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

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.