royal Military Police, Royal Navy Police, Royal Air Force Police and Defence Serious Crime Command.

3 A small number of cases on the Confidential Hotline were assigned to two investigation bodies. In such instances these cases are counted to both investigation bodies.

4 There are additional investigations on police databases which the Confidential Hotline does not hold records for.

5 In addition to the cases shown above, 48 cases were yet to be referred to an investigation body.

6 Fraud Defence had a moratorium on investigating new cases identified between October 2023 and May 2025.

Source: National Audit Office analysis of data from the Ministry of Defence's Confidential Hotline database

Cases handled by the MoD's police teams

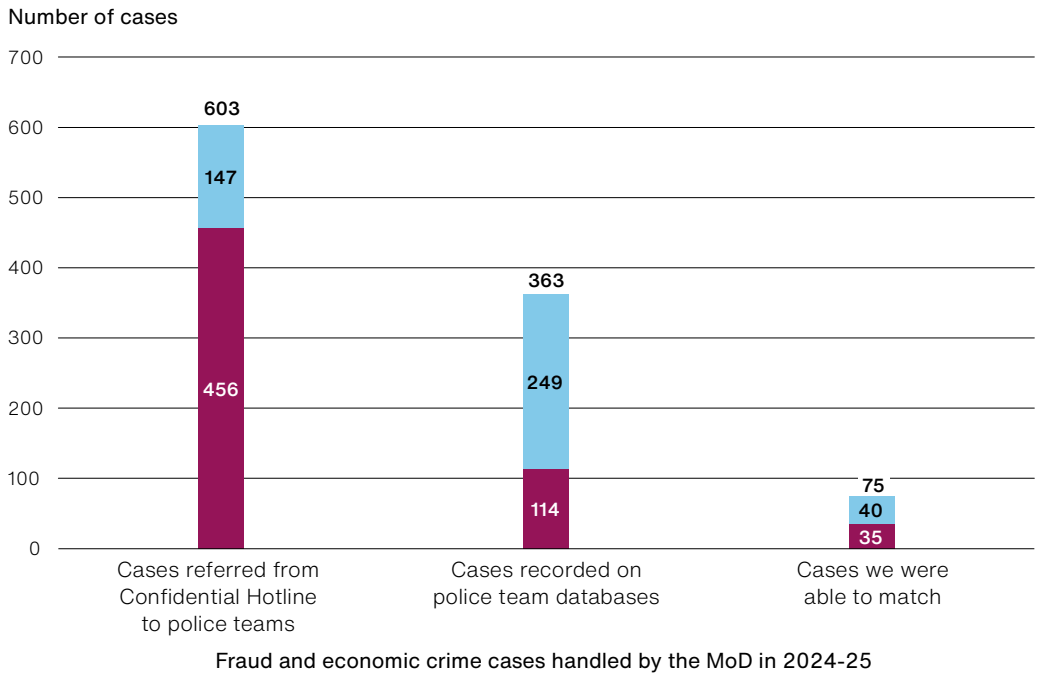
3.7 Similarly, the MoD does not always know and record how its police teams investigate fraud where the department may have been the victim. We found mismatches between the data held by Fraud Defence and the police authorities on ongoing investigations. The MoD told us its police can receive reports direct from the public, and the MoD's case management processes are very manual, with a number of hand-offs between teams. This makes reconciliation of case details difficult. Of the fraud cases active and on the Confidential Hotline in 2024-25, the MoD referred 603 (around 40%) to the Ministry of Defence Police Crime Command and service police teams. Separately, these teams provided datasets showing they investigated only 363 cases in 2024-25. We were only able to match 75 cases across the different systems (**Figure 8** overleaf). We asked the police teams to provide information about how a sample of cases referred to them were handled and found that some of the reasons for this mismatch included the following.

- **Cases closed without Fraud Defence being aware:** The police had closed some of the cases on its system, but for some of these it had not told Fraud Defence about this decision, and for others Fraud Defence was told but had not updated the Confidential Hotline.
- **Cases not recorded or investigated as crime:** The police determined that some cases did not reach the threshold for reported crime and treated them as 'intelligence'. This implies that the police team had a different view of what constituted a recordable and investigable crime than Fraud Defence, who had referred the cases to them. The police did not always tell Fraud Defence it had classified the case as intelligence and in some cases Fraud Defence was told but did not update the Confidential Hotline.
- **Cases not routed through the Confidential Hotline:** Some cases were received by police teams through separate reporting channels to the Confidential Hotline. While our sample was taken from cases referred to police from the Confidential Hotline, we were told that there were cases the police had not informed Fraud Defence about or where Fraud Defence had been informed but did not update the Confidential Hotline.
- **Cases where the reference number, which should be present across the Confidential Hotline and police data, did not match and could not be used to identify a case:** The police teams and Fraud Defence were able to conduct manual searches using more details of the case than the referral reference, and in doing so match more cases.

Figure 8

Fraud and economic crime cases in the Ministry of Defence's (MoD's) Confidential Hotline and police datasets that were open at some point in 2024-25

Of the cases referred to police from the Confidential Hotline we could match only a small number to police databases, showing that the MoD lacks complete, readily-available information on case progress



Notes

1 The service police consist of the Royal Military Police, Royal Navy Police, Royal Air Force Police and Defence Serious Crime Command.

2 Some of the reasons for why cases could not be readily matched include the police not always updating Fraud Defence on case progress, Fraud Defence not always updating the Confidential Hotline and the police receiving cases through channels outside the Confidential Hotline. Additionally, in some cases we were unable to match the case referral reference across systems. The MoD demonstrated that it was able to match more of these cases using more details of the case than the referral reference.

Source: National Audit Office analysis of data from the Ministry of Defence's Confidential Hotline and police case management systems

Outcomes from investigations

3.8 As well as low prevention and recovery figures (see Part One), the MoD's data suggest that investigations result in few outcomes that might serve as a deterrent to future fraud and economic crime. For example, of the 1,032 outcomes recorded on the Confidential Hotline in 2024-25, around 2% (18 outcomes) were criminal or service justice action. These took an average of 1.9 years to close. A further 18% (184 outcomes) were recorded as non-criminal outcomes, including formal actions such as dismissal and informal actions such as control improvements. For the remaining 80% (826 outcomes) the data show that no issue was identified or the MoD lacked evidence to pursue an allegation. These had been open for an average of 0.6 years before they were closed. Case data held by the MoD's police teams shows that 29 of the cases closed in 2024-25 resulted in a criminal or service justice outcome, such as prosecution or a caution, and took an average of 0.7 years to close. Most cases led to no criminal action or measurable financial outcome (**Figure 9** overleaf).

Figure 9

Outcomes from the Ministry of Defence's (MoD's) investigations into alleged fraud and economic crime that closed in 2024-25

The MoD's investigation bodies data record only a small number of cases that result in outcomes that could deter future fraud

Outcome	Confidential Hotline outcome	Average time taken to achieve outcome	MoD Police Crime Command (MDP) and service police outcome	Average time taken to achieve outcome
		(years)		(years)
Criminal or service justice action	18	1.9	29	0.7
Informal action	102	1	7	0.5
Formal action	82	1	4	1.1
No further action or unable to pursue	826	0.6	118	0.4
Other or not known	4	1	13	0.5
Overall outcomes achieved in 2024-25	**1,032**	**0.7**	**171**	**0.5**

Notes

1 The 'service police' consist of the Royal Military Police, Royal Navy Police, Royal Air Force Police and Defence Serious Crime Command.

2 Data, where available, show that the MoD achieved similar outcomes and times taken to achieve them in previous years.

3 Some outcomes recorded on the Confidential Hotline may also be included in the data provided by the MDP and service police.

4 The Confidential Hotline and police data use different definitions of case duration, which 'Average time taken to achieve outcome' is based on. The Confidential Hotline may not record a case as closed until all 'lessons learned' associated with a case are completed. This can be some time after other key dates such as the conclusion of the investigation associated with a case. By contrast, the police records note a case as closed when the police have concluded their investigation.

5 The 1,032 outcomes recorded in the Confidential Hotline relate to 909 unique cases. This is because there is more than one outcome listed for a small proportion of cases, often because a case can contain multiple allegations with separate outcomes, or because there are multiple outcomes from a single allegation. Of the 826 allegations reported as having an outcome of "No further action or unable to pursue", 18 also listed one of the outcomes such as "formal action", "informal action", or "criminal or service justice action." The MDP and service police data show one outcome per case.

6 Within 'criminal or service justice action', for the Confidential Hotline we included outcomes recorded as 'criminal/service justice action'. For MDP and the service police we included case outcomes recorded as 'charges/summons', 'adult caution', 'referral to Commanding Officer' and 'referral to the service prosecution authority'.

7 Within 'informal action', for the Confidential Hotline we included outcomes recorded as 'informal action', 'Cabinet Office internal fraud database referral' and 'control improvement'. For MDP and the service police we included case outcomes recorded as 'investigation not in the public interest – divisionary, educational or intervention activity' and 'community resolution'.

8 Within 'formal action', for the Confidential Hotline we included outcomes recorded as 'dismissal' and 'formal action'. The MDP had no cases categorised as formal action. After discussion with the service police we included cases that were either referred to another agency, including Home Office police forces, for further investigation, or were deemed appropriate to be investigated by a Commanding Officer from the offset. These cases may lead to administrative action but may also be escalated to service justice action.

Source: National Audit Office analysis of case data from the Confidential Hotline, the Ministry of Defence police and the service police

Part Four

Areas the Ministry of Defence could improve to realise greater savings from its counter-fraud work

4.1 In this part, we set out areas where the Ministry of Defence (MoD) needs to strengthen its response to fraud and economic crime if it is to achieve better results, and its plans to improve this in the future.

Objectives

4.2 The Defence Counter Fraud & Corruption Strategy 2023-2026 includes an objective to "*coordinate within the Defence Policing community a Whole Force response to ensure scarce investigation and intelligence capacity is leveraged for maximum impact and harm reduction*". But internal MoD reviews have raised concerns about the shared understanding of priorities, risks and opportunities between Fraud Defence and the police teams.

Structure

4.3 The MoD's response to fraud and economic crime is fragmented across several teams. This disjointed structure causes inefficiencies and can result in cases not being investigated by the most appropriate body. For example, Fraud Defence instituted a moratorium on new fraud investigations between October 2023 and May 2025, to clear a backlog of cases. The Ministry of Defence Police Crime Command (MDP) told us that over the same period it did not have a sufficient flow of complex cases to pursue. During the period of the moratorium, some cases that would have ordinarily been assigned to Fraud Defence were instead assigned to alternative investigation bodies. The fragmentation also means that no part of the system has the benefits of economies of scale, including the ability to build experience, or to justify the specialist resources to investigate economic crime effectively, such as digital forensics.

4.4 There is no single part of the MoD with overall responsibility to harness the various functions and their respective powers. In part, this is due to the necessity of retaining operational independence for the police services. Applying the Victims Code to the MoD could provide a framework for consulting with and updating the representative on all police investigations where the MoD had suffered an economic loss, while retaining police operational independence. The MoD's internal policy on Fraud, Bribery and Corruption already states that Fraud Defence should act as the 'single victim of crime' on behalf of the department for the purpose of fraud and criminal justice investigations. But our work has suggested this policy is not consistently used or working effectively when used.

Culture

4.5 Reviews of Defence policing have reported "*siloed working and inefficient working practices"* and the potential for *"unclear lines of reporting/accountability, duplication of work and missed investigative opportunities*". In particular, a 2023 peer review of MDP Crime Command highlighted a lack of trust between counter-fraud and police teams, and significant issues around collaboration and alignment. Some police officers told us that they did not see it as their role to update Fraud Defence on the progress or outcomes of the cases they are taking forward on behalf of the MoD, making it difficult for the MoD to understand and manage its overall fraud risk. The MoD told us this was improving and that, in the past year, a small number of commercial and police officials have been embedded into Fraud Defence. We were told that senior relationships are now more positive and focused on how the teams can work better together in the future.

4.6 We also found inconsistency in how seriously different parts of the MoD considered and responded to potential misconduct or fraud. Officials and police also told us that some areas of the MoD do not consider fraud to be a major risk and can be reluctant to engage.

Case triage

4.7 Fraud Defence and the police do not share a common view on whether items referred to the police are reported crimes (see paragraph 3.7). Internal reviews have found that the MoD as a whole lacks "*a coherent crime and risk threshold*" and that the rationale behind case acceptance for different investigation bodies is not clear. There is no monetary threshold for alleged case value that the MoD has agreed will be used in the various MoD teams to trigger investigation, and different teams are not aware of the criteria or thresholds different parts of the MoD use when deciding to pursue or prioritise a case.

4.8 The way that the MoD triages fraud cases out of the Confidential Hotline means that it may allocate them to the police before having exhausted more proportionate options to disrupt and recover losses. It also means that it assumes cases are being investigated when they may not be. We were told that, if the police look into a potential fraud and decide not to pursue a case criminally, there are no clear mechanisms for other parts of the MoD to continue looking at a case to see if non-criminal routes would be appropriate.

4.9 Although Fraud Defence has a small investigation team who could take significant non-criminal cases forward or work with the business areas to resolve matters, in practice the team largely considers its role to be the development of cases before handing them over to the business or Defence police authorities to investigate. Other public bodies, without their own in-house police services, may carry out more substantial internal investigation work before deciding that a significant allegation should be taken down a criminal investigation route.

Focus on prevention

4.10 The MoD's fraud risk assessments present an opportunity for the department to build preventative controls that can stop fraud happening. But the fraud risk assessments are not conducted across the whole department, are of varying quality, and are not consistently used to identify how fraud gets past the controls in place and to prevent future frauds (see paragraph 2.11).

4.11 The MoD also collects lessons learned on some cases to identify policy or process shortcomings and make improvements to minimise the risk of reoccurrence. Fraud Defence records 'control improvement' as the outcome for a small number of allegations. Similarly, Defence police authorities told us they identify lessons through some of their investigations. However, the MoD could not demonstrate that it has significantly reduced the occurrence of common issues through these processes. Some counter-fraud officials told us that they do not often see evidence of changes being made in response to lessons learned.

Data analytics

4.12 The MoD has conducted or commissioned several data analytics projects in recent years: a review of supplier 'master data' to detect procurement fraud; a deep dive into fraud within the Defence Infrastructure Organisation; and a project to develop a set of rules to identify high-risk transactions made with electronic purchasing cards. But, although these projects have identified potential fraud flags, the MoD has not demonstrated that they have produced significant savings or led to the introduction of preventative controls. The MoD has reported internally that some business areas lacked the capacity to investigate the flagged transactions in their area.

Intelligence-based prioritisation

4.13 The MoD's many fraud risk assessments have also not been translated into a comprehensive, 'ground-up' estimate of its fraud loss to inform where the MoD should prioritise its counter-fraud resources (paragraphs 2.3 and 2.11).

Case management and data

4.14 The MoD's data are not of sufficient quality or well-organised enough for it to manage its fraud and economic crime investigations effectively. The MoD's Confidential Hotline, overseen by Fraud Defence, is intended to be a central repository of all allegations and investigations of potential fraud across the MoD. But MDP and the service police have separate case management systems for recording fraud and economic crime cases (**Figure 10**). The different systems show multiple fields with incomplete data, use different definitions for key fields such as 'case closed', and cannot be used to extract meaningful management information that would allow the MoD to manage its fraud risk. There is no automation or linking across these systems, and referral references which are meant to allow identification across systems are often not helpful in performing this task, which meant that we struggled to follow cases through from allegation to closure. Where items can be identified on more than one system, the data often disagree.

Figure 10

Case management systems used by the Ministry of Defence's (MoD's) counter-fraud and police teams

Counter-fraud teams in the MoD use different case management systems which record different data, have different capabilities and cannot be easily connected

	Confidential Hotline data	MoD Police Crime Command (MDP) data (UNIFI)	Service police data (CONNECT)
Examples of key information recorded	Unique IDs, date of allegation, fraud types, financial information, investigation bodies, outcomes, case closure date.	Unique IDs, date of case creation, fraud types, outcome.	Unique IDs, fraud types, case summaries, service investigation body, status, date for incident reported, outcomes, disposal date.
How the MoD can use data from the system to manage fraud	Able to run reports that include information listed above.	Able to run reports that include information listed above.	The service police have set up regular reporting based on data from CONNECT.
Limitations to using data to manage fraud	Cannot be automatically linked to other case management systems. Contains case references that should link to other case management systems. However, without further details of an investigation, these cannot consistently be used to identify cases on other systems.	Cannot be automatically linked to other case management systems.	Cannot be automatically linked to other case management systems.
	Many fields are empty and significant cleaning is required for available data to be usable.	Unable to export data for dates of outcomes and any financial information without manually adding data.	
Key definitions used			
Case duration	When lessons learned exercises are complete, which can be some time after other key dates such as an investigation closing.	When a case is no longer being actively investigated, this does not incorporate any dates for later outcomes (e.g. trial dates).	Separate records for when an investigation part of a case is complete (e.g. a decision to drop a case or charge has been made), and for later outcomes.
Outcomes and fraud types	Own definitions for both, not aligned to other systems.	Uses Home Office definitions for both.	Uses Home Office definitions for both.

Note

1 The service police consist of the Royal Military Police, Royal Navy Police, Royal Air Force Police and Defence Serious Crime Command.

Source: National Audit Office analysis of the Confidential Hotline case management system, the Ministry of Defence Police UNIFI system, and the service police CONNECT system

Steps the MoD is taking to improve

4.15 The MoD had already identified some of these issues and has ambitions to address them. The MoD told us that:

- it is close to producing an enterprise-level fraud risk assessment, which will help facilitate discussions on risk appetite with the Accounting Officer;
- it plans to incorporate an organisation-level shared objective on tackling fraud in its next Defence Counter Fraud Strategy;
- police staff have been embedded to work in the Confidential Hotline team alongside Fraud Defence officials;
- Fraud Defence and the police have been working jointly on a new investigative model for fraud and economic crime – which could include joining police and Fraud Defence case management systems;
- Fraud Defence has been engaging with the MoD's commercial teams – as a source of intelligence for fraud activity, a source of expertise for contract issues, and to identify any previously unrecorded contributions to the department's fraud prevention figures;
- Fraud Defence is reprioritising its resources to focus on recovery, intelligence and analytics, and exploring the use of artificial intelligence; and
- Fraud Defence has identified commercial leakage as an area to target for increased detection and recovery, building on recent successes (see paragraphs 2.8, 2.9 and 2.15).

Appendix One

Previous reviews of Defence policing

1 The Ministry of Defence has conducted or commissioned several reviews of Defence policing that highlighted problems relevant to its management of fraud and economic crime. **Figure 11** on pages 42 and 43 shows the issues raised across different reviews.

Figure 11

Concerns raised in past reviews relevant to the Ministry of Defence's (MoD's) management of fraud and economic crime

Previous reviews of Defence policing have highlighted issues including siloed working, unclear objectives and inefficient working that are relevant to how the MoD manages fraud and economic crime

Review title	Nature and scope of review	Publicly available?	Extent of focus on fraud and economic crime	Review findings				
				Siloed working	Dysfunctional relationships	Lack of clarity on roles and objectives	Concerns about criminal investigations	Inefficiencies/ duplication of work
Service Justice System Policing Review (Part 1) **(Murphy, 2017)**	Independent review of the structure and skills of the service police and Ministry of Defence Police.	Yes	Minor	X		X		X
Service Police Transformation Report **(Finance and Military Capability, 2018)**	Internal review of the service police to identify inefficiencies, led by the MoD's Finance and Military Capability function.	No	Minor			X		X
A Study into the Service Justice System **(Davis & Pratt, 2019)**	Internal study examining the requirement and best framework for a separate system of justice for service personnel.	No	Minor	X		X		X
Review into the Framework, Processes and Skills that the Service Justice System Requires for Overseas Operations **(Henriques, 2021)**	Independent review of the MoD's handling of allegations of serious criminality in overseas operations.	Yes	Minor	X		X		X
Peer Review of Ministry of Defence Crime Command **(T/ACC Parkes, 2023)**	Review of Crime Command's capabilities and relationship with Fraud Defence, led by officers from external police authorities.	No	Significant	X	X	X	X	X
Defence Policing Security and Guarding Review **(DPSGR Programme Board, 2023–2024)**	Internal review of the MoD's policing operating model, including serious and economic crime.	No	Significant	X		X		X
Fraud Defence Investigators Case Conduct **(Cost Assurance and Analysis Service, 2025)**	Report examining the alignment of records held by Fraud Defence Investigations and the Confidential Hotline, led by the MoD's Cost Assurance and Analysis Service.	No	Significant			X		X

Note

1 The MoD is undertaking two further reviews that relate to Defence policing: one focusing on the governance of service policing and another on options for the most effective delivery of Defence policing. The MoD aims for these reviews to resolve the long-standing issues raised by past reviews and expects to provide recommendations during 2026.

Source: National Audit Office analysis of internal Ministry of Defence reviews and independent reviews by external parties

Appendix Two

Our investigative approach

Our scope

1 We have received whistleblowing disclosures over recent years indicating that individual allegations can take a long time to resolve or do not reach a satisfactory resolution, and that overall the Ministry of Defence (MoD) could manage fraud and economic crime far more effectively. This report investigates and provides transparency over the MoD's management of its losses from fraud and economic crime. It covers:

- how the MoD is set up to make savings by tackling fraud;
- the MoD's understanding of its fraud risks;
- how the MoD handles fraud investigations, and the outcomes of its work; and
- areas the MoD could improve to realise greater savings from its counter-fraud work.

2 We conducted fieldwork from July 2025 to November 2025.

Our evidence base

Quantitative analysis

3 We gathered data on fraud and economic crime cases from MoD databases and analysed this to understand the number and types of fraud that the MoD handles, and outcomes from this work. Data from the following systems were used:

- The Fraud Defence Confidential Hotline case management system;
- The Ministry of Defence Police UNIFI database; and
- The service police CONNECT database.

4 We analysed data from the various databases, but mostly used Confidential Hotline data to understand how the MoD manages fraud and economic crime. The Confidential Hotline data is intended to act as a central repository of allegations and investigations across the department. We conducted our analysis between August 2025 and November 2025.

5 Items reported to the Confidential Hotline are recorded under a unique case ID. Each case ID may contain multiple allegations covering different fraud types, with associated financial values and outcomes. In this report, the term "case" refers to the full Confidential Hotline record with a single unique case ID. For example, a case may include multiple fraud types, but the whole case is referred to an investigation body. "Allegations" referred to in this report are where all details within a single case are treated separately. For example, where a single case contains two alleged fraud types, we would treat those as two separate allegations.

6 Many figures in the report about the reports of potential fraud the MoD receives and investigations it conducts use data specific to 2024-25 and for some of these data sources, we have further information available for earlier years. We have conducted small amounts of further analysis on these previous years. We are content that presenting 2024-25 data is appropriate to provide an up-to-date view, and that this does not present significantly different findings than if we had included the data for earlier years.

7 This report uses Cabinet Office records derived from the MoD's submissions about its counter-fraud resource and the savings it achieved. Where possible, we have conducted small amounts of analysis to compare the MoD's submissions to Cabinet Office with the records shown on the MoD's Confidential Hotline. These did not align exactly but the two data sources suggested a broadly consistent level of performance and differences may have been a result of timing differences or other adjustments.

8 The NAO's analysis hub performed some exploratory work to determine if they could perform digital 'process mapping' of hand-offs and case progress across the MoD. This was mostly inconclusive because of the issues with the MoD's data, some of which we set out in the report.

Sample testing

9 Through our work, it became clear that there were mismatches between the Confidential Hotline data and the police data on ongoing investigations. There was no automation or linking across the systems, and referral references which are meant to allow identification across systems were often not helpful in performing this task. The Confidential Hotline data indicated that 603 cases had been referred from the Confidential Hotline to the police that were active at some point in 2024-25, while the police data indicated there were 363 cases being investigated. Using the referral references, we were able to link 75 cases between the Confidential Hotline and police data provided.

10 To understand this mismatch, we selected a sample of 20 referrals from the Confidential Hotline to the police and asked for information to understand the extent to which Fraud Defence, as the MoD's central counter-fraud team, had sight of the outcomes of cases it referred. We found that the police did not always update Fraud Defence on case progress or on whether a case was being treated as intelligence rather than reported crime, that Fraud Defence did not always update the Confidential Hotline following updates from the police, and that the police received cases through channels outside the Confidential Hotline. The police teams and Fraud Defence did demonstrate that they were able to conduct manual searches using more details of the case than the referral reference, and in doing so match more cases.

11 Separately, we also examined a sample of 12 cases that had been referred by the Confidential Hotline to parts of the MoD outside of its counter-fraud and police teams. We asked to be put in touch with the people who had investigated these cases, to understand details of the case and to understand the extent to which Fraud Defence had assurance that cases were properly investigated.

Interviews with MoD officials

12 We interviewed a wide range of MoD stakeholders, including:

- Chief of Defence People;
- Director of Assurance;
- Head of Fraud Defence;
- Various other Fraud Defence officials, including those in roles relating to risk assessment, analytics, investigations and training;
- Chief Constable of the Ministry of Defence Police;
- Provost Marshal (or Deputy) of the Royal Military Police, Royal Air Force Police and Royal Navy Police;
- Deputy Provost Marshal of the Defence Serious Crime Command;
- Deputy Head of the MoD's Cost Assurance and Analysis Service;
- Officials responsible for leading the MoD's most recent review of policing (the Defence Policing Security and Guarding Review); and
- 'Fraud Focal Points' from across the business.

Interviews with stakeholders outside the MoD

13 We interviewed stakeholders outside the department so we were able to better understand how other organisations managed allegations of fraud and economic crime:

- Public Sector Fraud Authority (PSFA, various officials);
- HM Revenue & Customs (investigations unit);
- Home Office (investigations unit);
- Department for Work & Pensions (investigations unit);
- Government Internal Audit Agency (investigations unit);
- City of London Police; and
- His Majesty's Inspectorate of Constabulary and Fire & Rescue Services.

14 Interviews took place between July 2025 and October 2025, and were conducted online.

Document review

15 We reviewed a range of MoD documents across several key work packages. The work packages were designed to ensure we had a strong understanding of how the MoD manages fraud and economic crime, and to help with identifying areas it can improve. The main work packages involving significant document review were as follows.

- **Mapping roles, responsibilities and resourcing:** This work included reviewing terms of reference, MoD organograms, and returns made by the MoD to Cabinet Office including Workforce and Performance Reviews and Consolidated Data Returns.
- **The MoD's understanding of its fraud risks:** This work included reviewing fraud risk registers, Initial Fraud Impact Assessments, strategic risk assessments held by parts of the MoD, and the PSFA's GovS013 assessment of the MoD's fraud maturity.
- **The MoD's internal reporting and governance:** This work included reviewing board minutes, Audit Committee papers, fraud dashboards, statistics on 'security incident' reporting forms, Government Internal Audit Agency reports, and information about the MoD's counter-fraud key performance indicators.
- **The MoD's response to previous reviews:** This work included reviewing previous reviews relevant to the MoD's management of fraud and economic crime.
- **The MoD's plans for improvement:** This work included reviewing proposed operating models and information about ongoing reviews.

16 Our review of documents was carried out between August 2025 and November 2025.

This report has been printed on Pro Digital Silk and contains material sourced from responsibly managed and sustainable forests certified in accordance with the FSC (Forest Stewardship Council).

The wood pulp is totally recyclable and acid-free. Our printers also have full ISO 14001 environmental accreditation, which ensures that they have effective procedures in place to manage waste and practices that may affect the environment.

National Audit Office

Design and Production by NAO Communications Team
DP Ref: 016946-001

£10.00
ISBN: 978-1-78604-655-0