Ministry
of Defence

PERMANENT SECRETARY

JEREMY POCKLINGTON CB
MINISTRY OF DEFENCE
FLOOR 5, ZONE D, MAIN BUILDING, WHITEHALL
LONDON SW1A 2HB

Telephone: 020 7218 7975
Fax: 020 7218 3048
E-mail: PUS-PrivateOffice@mod.gov.uk

D/PUS/11/7/1(24)

Sir Geoffrey Clifton-Brown MP
Chair, Public Accounts Committee

20 March 2026

Dear Sir Geoffrey,

Management of Fraud and Economic Crime by the Ministry of Defence

I am writing following the oral evidence session held by the Public Accounts Committee on 5 March 2026, at which I gave evidence alongside Aneen Blackmore, Director General Finance, Jim Carter, Director General Commercial & Industry and Acting Chief Constable Simon Dobinson, Ministry of Defence Police. I undertook to provide the Committee with further information on topics raised during the session.

<u>Blocked Invoices</u>

You quoted an Accountancy Age report that the MOD had blocked over £211 billion of suspicious invoices in 3 years, and asked what had happened to the blocked invoices.

This article was based on a Freedom of Information response from the Department, which made clear that the value of blocked invoices was abnormally high in 2022/23 because of a single rejected invoice of £210 billion, caused by a typographical error by a supplier.

Supplier invoices received by the Department are processed through the Oracle Contracting, Purchasing and Finance system and are subject to robust automated controls. Invoices are required to reference a valid purchase order and are validated through a three-way matching process between the invoice, the purchase order, and confirmation of receipt of goods or services.

Where an invoice cannot be validated, it is either placed on hold or formally rejected. Invoices placed on hold are not paid and remain blocked in the system pending corrective action, such as confirmation of receipt, correction of quantities or prices or resolution of data errors. Automated workflows notify the relevant MOD business owners, and escalation processes apply where action is not taken within defined timescales.

Invoices are formally rejected where issues cannot be corrected in a straightforward manner, for example where no valid purchase order exists, contractual limits have been exceeded, or the invoice fails system validation checks. This includes duplicate invoice controls and contractor code errors, which are the most common cause. Rejected invoices are not paid and suppliers are required to submit new corrected invoices where appropriate. The rejection of an invoice does not imply fraud.

These controls form an important part of the Department’s framework for preventing error, the misuse of public funds, and economic crime. No blocked invoice is paid unless all required controls are satisfied. The invoices to which the Committee referred during the evidence session will have been subject to this process.

Use of Advanced Analytics

You asked how advanced analytics could help us to detect incorrect invoices.

The Oracle Fusion Cloud solution is currently in the design and configuration stage, as a replacement for existing finance systems. It will bring more advanced data reporting tools and monitoring technology into day-to-day finance operations. The Fusion software suite includes automated (and human-in-the-loop) error and fraud detection reporting through a dedicated 'Risk Management' application. This will enhance financial audit and compliance capabilities, alongside improved user access controls.

Artificial Intelligence is embedded throughout the Oracle toolsets and applications, including analytical tools which can be leveraged to assist the MOD in identifying and reporting unwanted invoice activity. The use of an embedded supplier portal in this solution enables better communication with suppliers on invoice queries.

We are also developing enhanced “commercial leakage” capability through cloud analytics which will be rolled out more widely. That said, whistleblowers continue to be a key source of information in detecting fraud, including for the kinds of cases outlined in the Accountancy Age article.

Counter Fraud Strategy

As I explained during the session, we will publish our refreshed Counter Fraud Strategy in September and I will write to the Committee then with a fuller summary of the Strategy.

Estimate of Fraud Risk

We discussed during the hearing the complexity of developing a more accurate and granular estimate of our fraud risk exposure. I recognise the importance the Committee attaches to this issue, and the Department is prioritising this work: we have been engaging with other public sector bodies and external advisers on how to progress at pace. I noted that we have been advised by the NHS Counter Fraud Authority that it is an extensive task, but we are learning from their experience. The work will involve understanding the inherent fraud risk exposure, based on our new enterprise risk register; assessing the effectiveness of the fraud risk control landscape; and then calculating the residual fraud risk exposure. In some cases we will have good data from existing fraud detection, but in others benchmarking may be necessary as assessing procurement fraud risk is particularly challenging. I would expect the work to run over about a year, with initial assessments of the less complex categories by the end of 2026. We will set out a phased plan with delivery dates in the Counter Fraud Strategy which will be complete by September this year. I will share this with the Committee when I provide a summary of the Strategy after its publication.

I am grateful for the interest of the Committee in this issue, and reassure you that the effective management of fraud and economic crime remains a high priority for the MOD.

Yours sincerely,

Jeremy Pocklington