

Public Accounts Committee

Oral evidence: The MoD's tackling of economic crime and misconduct, HC 1733

Thursday 5 March 2026

Ordered by the House of Commons to be published on 5 March 2026.

[Watch the meeting](#)

Members present: Sir Geoffrey Clifton-Brown (Chair); Mr Clive Betts; Sarah Green; Rupert Lowe; Catherine McKinnell.

Gareth Davies, Comptroller and Auditor General, Joshua Reddaway, Director, National Audit Office, and Marnya Jain, Alternate Treasury Officer of Accounts, HM Treasury, were in attendance.

Questions 1-63

Witnesses

I: Jeremy Pocklington CB, Permanent Secretary, MoD; Aneen Blackmore, Director General Finance, MoD; Jim Carter, Director General Commercial, MoD; and Simon Dobinson, Acting Chief Constable, Ministry of Defence Police.

Report by the Comptroller and Auditor General

The Ministry of Defence's management of its losses from fraud and other economic crime (HC 1596)

Examination of witnesses

Witnesses: Jeremy Pocklington, Aneen Blackmore, Jim Carter and Simon Dobinson.

Q1 Chair: Welcome to the Public Accounts Committee on Thursday 5 March 2026. With high expenditure, complex procurement and a workforce split between the armed forces and the civil service, the Ministry of Defence faces particular challenges against the backdrop of a significant threat of economic crime and misconduct. As the Government move to fulfil their commitment to increase defence spending to 2.5% of GDP by 2027, exposure to threats is only set to grow.

Although the MoD receives hundreds of allegations of suspected fraud or economic crime each year, relatively few result in detection, disruption and recovery. The MoD reports that its potential exposure to fraud can reach £1.5 billion a year, mostly from procurement. However, that is only a broad estimate. Although the MoD recovered more than it spent on counter-fraud work in 2024-25, over the last four years it has on average recouped just 48p for every pound spent—substantially below the Government's expectation of £3 for every pound spent.

Today's session is an opportunity to challenge the MoD on how it maintains its central view of counter-fraud activity, consider plans to improve the counter-fraud culture and leadership, and explore how the MoD can achieve better outcomes from its counter-fraud work. We are very pleased to have with us a senior team from the MoD. A warm welcome, Jeremy, and congratulations on your promotion to permanent secretary; I hope you are still happy about the promotion, given the challenges you have. Will the witnesses please introduce themselves?

Jeremy Pocklington: I am Jeremy Pocklington, the permanent secretary at the Ministry of Defence. I was formerly the permanent secretary at the Department for Energy Security and Net Zero, and before that I was the permanent secretary at the Ministry of Housing, Communities and Local Government.

Aneen Blackmore: Good morning. I am Aneen Blackmore, the director general of finance at the MoD.

Jim Carter: Good morning. I am Jim Carter, director general of commercial and industry at the Ministry of Defence.

Chair: And finally, but by no means least, Simon.



HOUSE OF COMMONS

Simon Dobinson: Good morning. My name is Simon Dobinson and I am the acting chief constable of the Ministry of Defence police.

Chair: Thank you all very much for coming. I know you are busy people.

Q2 **Catherine McKinnell:** Good morning. I want to ask about a couple of the points the Chair highlighted in his opening comments. The Ministry of Defence is responsible for huge-scale contracts and billions of pounds of public money, and, clearly, counter-fraud initiatives could not be more important. As the Chair mentioned, the Treasury expects savings of £3 for every £1 spent on counter-fraud measures. Jeremy, could you explain why the MoD has saved only 48p in every £1 over the last four years?

Jeremy Pocklington: Can I start by welcoming the Report and today's hearing? Everyone on the panel, but especially myself as accounting officer, takes safeguarding taxpayers' money incredibly seriously, given the scale of the spend and the work of the Ministry of Defence. Our job is to maximise the impact of every pound we receive so that that can be spent on improving the warfighting capability of our military. That requires a whole set of robust financial and commercial controls, which are absolutely part of the picture we are talking about today. Of course, we also need specific controls in place around fraud, error and economic crime.

The Department is making good progress, but the Report reflects a lot of work that we already had under way, and that we want to go further on in the Department to strengthen our controls in this place. In particular, on the specific issue you raised, in respect of the spend and return on investment, we have already seen a significant upward trend. The most recent data showed £1.34 returned on every £1 spend, and that reflected the increased use of new tools and techniques, and better analytics as well. We think we are on track to receive the Public Sector Fraud Authority target of 3:1 by 2028, if not sooner.

Why were the numbers lower in the past? We think we need to do more to record the benefits and the impact of our recovery, which may have affected some of the data. That partly reflects, as the Chair referred to in his opening statement, the complexity of the operating environment, but we are in no way complacent, and we recognise that we need to do more to capture the benefits and make sure that we are wholly focused on this important issue.

Q3 **Catherine McKinnell:** Can I come back to your assessment of good progress? That is not the reflection that I took from the Report, so it would be really helpful to understand where you see good progress being made and how you are confident about your trajectory. From what I understand, the reason why there is a slight improvement on the 48p in the pound is that there was a one-off recovery, as opposed to there being a trajectory in the pattern of recovery. Could you explain that discrepancy and where you see the trajectory improving, because the Report does not indicate that to me?



Jeremy Pocklington: The Report does suggest elements of the progress we have made, and I am confident that I have seen evidence of that in my first few months at the Department. We will talk in more detail about that during this hearing. It reflects the fact that there is already closer joint working between the different elements of the Department and the Ministry of Defence police, represented by Simon today, but also the service police forces in the Service Justice System. We have already made progress on that. An example would be the police embed in our defence fraud team, improving our focus and making sure there is better alignment between the Department and the police.

We are strengthening our systems of accountability in the Department, and our capability as well, and we are focusing more on how analytics can help us with recovery. We are investing in new tools and techniques that enable us to leverage technology to really enable us to—I would summarise it as—identify irregularities in the system that need to be explored further by our fraud experts. Our policy is very clear: we have a zero-tolerance policy on fraud, and all allegations are investigated. But we do need to go further, as is set out in the Report.

My team—my Department—is refreshing the counter-fraud strategy. Some of the steps have already been set out, and we will have an implementation plan around that. It is a three-year strategy, and the three years are coming to an end, so now is the time to refresh our counter-fraud strategy. That is going to include, for example, work on getting a better estimate of fraud exposure. You have already alluded to the quite theoretical estimate in the Report; we will have clearer objectives as part of a very important, quite fundamental, set of reforms at the Department, under defence reform. We will clarify accountabilities. We will have new oversight of risk registers. We are improving and consolidating our approach to the confidential hotline and the case management system, and how our teams work together in order to go after this issue.

Q4 **Catherine McKinnell:** Are you confident that by next year we are going to see a significant increase on that 48p in the pound recovery?

Jeremy Pocklington: I think we have already seen an increase on that 48p in the pound recovery. But I recognise—

Catherine McKinnell: Sorry; I think we need to be clear that the £1.34 appears to be a one-off, because there was a review of commercial leakage that brought about a one-off recovery. Putting that to one side, are you confident that, overall, we are going to see an increase on the 48p in the pound, which is already well below the £3 in the pound that the Treasury expects?

Jeremy Pocklington: I am confident that with our approach we will see improvements, particularly through greater analytics. On the £1.34, I recognise that you want to see more evidence of the trend, but it is a real fact.

Q5 **Catherine McKinnell:** I absolutely acknowledge that it is a real fact—it is



noted very clearly in the Report—but it does not necessarily solve the underlying challenges of how we improve the situation. With respect, it does not feel like there is an acknowledgment of the scale of the challenge; that is my impression, having read the Report. But I am happy to get into a bit more of the detail.

Jeremy Pocklington: What we should do is to get into the detail of the counter-fraud strategy we are working on and the many steps we are taking.

This is all part of a wider system of financial controls and commercial controls in the Department. We need a balanced approach, looking at prevention, detection and recovery. Prevention is incredibly important, and that also means looking at the wider context of the Department and the controls we have in place. We do spend very large amounts of money. You could use different definitions, but roughly £40 billion is spent on procurement—that is the number in the Report. A bit under half of that—again, it depends on exactly how you count it—is through the single source contracting regulations. They are very specific and tight regulations that reflect the fact that in the Ministry of Defence it is not always possible to compete on our contracts. That gives the Department particular access, in open-book arrangements and benchmarking arrangements, to identify what is happening with our suppliers.

None of that is to take away from the importance of this issue, and the serious risk it is in a Department like the MoD—as it is in many Government Departments, but we have a particular reason to be focused on it—and the recognition that we need to continue our efforts and do more.

Q6 Catherine McKinnell: Okay; thank you. Jim, what are you doing to make sure that your commercial teams are increasing the counter-fraud savings and that we see an improvement on the 48p in the pound that is currently the trajectory?

Jim Carter: It is probably helpful context for the Committee if I quickly set out the commercial controls framework that Jeremy referenced, and then I will answer your specific question. There are controls throughout the contract life cycle to consider, prevent and minimise fraud, including by embedding rigorous prevention and enforcement measures.

At the top level are the joint services publications, which define our zero-tolerance stance, and then there are the specific commercial policies that underpin that, related to bid rigging and collusion. Also, the Procurement Act 2023 gave us exclusions and debarment policy, so that if suppliers are guilty of fraud, we can debar. Underneath that, we have mandatory contract clauses and supplier ethics oversight to minimise fraud. Working very closely with Aneen, we have strict segmentation of duties, following the Government's functional standards.

Post award, our contract management and supplier relationship management processes mitigate fraud, and we have anti-counterfeit and IPR protections in our supply chains. I am trying to describe a nested set

of controls that particularly focus on preventing fraud and protecting public money.

Q7 Catherine McKinnell: I guess the question is whether they are working.

Jim Carter: On Jeremy's specific point about recovery, I also have confidence, because we are deploying more widely the technology that we use to identify and recover. We applied it to a particular kind of business unit, and we can apply it more widely. I would be happy to talk to the Committee about the opportunities we see ahead in terms of some of those digital tools can reduce fraud.

Q8 Catherine McKinnell: Are you confident that you have sufficient sight of what is happening throughout that chain of process in order to minimise the fraud risks? I appreciate that you have outlined what the policies are, but what is the reality on the ground? The indications are that there isn't sufficient oversight, so how are you making sure that there is?

Jim Carter: There are opportunities to improve that. I totally agree with Jeremy that we are not complacent. I think we have good controls. Whether it is in our single source environment, which I can talk more about, or in our competitive environment, our processes follow really good practice in terms of the segregation of duties, independent moderation of our approach, and an assurance, scrutiny and approval process that makes sure there is independence. The opportunity we have through analytics is to use technology to spot some of the flags and some of the irregularities, so that we can home in on and focus on where they are occurring.

Q9 Catherine McKinnell: Could you explain that? As I said, in the last four years, the figure is 48p in every pound. Can you explain what is being changed in order to improve that?

Jim Carter: It is the use of some of those technologies so that we have the preventive frameworks I have described and can detect irregularities more. We are engaging in implementing new tools for our commercial and finance colleagues through corporate services modernisation, and we are embedding in our processes those fraud-prevention flags, at every stage of the procurement cycle, so that we capture them.

Jeremy Pocklington: Can I come in here? There is a risk of a bit of confusion during this hearing, and I think it is important that we unpack the different issues early on.

We have in place specific teams and measures on the very specific issue of fraud, led by the fraud defence team, which is a team of about 24 people in the core Department of State bit of the Ministry of Defence, and there are about 50 or so experts in total in the wider Department. They undertake specific activities using specific tools and techniques, but they are embedded and part of a much bigger system of financial and commercial controls. The PSFA also does not measure the wider finance and commercial controls in all the detail. We need to look at the whole picture to get a proper assessment of the success and controls that the

Department has in place, while again recognising that we need to do more.

I will give you a specific example. We have already alluded to—Jim talked about this—the single source controls. We have an absolutely class-leading cost assurance and analysis service, which is part of that system. The billions of pounds of spend that go through single source are examined in detail to ensure that suppliers' costs are genuine. Where necessary, those costs are disallowed or even, in some cases, payments are recovered. That is when suppliers are incorrectly allocating overheads, their estimates are not supported or their labour rates are not actually consistent with the market.

Last year, that team disallowed £400 million of potential cost that the Department would have incurred. That is, and they are, evidence of the robust controls that the Department has in the place to protect the taxpayer, but they are not captured in that 48p return you alluded to, which is a very specific subset of this. We need to do more on that, and the key there will be analytics—that is what will make the difference to increase the return on investment in that particular bit of activity. What I am encouraging the Committee to do is not only look at that but see this as part of a broader picture.

Q10 Catherine McKinnell: Okay; thank you. Aneen, I want to ask about the fraud defence team's work and the 130 bespoke risk registers that you operate to. Some have severe and critical activity risks but have not been updated or acted on—some of them for up to five years, it says in the Report. Do you have a sense of how well those existing controls are operating? What are you doing to ensure that they are operating at their maximum effectiveness?

Aneen Blackmore: You are absolutely right to note that we have an established regime of risk registers in place throughout the organisation. As the Chair noted in his opening remarks, we have a large-scale, complex organisation, which requires risk registers at each level so that we are driving our best understanding.

Let me share a little bit about how we are improving the registers, and then how we are going to use them to drive focus on where we want to ensure that we have resources and investment going forward. As Jeremy alluded to, that will be part of how we improve our return on investment and drive value for the taxpayer.

As you will all be aware, defence reform has restructured the Department. We will be taking this opportunity to review how we are structuring our risk registers to match the broader governance in the Department, and we have an enterprise risk register framework that we have developed recently. That will be rolled out this year so that, from the board downwards, we will be nestling our risk registers in a consistent framework. The fraud defence team is now working with each of the new areas to ensure that they have a risk register at the area level.



HOUSE OF COMMONS

Below that, we will then be maturing the well-established risk registers that already exist in our frontline commands in enabling organisations. Below that, we will again focus on our programme risk registers. As the NAO Report highlighted, we were really pleased that we have ensured that all 22 of the major programmes where we asked for an initial fraud assessment were completed to the relevant standard.

We are absolutely not stopping there, though. As we speak, we are rolling out the Public Sector Fraud Authority's accelerator tool, which will allow us to produce risk registers more quickly to a data-consistent standard, so that we can roll that out more broadly. That ensures that we have the right structure in place that nestles into a consistent framework, and we can drive activity and focus from the board downwards. As you rightly allude to though, the challenge then is making sure that we are actively using them and that we are using them to ensure that we are focusing our resources, both people and investment in new tooling, in the places where we think it will make the most difference.

To support that—and we will set this out in our counter-fraud strategy refresh that Jeremy alluded to—we will set out how we expect the risk registers to be used. We will be building a programme of work on the back of that to say where we should invest. The commercial leakage tool is a good example of some of that early intervention, where we are proactively saying, "This is where our risk sits. It is not where we get the majority of the fraud allegations, but we know this is where our material risk sits, so how can we get after that more proactively?"

Really importantly, we are also strengthening the functional oversight. That will be through my role as DG finance. That strengthening will allow us to use the risk registers in a more focused way, holding the organisation to account for their activities.

Q11 Chair: Thank you very much for those excellent opening questions, Catherine.

Permanent secretary, as a point of clarification, I want to pick up on one important thing you said, for your refreshed plan. The Government have pledged to go to 2.5% of GDP, so you are going to get another £11 billion-odd in the next financial year.

I would have thought that the refreshed plan is absolutely urgent, because clearly the potential fraud with that increased budget must be going up considerably. When will the refreshed plan be available, and will you publish it in full? In order not to try and guide you on the answer on that, some Departments are a little bit shy about publishing everything on fraud, because you don't want to give the fraudsters too much information.

Jeremy Pocklington: Exactly. That is an important point in my mind. The first thing I would say is that we already have a plan that we are working on improving. This is part of our three-yearly process, which is why we



HOUSE OF COMMONS

welcome the Report, which has come out at just the right time, actually—as we are finalising our plan.

We are working to complete the new plan by September. Perhaps I can write to the Committee with a summary of the plan—would that be an appropriate method?

Chair: Yes, that would be really helpful.

Jeremy Pocklington: This is an internal management document—I would not want to publish all elements of it.

Chair: No. I absolutely understand that.

Jeremy Pocklington: I oversee a very complex system here, but I would be very happy to write to the Committee with a summary of the plan.

Q12 **Chair:** We do not want to be the cause of giving the fraudsters any information they should not have.

Aneen, I have one very quick question and then I will move on to Sarah Green. We have had evidence from Accountancy Age, which tells us that between 2022 and 2025, you blocked 8,918 invoices totalling £211 billion-odd. Just over half—5,063 were later corrected and resubmitted successfully by suppliers, but the remaining 3,855 were permanently rejected. That is presumably a significant amount of money.

What happened to those invoices and suppliers? If they did not resubmit the invoices, what happened to those invoices you blocked?

Aneen Blackmore: I am not sure of the specifics of what underpinned the information you are sharing. I would have to go away and look at the specifics of that report. What I would say—this is a slight supposition on my part, but links to the example that Jeremy gave—is that as part of our financial and commercial control framework, we have teams that look at invoices as they come in and confirm against the contract whether we would see them as allowable or disallowable expenditure. That is part of our normal activity. It is a very complex regime.

Where we see disallowances, we engage with the supplier to understand whether there is a mistake or a misunderstanding, and there are a range of routes in response.

Q13 **Chair:** Could you let us have a note on that? If you have not seen the evidence from Accountancy Age, I apologise. We will supply that and then could you let us have a note on that?

Advanced analytics, AI and so on seem to be an absolutely prime case for scanning these invoices—the permanent secretary referred to that. Could you let us have a note on that too—how that is going to help you detect which invoices are correct and which are not? I would have thought it is a fairly simple accounting function.

Aneen Blackmore: Absolutely. I think Jim wants to come in on that one.

Jim Carter: Can I come in quickly on that? We are embedding in our new tooling a continuous duplicate invoice check. In the past, we have applied analytics retrospectively to that, but it will be happening through the process, which will avoid that in future.

Chair: Retrospective is no good if you have paid out the money.

Jeremy Pocklington: The trick is moving away from just relying on people reporting concerns—important though that is and very much welcomed—and sampling through first and second lines of defence in the Department. Analytics enables us, in time, to review the whole picture as it is happening to spot those irregularities. That is the prize that, over time, we and all organisations will need to get; it is wider than just Defence.

Q14 **Sarah Green:** My question is for Aneen and Simon. The permanent secretary, in his answer to Catherine, said that the Department has a zero-tolerance approach to fraud and economic crime. I am curious to understand why so few investigations result in criminal action or service justice action or, indeed, moneys recovered.

Aneen Blackmore: The Department's zero tolerance of fraud is an absolutely critical part of our culture and stance. What that means for us in the Department is that we investigate all allegations through the confidential hotline. Many of those allegations do not come with sufficient evidence, and we will follow up where we can to try and build that evidence so that we can take forward an investigation.

We investigate all allegations that come through, and they cover a very wide range of potential outcomes. That reflects the complex environment that exists in the MoD. We investigate all allegations. What we find, and what the Report shows, is that where we can investigate those allegations, 30% of them result in both a formal and an informal finding. They may be criminal—Simon can talk a little bit about that—or they may be informal responses on the civilian side.

It would be helpful for the Committee to be aware that we pick up the lessons learned and look for control weaknesses. We have that feedback loop back to our control environment. We do have findings in 30% of the cases that we are able to investigate.

Simon Dobinson: To give some context, the Ministry of Defence Police has an operational footprint in relation to how we provide protective security and physical security across the MoD estate at certain locations. Those requirements are laid out to us by the directorate of security and resilience around a number of sites that require the high-end specialist armed policing capability.

We also maintain a relatively small investigative capability for investigating specific offences that present a risk to the safety and security of the homeland. Those offences are not wholesale in the same way as all Home Office forces would investigate. They are specific to economic crime,

such as corruption and bribery. They also include those types of offences that are a risk around theft of, or damage to, the estate.

We have the full-time equivalent of about seven staff who provide a dedicated investigative capability to investigate economic crime at any one time. The majority of referrals to the crime command investigative capability come through the hotline. That is why we have the embed involved in that. The embed is able to assist with that triaging process to ensure that the right types of offences are being reported to, and then prioritised by, that small team of seven people.

Alongside that, we have certain capabilities that are specific to the Ministry of Defence Police, such as being able to seek confiscation orders under the Proceeds of Crime Act, which neither the service police nor fraud defence staff and colleagues have. That is one of our USPs around the ability to actually draw down on that. Our recoveries for last year were just over £850,000 with predictions that we would seek to improve that as we start to see transformation through improved joint working.

Our detection rate for last year was 38%, which is up from 31% the previous year, so there is some improvement there. If we look at the timeliness of our investigations, it takes just over a year on average to investigate. The City of London investigative policy suggests that an investigation should last no longer than about two years nationally, so our timeliness is quite good.

That is some of the context, but on your point about the detection rate, we are governed by the national crime recording standards and the Scottish crime recording standards. When an offence is reported to us, we have to record it in line with those, and we will then seek to carry out a proportionate investigation in line with all investigative opportunities. Many of those things will be affected by whether the type of offence that has been reported to us is done so in a timely enough way to provide us with the opportunity to secure and preserve evidence, but we are also subject to the Crown Prosecution Service and the criminal justice system, unlike colleagues within the service police who work with the Service Justice System.

In summary, we try to get upstream by having the embed, so that fraud defence are talking the same language around how things are prioritised and what is referred to us. We then have to make sure that we record appropriately and carry out a proportionate and thorough investigation, and we provide that as grounds for charging to the CPS. At the moment, the outcomes indicate about a 38% detection rate for the offences that we are investigating.

- Q15 **Sarah Green:** What change would you request to help you to achieve more criminal outcomes? You mentioned that there are seven dedicated staff; is that an area you would request more investment in? The permanent secretary said a great deal about technology earlier, but you talked specifically about the seven team members. Would something to do with team collaboration, co-operation and leadership help with that?



Simon Dobinson: It is a very timely question, because some of the work that has been going on in the background for quite a while as part of the defence reform is on how we can better align our capabilities across fraud defence, civilian policing and single service policing. The governance has now been put in place: there is a sitting defence police board that is chaired by a general, and the main purpose behind that is to get oversight of the risks that are affecting policing across defence and to see what the totality of output is so that we are talking the same language.

Sarah Green: Do you mind me asking how new that is? Is it already in place?

Simon Dobinson: It is already in place.

Sarah Green: How long has it been in place?

Simon Dobinson: It has been in place with effect for about six to eight months. The defence police chiefs' council supports it, and each of the provost marshals, myself or the deputy, and fraud defence sit on that, and it is where we come together to try to look at where we can cohere where possible. Part of the work that has been commissioned is around developing a concept or a course of action for how we can move to a more regular way of working, whether it is collaborative or co-location, but there are some hurdles to overcome and constraints such as how we share information, access to police systems and how integrity must be maintained, because the operational independence of civilian policing must be maintained so that we do not have perverse outcomes.

We are also trying to work on a clearer path around the timeliness of investigations. The quicker a crime or matter can be referred to us, the quicker we can make that assessment of whether it is a crime and pursue it. A key point linked to that is recognising that as an entity, we are limited in the resources that we have. We have a significant challenge around recruitment—and that is not affecting just us in the Ministry of Defence Police, but all Home Office policing as well. I am glad to say that a decision has recently been made around ensuring that there is a crime command capability to support defence, and because it is a commissioned service, that means that we will now be able to double down on our recruitment requirements and recruit the best people that we can to provide the outcomes we need.

Q16 **Sarah Green:** Forgive me, but on operational independence it seems from the Report that, with a little bit of knowledge, I could fall through the cracks and get away with something that is costing taxpayers a lot of money. Are you confident that will not be the case going forward?

Simon Dobinson: From my perspective, I am confident that if a matter is referred to us through the hotline or, as we are doing at the moment, if we identify opportunities through open source research—matters that are referred to us through security incident reporting forms, which we pick up on—we are identifying opportunities for investigations. What we need to

do is refer more of this back into fraud defence so that we can get a really clear assessment of all offences.

Q17 Sarah Green: What is preventing that from happening at the moment?

Simon Dobinson: Historically, there have been challenges in relation to the way people have worked. I think that was very much driven by a lack of understanding around what can be shared and how it can be shared. That is very much historical now. We are in a very different place, with a real ambition to move forward with a single course of action.

Sarah Green: Thank you. Sorry, Aneen, I think I cut across you as you were trying to say something.

Aneen Blackmore: The conversation focused on the criminal route, and I just wanted to reassure the Committee that our programme of work is very much focused on ensuring that we have robust investigations throughout the organisation. We are very alive to the fact that 60% of allegations end up being investigated by local areas, not through our police partners, so our approach is very focused on how we ensure that we have the right support and the right skills to support those local area investigations. That is to ensure that we have accredited focal points in every area, as well as support from counter-fraud and HR colleagues, but also the assurance that we have in place. The NAO Report is really helpful in highlighting some further improvements that we could make in this space, particularly around sampling, which we will be taking forward. I reassure the Committee that both our structure and our future plans are very much focused on how we ensure robust investigation across the enterprise.

Q18 Sarah Green: How many regional teams are there? You said you do it by area.

Aneen Blackmore: They aren't set regional teams. The structure we operate in ensures that the investigation, where it is felt that it will not go down the criminal route, can be carried out in the relevant organisation. That will be carried out lower down in the organisation.

Jeremy Pocklington: The Ministry of Defence is now divided into four areas—that is the phrase we will use. There is the Department of State, which is the relatively small bit at the centre; the military strategic headquarters—the military—which is also where about half the civil servants work; the national armaments director group, where Jim is and where a lot of the procurement takes place; and the nuclear enterprise, with specific procurement around the nuclear deterrent.

Chair: I appeal for shorter questions and, particularly, shorter answers, because we have only begun to touch the subject and we have had three quarters of an hour or so.

Q19 Rupert Lowe: I don't quite know where to start. I don't think this Report tells you about all the leakage that is taking place. When I look at the taxes being levied on farmers and small businesses that are forcing them



HOUSE OF COMMONS

to sell their farms and businesses, and I look at this leakage—you talk about £1.5 billion here—you are probably not capturing all the leakage that is going on.

I think my question is to you, Jeremy. I think the NAO Report is excellent. There is no room for complacency, as you said, and I am very glad to hear that you are not complacent. If I were on the end of a Report like this, I would certainly not be complacent. Let's look at the culture. The Report found "a lack of trust between counter-fraud and police teams, and noted unclear lines of reporting, duplication and missed investigative opportunities." I then read about "siloed working between different teams, inefficiencies and duplication, and relatively few criminal investigations," which "tend not to be complex or serious." I then go on and read something that really concerns me: "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."

I run lots of contracting businesses, and we do lots of procurement. I look at this and just do not think there is any joined-up thinking evident at all. You will be spending a lot more than £46 billion, or whatever it is you are currently spending—it is likely to go up to £75 billion. If these endemic cultural and structural inefficiencies continue, there will be more leakage, and therefore more taxes will be required on the private sector. This is very concerning, and I would like to know, Jeremy, how you are going to improve it. Are you going to give it the seriousness it requires?

Jeremy Pocklington: I said at the outset of the hearing that I take this seriously. There is absolutely no room for complacency. It is the heart of my job, and the job of everyone on this panel and in the Department, to make sure that we maximise the value we get from every pound of taxpayers' spend. That requires controls to be in place. It requires skills and capability, but it also requires the right culture, which you alluded to.

Having spent a lot of time preparing for today, I think some of the issues highlighted in the Report reflect the complexity of the environment in which we are operating in the MoD. It is a very large, complex organisation. We have the military workforce and the civilian workforce. We work with multiple different police forces. I want to assure you that I and the other senior leaders are placing great importance on the right culture of trust and collaboration. We have fresh leadership in the Department, in the fraud defence team, and it is fantastic that we have Simon here today. In particular, we have a new integrated investigative model that requires all the different parties to come together and work collaboratively to drive the behaviour we need to see.

Q20 Rupert Lowe: Can I interrupt? You are talking in generalities. Let us go through the Report. On theft of assets: "Around two-thirds of these reports related to lost assets, with theft making up only 13%." Can you define "lost assets"? On personnel management issues and information exploitation, the Report mentions "failure to follow gifts and hospitality



HOUSE OF COMMONS

rules, abuse of flexible working time, and deceit and misrepresentation for financial advantage” and “unlawfully obtaining or disclosing official documentation.” This is serious stuff, so please don’t talk in generalities. What are you practically going to do to sort this out? These aren’t generalities; these are actual events.

Jeremy Pocklington: There is no disagreement between us on the seriousness and the importance of the issue. I will talk specifically about assets and then the wider strategy to deal with fraud, because you are raising a whole set of different issues. Control of assets is very important in a Department like the Ministry—

Rupert Lowe: But what is lost, when you say lost assets? Most of them are apparently lost. What does that mean? Does anyone get punished for losing an asset? In my business, if somebody loses an asset with no justification, they have to pay for it.

Aneen Blackmore: We record and follow up all lost assets. The process is underpinned by our security control framework. The majority of our lost assets relate to phones or laptops. As you can imagine, we want to ensure that we track those carefully. As you rightly note, the response will depend on the justification given. We will absolutely be alive to any patterns if we think they are occurring, but the majority are cases of misplacement of phones and laptops. We will record the reason and where it happened to check the security concerns.

Q21 **Rupert Lowe:** You can have as many risk registers, processes and analytical tools as you like. In the end, you have to send people to prison for being dishonest. I know we have issues with the courts, which do not punish people properly, but in the end, people have to fear that when they break the law, when they are deceitful, when they steal, they go to prison.

I am going to ask you a few more questions. You talked about prescriptive or nominated procurement—you mentioned that. In my businesses, we have an annual or six-monthly review of where all the spend goes, the biggest supplier first. We then review them and have a discussion with those suppliers. We ask them for rebates. We discuss proactively with them how we can reduce the cost to our business, because in the private sector we are being loaded with taxes, national insurance and all sorts of stuff that is leaking out the side through MoD procurement, clearly. Do you have those meetings? When people nominate suppliers, I am immediately suspicious. Why are you nominating a supplier? Is there some further dishonesty going on? Often, you do not necessarily need to nominate, unless there is a really good reason. Just say, “Look, there’s loads of stuff that we need to be doing here”—

Chair: Rupert, shall we let them answer a little bit? You can then come back.

Rupert Lowe: But we do not want to talk generalities, Geoffrey. We want actual specifics.

Jeremy Pocklington: Let me give one specific and then hand over to Jim to talk about oversight of suppliers. One specific is that the Department is now using the new powers available to us in the Procurement Act 2023 to require suppliers to disclose conflicts of interest, on which they have a new duty, to ensure that we are bearing down on exactly the issues you have raised.

In preparing for this hearing, I spent a lot of time with the teams and our lawyers, asking what is actually happening in the Department to try to get that understanding. I am aware of cases where our commercial lawyers have found issues and have said, "Hang on, we think the intent here is such that it might pass the criminal threshold." They either reported the case to the police or to criminal counsel to take the matter further. I am not saying that we do not need to do more in the Department; this is something that we take very seriously. Mr Lowe asked specifically about how we oversee and manage our relationships with suppliers. That is Jim's role, so I will hand over to him.

Chair: Briefly please, Jim.

Jim Carter: We absolutely do robustly manage the performance of our suppliers to deliver to schedule, cost and time. Through reviews with them, we also specifically pick up on how they are managing fraud. We check their whistleblowing frameworks, their ethics, their supply chain risks and their modern slavery compliance. Your question was more broadly around culture. We obviously have mandatory fraud and corruption training for commercial staff, but we also set expectations on our supply chain that they also conduct that training.

Q22 **Rupert Lowe:** If you run a whistleblowing line, you have to make it effective. You had 1,037 cases, of which 363 ended up being properly investigated by the police. If you do not have a properly functioning whistleblowing line, people will not whistleblow. Anyway, I think I have covered that off.

I have one last question, because I know we are under time pressure. The NAO said in its conclusion: "The MoD has an opportunity to save money through better co-ordination and management of its counter-fraud and economic crime activity." Jeremy, to make that happen, you not only have to change the culture but pull together all the Department so that it has a common approach to saving money for the taxpayer—the poor taxpayer who is being abused here. We need to make sure they are looked after. How are you going to do that? How are you going to pull this together and stop it being siloed?

Jeremy Pocklington: That question is at the heart of the revised counter-fraud strategy we are working on, which takes into account our internal work and the findings of the Report. In an organisation as large and complex as the MoD, that requires a systemic approach—an approach across the system—for us to operate at multiple different levels. First, it requires us to continue to refine our estimate. That is important in its own right, but it also gives us a clue: where should we go after? Where should



HOUSE OF COMMONS

we work harder because we think there might be fraud or other things creating risk here? That is about leadership. We have talked about that. It is also particularly about Aneen's role as DG for finance, and having particular responsibility on exco—she is on our board for that. It is about how each area and each team in the Department oversees that.

You also specifically asked about the hotline and how we deal with people who raise concerns. We think the confidential hotline is a very good thing, but we need to rationalise the number of hotlines we have in the Ministry of Defence. It is very large and complex, and some of the hotlines do different things. It is not just about financial crime; we also need people to report concerns about staff behaviour, to give you another example. We need to rationalise the number and the approach.

We need the integrated investigative model that we have also talked about—there is more we could say about that. We also need to look at our case management system as well. This requires a systemic approach. Ultimately, it also requires leadership and culture. Because this hearing will be seen by many people in the Ministry of Defence, it also requires me to be saying today, "This matters. This is something that all leaders in my Department should be taking seriously."

Rupert Lowe: On that, perhaps you should start by getting your counter-fraud and police teams to trust and work together. That is your cultural problem; if people do not work together, nothing happens. I think I have done my bit for now, Chair.

Q23 Chair: I would just like to build on that. I have two or three very brief, pithy questions, and then we will take a break. On that question, it seems to me that there are too many organisations involved. There must be a case for rationalising all this into one police force that does the job professionally. Why do we need all the different police forces? Why don't we have just one service police and rationalise the whole thing?

Simon Dobinson: First of all, there will be an element of constraint in relation to the criminal justice system in which you receive the outcomes, whether it be service justice or criminal justice. There will be a natural separation between what the civilian police—ourselves—investigate, and how we prosecute, versus the Service Justice System. However, the work being undertaken by the defence police secretariat, supporting the defence police board, is looking at how to cohere better together the functionalities and outputs of the Service Justice System. Myself, representing the MDP, and colleagues from fraud defence are part of that conversation under a new governance structure. That is the first point.

The second point goes back to the point another Committee member made about the necessity for operational independence. There is a sterile corridor in decision making so that an investigation cannot be unduly influenced and we do not end up with a perverse outcome.

The next point is about how we make sure that we are better co-ordinated with other policing. We have a watching eye on police reform and what is



happening with that. I have had conversations with Gavin Stephens, chair of the NPCC, and we are engaged in watching how that works. Whatever function and format it takes in the future around investigation of fraud, we will make sure that we are part of those conversations in the same way that we engage now, where necessary, with the Serious Fraud Office or the City of London police.

It is certainly about collaboration and regular engagement, but it is also about making sure there is a structure that pulls all the levers across defence, whether that be in procurement, contract management or managing cultural change. A cultural shift needs to take place to recognise where risk and threat sit within defence, and to recognise that loss of laptops and phones as not only a security risk but a financial risk.

Q24 Chair: On a point of clarification, I cannot remember whether it was Simon or Aneen who mentioned this, but I refer you to paragraph 3.8 of the Report, which is on the important issue that Sarah raised around the number of prosecutions. Rupert also mentioned this, and it is related to table 9 on page 34. Paragraph 3.8 says, "of the 1,032 outcomes recorded on the Confidential Hotline...around 2%...were criminal or service justice action." It also says that a "further 18%...were recorded as non-criminal outcomes", and for the others, which is about 80%, no action was taken at all. I might be adding two and two together and making five, but taking into account your previous comment that you have limited resources, it slightly suggests to me that there is a culture within your organisation that you will only investigate the cases that are absolutely clearcut. There might be other cases that could and should be investigated but are not because you lack the resources. Am I making the wrong conclusion or not?

Simon Dobinson: To be fair, Chair, when it comes to the tasking for the civilian investigative capability, I can speak only for the Ministry of Defence Police. We will be tasked through the hotline, so that triaging process means we get what we are fed from the hotline and then respond appropriately, making sure it is compliant with the national recording crime standard, and carry out proportionate investigation.

We also look elsewhere. We look into the security forms and open source opportunities to investigate economic crime. Could we do more if we had more referrals through the hotline? Yes, we could. That hotline is complex, and there are a number of them, as Jeremy mentioned. Getting visibility of all of that is a challenge because of the various sizes, structures and cultures within Defence. There is more we can do.

The key bit is that the next model we move towards to work better together means we will get that information flow working better. The key bit around building trust, after what has been a tricky relationship in the past, is a willingness to share more, and the key bit around this is timeliness—expediting some of those investigations so that we can get ahead of the game, securing and preserving evidence better and putting a package together that the CPS can prosecute.

Chair: I entirely agree with you. It was a challenge for me as a reader to

work out how you had the cases referred to you from the hotline, but that is for others to question after the break.

We will now take a break. The clock is at 11.06 am. Let us be back here sharply, if possible, just before quarter past 11, for the final run of this investigation. I thank you all very much. If we get slightly cross, it is because we are frustrated; we want you to be doing more, quicker—but you understand that.

Sitting suspended.

On resuming—

- Q25 **Chair:** Could I start with a point of clarification, Simon? Maybe I did not ask my question before the break very well, but I think you have now said twice that the level of prosecutions is 30%. Actually, as I said, paragraph 3.8 on page 33, and the table following it—figure 9—show that about 80% are not prosecuted at all. Can we clarify those figures? Can you look at those pages and that table, and clarify those figures for us?

Simon Dobinson: My apologies, Chair. The number I referred to earlier—the 38%—was the detection rate for our investigations. Where we have prosecuted, the outcome for last year—2025—was around 38%, and previous to that it was about 31%. That is an outcome rate, as opposed to the number of offences being investigated or prosecuted.

Aneen Blackmore: May I offer a clarification? I think I also used the 30% figure. The 30% figure for the totality relates to where we are able to investigate. We have allegations that come into the fraud hotline that do not have sufficient information, and may be anonymous, and we are not able to forward those for investigation, but where we can investigate, 30% have an outcome.

Chair: Thank you for clarifying that.

- Q26 **Mr Betts:** to follow up on one point about the hotline and whistleblowing, what feedback to you give to people who have given you allegations or accusations to follow up? Do they get told what happens?

Aneen Blackmore: We see safeguarding through our hotline process as incredibly important, as the Committee would expect. We were cited in a recent NAO Report for the support that we give to whistleblowers, which we are incredibly proud of. Whistleblowers are kept updated throughout the process. With regard to outcomes, as the Committee can appreciate, that will depend on what the outcomes are and what information we are able to share with the whistleblower. We would usually be able to share where processes have changed, but we would not share personal information that relates to individuals.

Mr Betts: So you wouldn't share whether there had been a prosecution.

Aneen Blackmore: I think it would be very case-specific, and we would abide by the relevant laws and guidelines.



HOUSE OF COMMONS

Q27 **Mr Betts:** Have you reviewed how you deal with this? There is always a challenge for people who consider whistleblowing: "Oh, they'll not take any notice of it. We'll just put it in and it'll disappear into a black hole somewhere and we won't be kept updated about what happens."

Aneen Blackmore: At the end of the process, we certainly give the whistleblower an outcome letter. What is shared in detail will be case-specific, but they will have the reassurance that the case has been investigated and they will know when the case has been closed.

Mr Betts: In every case?

Aneen Blackmore: In every case.

Q28 **Mr Betts:** Right. Let's move on. Permanent secretary, you have come into the Department new, and you have this Report, which is not happy reading for the most part. I perhaps would have wanted to hear from you something along the lines of, "I've come into this Department and I'm really quite surprised and upset by what I have found about the way fraud has been treated. I'm going to change it."

Jeremy Pocklington: I have already expressed to the Committee the seriousness with which I take the issue. I have already set out the importance that I am attaching to us making improvements—making those changes. That is why I am very supportive and am driving the work to have that revised counter-fraud strategy, which is the vehicle that I talked about to drive the next stages of—

Q29 **Mr Betts:** What is happening at present is not good enough, is it?

Jeremy Pocklington: There is more that we need—

Mr Betts: No, no, it isn't good enough, is it? Can we just use language that is fairly clear rather than generalised?

Jeremy Pocklington: There is definitely more that we need to do to get better at this. I am going to use my words rather than your words, Mr Betts, but—

Mr Betts: Which are a bit general.

Jeremy Pocklington: But there is more that we need to do.

Q30 **Mr Betts:** It is difficult to tackle this, isn't it, unless you have an accurate description of what the fraud actually amounts to? You do not have a figure that you could come here today and say, "That's it."

Jeremy Pocklington: Measuring fraud is really difficult—

Mr Betts: I know it is difficult. You have not been able to do it, have you?

Jeremy Pocklington: May I answer the question, Mr Betts?

Mr Betts: You can, yes.



Jeremy Pocklington: We want to get a better estimate of our losses to fraud. The team are actively looking at what is the best—I will use this word—technology that we can identify to help us get the best possible estimate. Of course, where fraud is detected, it is easy. In 2024-25, detected fraud and error was £6.2 million, but that is not the amount of fraud. I am not saying that that is the amount of fraud in the Department, but the moment you are looking at something for which you do not have direct evidence, it gets harder. We are going to look at what the best technology for us is and at what other Departments and other organisations, like the NHS, have done. It will still be very assumption-dependent. It is easier where there is robust data or you can make comparative loss assessments; it is hardest to get a handle on levels of fraud where you have to make an assessment, essentially—what is described as the baseline vulnerability assessment—but we are going to do that, because it is important in its own right. As I said, the key thing is that it helps us to identify the areas in the Department where we will need to do more.

Q31 **Mr Betts:** Right, so when are we going to get a robust and accurate estimate of fraud losses?

Jeremy Pocklington: That is what we will set out in the strategy. I do not know if Aneen wants to say anything else about that work.

Aneen Blackmore: As Jeremy set out, it is absolutely a priority for us to improve our estimate, as part of that balanced plan—we have talked about the importance of having a good estimate, having the right controls in place to prevent fraud, and how we drive return on investment—to drive value for the taxpayer, which is at the heart of what we are trying to do.

As Jeremy alluded to, we have been working very closely with the PSFA on what the best methodologies are to help us get after this. The NAO reported back in 2023 that the MoD was forward leaning in this space, with our estimate, but we know we want to do more to mature it and that it is going to be critical. As Jeremy also alluded to, we are learning from the NHS, which has been introducing both the methodology and the practical advice about how you get after that. In the counter-fraud strategy we will be setting out how we expect to improve that. It is likely going to be in phases, because it is complex. We will start in the place where we think we have the most exposure to fraud, because that is where we think it is really important to have a more mature estimate. We will be using our risk register to focus on where the estimate should be matured, and what methodologies we can use to build out our confidence.

Q32 **Mr Betts:** Right. Back to the question I asked: when will we have a robust estimate?

Aneen Blackmore: What we are seeing from the NHS, which is some way along this pathway, is that it is not something that we are going to be able to quickly assure ourselves of, on a more detailed methodology, across the whole of Defence, but what we will be doing over the next year is really

focusing in on the areas of highest risk and building out our estimate—and our confidence in that estimate—in that space.

Mr Betts: So you haven't got a date.

Aneen Blackmore: The date will be set out in the counter-fraud strategy refresh. We will set out the phases—

Q33 **Mr Betts:** How far away is that?

Aneen Blackmore: That is what we are writing now. We will have that complete in September, and it will detail the phases of what we are going after.

Mr Betts: So in September you will be able to give us a robust estimate.

Aneen Blackmore: In September we will set out a plan of the phased approach, and we will be focusing in on the areas of the highest risk, in the first case.

Q34 **Chair:** You have not answered the question, though. What Mr Betts is asking you very clearly—both of you—is: when will we have a reliable estimate? I think this goes to the heart of the entire hearing. Somebody has assessed a figure of £1.5 billion of potential fraud, but I do not believe that the culture within the MoD actually believes that figure is accurate. You need to come up with a robust figure that everyone believes and that they are working towards. You have estimated it at £1.5 billion, and you are only recovering around £6 million—there is a huge gap there. Please could you—I do not mind which of you—answer Mr Betts's question: when will you have a robust estimate?

Aneen Blackmore: What we have learned from engaging with the NHS is that it is an incredibly complex and challenging thing to do. We are taking lessons from the NHS so that we are not starting from a low base but can learn from what it sets out. It would be inaccurate and misleading for us to say that there is a hard date, at this point in time, when we will be able to have redefined our estimate for the whole of Defence.

What we can assure you of is that it is really critical to us. We absolutely accept that a robust estimate drives the heart of how we understand the totality of the loss and where we want to direct our activities, and therefore we will be focusing on the areas of highest risk. By September we will be able to set out a plan for exactly when we will be able to have a more mature estimate in those areas of highest risk, but I do not think that here today, recognising the complexity of the challenge, which we have learned about from organisations that are further along on this journey than us, we are able to set out a specific date.

Q35 **Chair:** Okay, so by September you will start to break it down into the different areas, and there are lots of different areas involved in this, but unless you have a robust figure that you are aiming at, how can all of your organisations start to work towards what they are supposed to be achieving? I am beginning to lose the will to live here. This is a substantial



HOUSE OF COMMONS

amount of money, and if your organisations do not think the £1.5 billion is accurate, fine, but when will we have an accurate figure? You can add all the different sections up and come up with an overall figure that the MoD thinks it is losing to fraud each year. Surely that is not impossible. All the Committee is asking is when that figure is likely to appear before us.

Jeremy Pocklington: Let me write to the Committee to set out the workplan around that. We are all aware of the £1.5 billion, and the Report sets out what that is. You describe it as a broad estimate, but I would say it is quite a theoretical number based on the academic benchmarking of organisations that do not include the Ministry of Defence. It is therefore quite a conceptual estimate of the risk. None of that, though, takes away from the importance. It is a very difficult thing to get a robust estimate of fraud risk that is reliable—

Q36 **Chair:** You know where I am coming from next: if you don't think it is the correct answer, you should give us the correct answer. Otherwise we cannot assess how you are doing.

Jeremy Pocklington: That is why, when I earlier talked about the work that we have under way on a counter-fraud strategy refresh, the first thing I mentioned was the need to get a better estimate of fraud. There is no difference between us on that, Sir Geoffrey; I recognise the value of that. Let me write to the Committee to give you further details of how that work is structured and what our estimated timetable would be. I am worried that the Committee might think this is a sort of lack of will or of effort; it is not. It is a very hard thing to do, because we are trying to estimate something that we cannot see.

Q37 **Chair:** No, I accept that, but unless you have a reasonably reliable total estimate, it is going to be much more difficult for all the good people working for you in the Ministry of Defence. The current figures are pretty stark: an estimate of £1.5 billion and recovering £6 million-odd is pretty—

Jeremy Pocklington: Sorry, that is not—the £1.5 billion number is essentially an academic construct—

Mr Betts: Well, that makes you wonder what the Department has been doing for the last few years, if it is having to rely on an “academic construct”.

Jeremy Pocklington: I think there was a previous NAO Report as well. Getting better technology is something that all parts of Government are working on. There are new tools and techniques to help us to do this, and analytics will also help us on this. This is a developing area of focus in Government and further afield. It is not the case that—

Q38 **Chair:** You know where we want you to get to; you will write to us and set it out very clearly, and we will obviously have a really good assessment of that, but we will want to have you back at some stage to account for how well you have done under that new process.

Jeremy Pocklington: Of course.

Q39 Mr Betts: We will move on, then, to the risk areas and the assessment of risk. Again, there are no accurate assessments of the financial value of the various risks that you face, are there?

Aneen Blackmore: On the risk registers, as I alluding to earlier, we are going through a programme to continue to mature how we set those out, both in how we nest them in the organisation, from the enterprise downwards, and how we can continue to develop them as risk registers that can be actively used in the organisation. As you rightly point out, that will include estimation around fraud value.

Mr Betts: And that will be available by September, will it?

Aneen Blackmore: That is a programme of work, but it is happening now, and we expect that to be in place during this coming financial year.

Q40 Mr Betts: If you are developing a fraud strategy, how do you do it without any assessments of the various risks involved?

Aneen Blackmore: The fraud strategy will be setting out how we will be responding to high risk. Then, underneath that, we will have a detailed plan of where we want to focus resource and activity. The enterprise risk register has been developed and will be rolled out imminently. The risk registers that exist through our frontline commands and our enabling organisations are in place. We are going through a programme now to ensure that we are able to include financial value. We will then be looking at how we can use those to influence where we are investing—particularly in new technology and tools—going forward.

Q41 Mr Betts: Yes, but if you do not know what the values are, you cannot determine what priorities you should be giving to different areas, can you?

Aneen Blackmore: That is absolutely right.

Mr Betts: So that will be available in September. It must be part of the strategy, mustn't it?

Aneen Blackmore: Absolutely, that will be part of the strategy. What I am conscious of is that it will not be a once-and-done programme; what we have in place is an ongoing programme to ensure that those risk registers are constantly updated, that they are used, and that they are useful tools.

Mr Betts: So by September, as part of the strategy, you will have some assessments of the value of the various risks.

Aneen Blackmore: Correct.

Q42 Mr Betts: Okay, thank you. Let's go on to procurement and commercial risk, which is obviously a pretty serious matter that could involve very large sums of money—we just do not know at this stage. How well are the commercial operations, the staff there and the fraud part of the Department linked together? In the end, the people on the frontline doing the commercial operations should be the first ones to identify any

problems, shouldn't they?

Jim Carter: There are members of my commercial and industry organisation on the defence fraud board. Clearly, where we identified any issues or expected fraud, we would feed that in. To the question around clearer accountabilities for commercial, it picks up a bit of what Jeremy was talking about on defence reform, which is a key objective around simplification and clearer accountabilities.

Under the national armaments director group, you have a consolidation of procurement budgets and end-to-end ownership of the acquisition system, as well as stronger functional leadership. In terms of the ownership of the budgets and people for finance and commercial, that is rationalised, and that helps with the visibility and driving improvements in this area.

- Q43 **Mr Betts:** I was pretty shocked by paragraph 2.14 in the Report, which said, "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". That is really quite shocking, isn't it? You can all see that there is big money that could be made by people wanting to defraud the system.

Jim Carter: I would not recognise that characterisation.

Mr Betts: Sorry, but it is in the Report and it has been approved by the Department.

Jim Carter: I understand, but I don't think anyone on my commercial team were interviewed as part of the Report, and I know that we look out for that. I also know, because we have mandatory fraud and corruption training, that it is front of mind. It is critical, particularly with the geopolitical context, that every pound is going to address capability and warfighting readiness.

- Q44 **Mr Betts:** When we get Reports in this Committee, we assume the Department has agreed them—because they have. It is no use saying, "Someone down there hasn't been talked to." The Department, at a senior level, has agreed this Report, and it has agreed some very worrying comments about the lack of understanding of fraud in the commercial teams. Do you recognise that?

Jim Carter: I would agree that it is critical that my commercial organisation, the finance organisation and defence fraud work collaboratively and closely in terms of that reporting, so I absolutely agree with that.

Mr Betts: The suggestion here is that they are not, currently.

- Q45 **Chair:** You made a statement, Jim—and I am going to bring the C&AG, or his head of team, Joshua—that nobody interviewed anybody in your commercial teams. Could you clarify that?

Gareth Davies: The Report is very clear; we are quoting MoD staff who have that view. It is precisely worded in the Report, so I don't think there is any dispute about that. This is a view from the assurance teams and the finance teams observing the culture they are working with.

Joshua Reddaway: And just to be clearer, the assurance team there includes the cost advisory service, which is commercial staff, commercial assurance and counter-fraud teams, which would be fraud defence and other people working on counter-fraud.

Jeremy Pocklington: The Report is agreed. This is Jim's first hearing, so just to be clear: constitutionally, the Report is agreed with the Department, and the teams that Joshua has referred to work for Aneen. The cost advisory service and fraud defence are incredibly important. My reflection—new into the job, taking this seriously—is that the first port of call is often to think about this commercially and drive value for the taxpayer, commercially. We have a class-leading cost assurance team that is driving down on costs, using the great advantages of single source contracting regulations. Because of the economic construct of the market, that is the route that we have to go down. I also see really strong evidence of robust commercial negotiations and strong controls in place.

The difficult boundary is what I would describe as sharp commercial practice. We have lots of excellent suppliers with very high reputations that work well with the Department, but it is about the boundary between sharp practice and fraud, and the intent that is involved in fraud. In preparing for this hearing, I have seen evidence that the Department is focused on that boundary, but there is more that we need to do in order to really build an understanding of that boundary and when something has crossed the line.

These are technical, complex issues that we are dealing with. That is why it is great that everyone needs to do training, but we also need to balance that with real experts and fraud defence in the areas to make sure we are constantly looking at that. Sir Geoffrey, does that help the Committee?

Q46 **Chair:** It is helpful, because you said something that I was about to ask you about: training. Do all the top people in DE&S and everybody else who has anything to do with procurement receive training so that they know what they are looking out for when they are procuring this equipment?

Aneen Blackmore: All staff receive mandatory counter-fraud training, and then you receive specific training depending on your role. We would have to follow up and write to the Committee about at exactly what level the training is rolled out to in DE&S, but there is a focus on the common culture that we are trying to create in defence. There is mandatory training for all staff, and we have more specific bespoke training to ensure people are accredited if they are in counter-fraud roles, in particular.

Can I just come back to the point raised about the join-up around the counter-fraud and commercial teams? We recognise what the NAO Report has pulled out. We would like to codify more of that relationship between



HOUSE OF COMMONS

us, particularly to ensure the counter-fraud team has visibility of activities across the enterprise. We see a real opportunity there, both by being able to report a more accurate figure of our activities, and how we can do more to effectively drive outcomes.

The commercial leakage tool that we introduced is a really powerful example of that. It has been a stepping stone into that close relationship between the counter-fraud and the commercial teams. We want to build on that, codify it in our ways of working and set out those obligations. One of the ways that we will be strengthening the obligations through the counter-fraud strategy is that clear holding to account through the functional route so that we can set out clear, measurable KPIs that every area and every function in the Department needs to report into.

Q47 Mr Betts: I have one follow-up on a slightly different issue: relationships between suppliers and MoD staff. The suspicion is that relationships may sometimes get a bit close. People obviously get close personal relationships; that is natural in business. But sometimes there is a prospect, and indeed an actuality, that the MoD staff—uniformed staff and others—move on to work for the companies that they have commercial relationships with. How do you ensure that that does not lead to fraud or, shall we say, non-vigilant action by MoD staff?

Jim Carter: I will start, and then the permanent secretary may want to come in. Clearly, we follow robust business appointment rules. There are clear conditions put on staff, in terms of both the timing and the type of relationship that they can have with those suppliers. As part of our procurement process, we also have very clear conflict of interest declarations. I was talking about new technology, and one advantage is that that can do more sophisticated checking of the wider financial systems, ownership of companies, and politically exposed persons. That will help us to make sure that that is even better in terms of the declarations around that.

Mr Betts: But quite a few staff will go on to work for the suppliers they are now dealing with as a customer.

Jim Carter: I think that is true. I do not personally think that that is unhealthy. We recognise as a defence enterprise that, particularly to meet some of the challenges, we need this profound transformation of our system to deliver the strategic defence review and the defence industrial strategy. The skills that you might have working in the MoD can be valuable in the supply chain, or vice versa. What we need to make sure is that the rules around what they can influence in procurements and how they can lobby or sell into government are really robust and tracked through.

Jeremy Pocklington: I want to really emphasise, as the permanent secretary, the importance I attach to proper, robust business appointments rules and the importance of policing those. That is something that I have always done and will continue to do in this role.



HOUSE OF COMMONS

Q48 **Mr Betts:** How do you then control people going on to those private sector jobs with knowledge?

Jeremy Pocklington: It is about following best Government practice and policy, and employment law in this country today, to make sure we have robust controls and conditions in place, and periods where you debar people from taking on roles. I have only been in the Department a very small number of months, but I want to reassure the Committee that I will be approaching cases robustly.

Q49 **Chair:** In order to test that culture within the MoD, Andrew Feinstein—I accept you do not get this evidence in advance—tells us that Raytheon UK’s “parent company RTX recently faced significant legal sanctions in the US—including penalties of almost a billion dollars”. This is a really well-known name in the defence industries. Would that sanction have been applied in the UK? That is the acid test. With the same evidence used to prosecute in the United States, would it have happened here in the United Kingdom?

Jeremy Pocklington: I don’t think I can answer that. On the very brief summary you have given me, I am afraid it is too hard. What I will say is that the Procurement Act 2023 gives us new powers, including powers to disbar suppliers from working with the Department where they are found to have done wrong. It gives us additional powers, additional protections. Exactly how the legal process would treat companies is a bit hypothetical.

Q50 **Chair:** I accept that you have not seen the case, but it is the principle of the thing with such a well-known company. If you had the evidence, would you have the wherewithal, ability and wish to prosecute that company?

Jim Carter: I can answer yes to that. Where we see underperformance from our suppliers, we will terminate—well, clearly, if it is fraud, we will rigorously pursue that—but where we see underperformance and that is a breach of contract, we will terminate and seek costs. So we do robustly manage suppliers. One of the opportunities—it is linked to the work we have done under the defence industrial strategy—is that we recognise as a commercial industry and the MoD that we need better understanding and illumination of the supply chain. That is also about us being able to deliver effective capability and make sure we have the right shape of our supply chain. But it does contribute to some of the risks we are discussing as a Committee. A really good understanding for the MoD of who—

Chair: Okay. It was almost a yes or no answer, and you have answered it. Thank you.

Q51 **Sarah Green:** I want to move us on to triage and how the allegations are triaged at the moment. At the end of paragraph 4.7 of the NAO Report, it states, “different teams are not aware of the criteria or thresholds different parts of the MoD use when deciding to pursue or prioritise a case.” I am keen to understand—this is a question for you, Aneen; correct me if I am wrong—how you ensure the MoD chooses the most proportionate way to investigate potential fraud cases if there is not a common understanding across the MoD.



HOUSE OF COMMONS

Aneen Blackmore: There is a common understanding within the counter-fraud team of how those cases should be triaged. As you would expect, there is a standard operating set of procedures. They look at the type of allegation raised, whether we think it could be investigated on a criminality route, whether the information is sufficient and whether we can do more to gather information before allocating, and, of course, at safeguarding, which is at the heart of the triage process.

The heart of the triage is ensuring that the case goes to the right part of the Ministry of Defence. As I said at the start, zero tolerance of fraud means that we review and investigate every case. Simon talked a bit more about the police process, but the advice and support we give to local areas when they are investigating includes a view of the materiality, which is why cases with a higher materiality level form a significant part of our recovery. That is where we will be focusing our activity, because there is often the strongest evidence and the greatest return on investment, and it is important to defence to recover that.

- Q52 **Sarah Green:** Just to follow up on what you are saying, paragraph 4.8 says that the NAO was 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." Can you talk about that and what the Department is doing to address it?

Aneen Blackmore: Absolutely. That comes back to the heart of the ways of working that we have discussed and is absolutely critical to how we want to improve and continue to build out the mechanism we have. As Jeremy alluded to earlier, we will have an integrated investigative team that will ensure that as cases are closed by our police partners, they can seamlessly come back into counter-fraud to be triaged out into a local area where that is appropriate.

- Q53 **Sarah Green:** Is that not currently happening?

Aneen Blackmore: It does happen, but we want to ensure that we have a really robust mechanism to ensure that it happens in every case.

Simon Dobinson: What is critical to this is that although a case may not meet the criminal threshold for investigation, that does not mean we do not record it as intelligence. We capture it and use it to build a more robust intelligence picture. Then we might start to see patterns of behaviour that fall behind it that may support the need for a criminal investigation in the future.

Sarah Green: It is not lost information.

Simon Dobinson: Correct.

- Q54 **Chair:** Why do you do this on a local level? Fraud is such a difficult thing to detect. Why do you not have a specialist team at the centre that handles all fraud matters?



Aneen Blackmore: We are very reflective of the fact that fraud allegations through the confidential hotline cover a huge range of potential allegations. We want to ensure that we have a system that supports robust, effective and proportionate investigations that we can carry out. A large proportion of cases that come into the fraud hotline do not relate directly to fraudulent activities. We ensure that we can very often triage those to our HR colleagues. The heart of the system is making sure that the allegation is investigated at the right point in the organisation.

What I would say—this is why I wanted to give assurance to the Committee earlier—is that we are very conscious when we are allocating to local areas that local areas have the right skills and support to carry out an appropriate investigation. That is through formal training, accredited people based in the local area and, of course, regular engagement through the counter-fraud team.

- Q55 **Chair:** Following on from that, I am concerned about the role of fraud defence. As I understand, they are the people who allocate out these cases from the hotline to Simon's organisation, and they are composed of part-timers. I just wonder whether they are doing a good enough job, and whether Simon's organisation should not actually handle the calls directly from the hotline, so that he and his professional colleagues can make an assessment of whether the cases should then be taken further.

Aneen Blackmore: That is why the embed that we introduced has had a really powerful effect. It ensures that we are joined up at the triage stage on any live police investigations and, as Simon alluded to, the intelligence that the police have covered. It also confirms that we are following the right triage allocation rate.

- Q56 **Chair:** The Report reads as though fraud defence can sit on these cases, and they are not necessarily progressed. I would like to think that when a case comes in through the fraud hotline, it is progressed in one way or another—it could be progressed into taking action, and hopefully a prosecution, if the evidence is there. However, it should be acted on quickly, and the Report does not imply that.

Aneen Blackmore: The average triage time is 12 days, so the team looks at it, triages and allocates out to the relevant part of the organisation, whether that is police or partners in our local areas. We absolutely monitor and track our triage time to ensure that we are not spending a lot of time on triage but getting the cases out so that they can be investigated.

Chair: Fair enough. Thank you very much.

- Q57 **Rupert Lowe:** I think my question is to Simon. I am again reading the MoD Report, and I would just like some clarity. It states: "The MoD told us...Fraud Defence and the police are also working jointly on a new investigative model for fraud and economic crime—which"—this is the key word—"could include joining police and Fraud Defence case management systems." Is it going to do that, or is it still just a possibility, as that would suggest?



HOUSE OF COMMONS

Simon Dobinson: I have two points to make, if I may. First, the development of joint working has gone much further than the embed in the hotline. This is currently being developed as a course of action that is broader than the MDP and fraud defence, as it also includes the single service police—they have an ownership of this responsibility as well. That is being worked through at the moment as part of wider defence reform. That is a very complex area, because that is looking at the whole set of capabilities that sit within the service police, and how you manage the level of investigation and ownership through two different criminal justice systems.

I will turn specifically to your point about the outcome, and what that would look like in how you then develop that through a case management system. First, fraud defence is developing access to an alternative system, which Aneen might be able to comment on. We ourselves in the Ministry of Defence Police are embarking on developing a new system that is broader than just case management; it also involves command and control, as well as intelligence. I believe that process is now through a tendering process.

There may be licensing opportunities there for fraud defence to have access to that, but that will be very much governed by whether the access controls can be put in place on the protection of police information, as per the Information Commissioner's Office, MOPI and the necessary data protection laws. That is all being worked through at the moment, but the ambition is very much to see how we can data share through blended ways of working, which again—having made the point earlier—means that we work to the sum of our parts but recognise the independent skills and capabilities that are required.

Q58 Rupert Lowe: I think that word should be “should”, not “could”, which seems to be common sense. I hear your answer, and I hear you talking about the reasons why it is difficult, but you have to overcome those problems. This is about fraud and dishonesty, and as I said, this needs to be dealt with.

We have basically moved from being a nation of shopkeepers. As the private sector is taxed into oblivion, and the public sector grows like a weed, you are going to see more fraud. The nation of shopkeepers used to keep their own accounts, but the state is incapable of keeping its accounts. I have always had this theory—I would be interested to know what you think—that the state often builds up great big numbers of people who do not communicate or work together. They sit in silos and cost the taxpayer a lot of money.

If you put together a lightweight team, with a combination of both police and the MoD, and use your whistleblowing line to identify cases that need to be investigated, you could then work through those cases and investigate the ones you need to. Equally, you could decide that you wanted to drop in on a Department without any notice to do a thorough audit and pull apart every single thing it is doing. If need be, you could listen to tape recorded lines, or whatever it is that you do. I do not know whether you tape record lines, but in financial services, everything was



taped, so you could go back to listen to every single detail of messages, phone calls, orders placed—the lot.

If you have a genuine desire to look after the taxpayer, you need to get together this lightweight team, which would cost you a lot less than a vast group of people who do not talk to each other. You would then make people fear what happens when they are caught doing something wrong. As I said earlier, people have to fear that when they get caught doing something wrong, they will go to prison. Prison is not a comfortable place. You have to have some fear in there so that if these people who are procuring large quantities of arms, munitions and other such things that are now so important to this country are caught committing fraud, they are punished. I am interested to know: why can you not cut down this fixed cost base and set up a joint venture that actually attacks the issue?

Simon Dobinson: There were a couple of points there. First, I wholeheartedly agree that there is an absolute moral, ethical and financial imperative to get to a point where we are reducing the risk of fraud in the organisation, for those reasons and from a security perspective as well.

Secondly, on how we could do that, we have already embarked on that journey of looking at how we can work better together. The NAO Report is helpful in that it holds a mirror up to where some of the risks and vulnerabilities are. The reassuring part is that we are already in train on delivering some of those capabilities. The detail on how we coalesce together in that work is still in development, but the direction of travel is very much toward doing something where the whole is greater than the sum of its parts, according to the individual capabilities of each part of the organisation.

Q59 **Rupert Lowe:** When you have machinated long enough, I think we need to have a report on exactly what that is. Will this “could” become a “should”, or will we be given all sorts of complex reasons why the MoD cannot make it a “should”? If a report like this NAO Report was done about my Department, I would be very worried and have all the drains up. You have told me that it is still in flux: it is still not decided and it is still not done. We want action, not words.

Chair: We will deliberate on all the evidence we have heard today, Rupert, and produce a report with recommendations. I cannot pre-empt what will be in our report, but we will look at all these things.

Rupert Lowe: Okay.

Aneen Blackmore: If I may, the counter-fraud strategy refresh in September will absolutely set out how we are taking forward the joint investigative model. You are quite right; we see that as the heart of how we effectively join up.

We reviewed the structure between counter-fraud and the MDP to make sure that it was still the most robust model. We concluded that it was, but we wanted to codify some of the governance arrangements. Again, that



HOUSE OF COMMONS

will be included in the strategy refresh; you will have sight of the summary of that.

Rupert Lowe: I would rather watch what the hands are doing than what the mouth is saying. What we as a Committee want to see is some action.

Q60 **Chair:** You will be glad to know that we have almost got to the end of our questions. Going back to Catherine's questions and this 48p return for every £1 spent growing to £1.34 in 2024-25, I imagine that a lot of that will have come from two cases, of which I will give you the details, but not the names—although they may well be published; this evidence is from Accountancy Age, so I think it is reliable and it will be published. I will quote the two cases to you and then ask what your organisation will do to try to prevent such things at an earlier stage.

In April 2025, an ex-corporal, who I will not name, was sentenced to prison for defrauding the MoD of £911,677 through fraudulent expense claims submitted via an internal online platform. As an aside, the court heard that he retained over £550,000 for his own personal use—which I think says something about the court process.

In a separate case, an Army financial administrator was found to have stolen more than £300,000 by issuing cheques to himself while falsifying stubs to make them appear as payments to legitimate vendors.

These are very serious matters. What more can your system do to tighten things up? It is exactly as Rupert says: if these people know they are going to be caught, they will not do it. I am surprised that these were not picked up. I absolutely appreciate that you have not had time to investigate them. However, using the cases as an example, what more can your system do in general?

Aneen Blackmore: Absolutely—they are really serious cases, and we take them very seriously. As part of our process through the confidential hotline and, more broadly, through our financial governance, we ensure that where we identify that something has gone wrong we look at our control framework and understand the controls that let us down. Was it that the controls were not designed effectively, or was there a reason why they were not operating effectively? That is at the heart of what we do. It is not just the lessons learned but making sure that we are closing that gap.

We are also thinking through how we can more systematically improve our control environment, both through the structures that we set up and through the opportunities offered by technology. Briefly on both, as part of the defence reform programme that the Secretary of State has set out, we are strengthening functional control. That has a very real impact on finance in that we are bringing it into a more integrated and aligned structure sitting under me so that I can more formally hold to account and drive common standards and processes. That will have a real-life impact on how we are going to operate.



HOUSE OF COMMONS

We are also looking at the opportunities that we can introduce through technological advances. There are two key elements to highlight. We have a corporate services modernisation programme covering finance, commercial and HR activities. That will move our systems on to the cloud.

As part of that, as you would expect, we will be building more of our control checks into the system. In a number of cases currently, we have to have manual checks; this will enable us to automate those controls in a way that is quick, seamless and data-driven so that the checks will be more efficient and effective. That will also free up my team's time to intervene in areas of high risk where we see that more manual intervention might be required.

We are also introducing data analytical tools, which we have talked a bit about today. As a core example, that will allow us to interrogate expenses and look for patterns of behaviour that will allow us to prove intent, not just pick them up on a recovery basis.

Q61 **Chair:** I have brought to your—and therefore the public's—attention that when these things are found they should be well and truly publicised so that other people thinking of attempting the same will hopefully be deterred. That is really important.

Permanent Secretary, I have one question that I was going to ask you at the top of the session. If you look at yesterday's debate on the defence estimates, there was a lot—I mean a lot—of dissatisfaction across all parties about the lateness of the defence investment plan. It is causing huge frustration, particularly here in this Committee, that we cannot examine whether your programme laid out in the strategic defence review is realistic or not according to the budget that you are going to set. What is the problem? Why has it been so late?

Jeremy Pocklington: First, I appreciate the interest in the defence investment plan. It is incredibly important that we set out our plans to turn the SDR into action. We are working very hard on the plan and intend to publish it as soon as we possibly can. Our Ministers have been clear.

Chair: That does not mean anything—"as soon as we possibly can" means nothing.

Jeremy Pocklington: Our Ministers have been clear in Parliament. There are a lot of discussions under way to finalise the plan. It is a very significant exercise. It is the first time in 18 years that a Government have conducted a zero-based review of Defence's budgets.

The key point is that it is a zero-based review, looking not just at our equipment programme but at every budget line, including the support we offer to people and our wider infrastructure, to deliver a very significant transformation, as set out in the SDR—all at a time when demands on my Department are rising. We have all seen that with action in the middle east and the Ukraine, and activity in the High North; my Secretary of State has talked about that.



HOUSE OF COMMONS

Q62 **Chair:** We know all that; we appreciate that. We know that there are lots of demands on your and the Ministry's time. The simple question was this: what are the issues that are causing you so much difficulty at the moment? It was promised in the autumn. Here we are into the spring. I have no doubt that, if we are not careful, it will be the summer, because you will get into purdah with the local government elections. What is the problem? Why is it being held up so much?

Jeremy Pocklington: The reassurance I can give the Committee is that we are working as hard as we can to complete the plan. We need to make sure that the investment choices that the Government are making in these very uncertain times are right for now and right for the future.

Q63 **Chair:** You see, no doubt what has happened in the middle east this week will cause you to almost rewrite the thing. If you keep on delaying, events will keep on happening. How are we ever going to get to an end-state on this?

Jeremy Pocklington: We are working as hard as we can—

Chair: I have heard that twice.

Jeremy Pocklington: To complete the plan. We will publish the plan as soon as we can. It is very important that we get this right, to ensure that our military is ready to war-fight, as we have set out as the Government's objective, and also to take account of the context that we are dealing with.

You have referred to events in the middle east. There is also activity in Ukraine, with a potential coalition of the willing and our potentially having troops on the ground there. There is activity in the High North. Demands are rising. We are working very hard on the plan to ensure that the military have the support that they need. It is important that we get this right.

Chair: I understand all that. It sounds as though you do not have enough money for what you need to do. But anyway, that is a different issue and we will find that out in due course.

I thank all four of you very much indeed for coming today. We will look carefully at what you have told us, or what you have not told us. We will produce a report in due course, with recommendations that I hope you will examine carefully, and we will see where we go after that. Permanent Secretary, as I indicated earlier we will look at your new refresh plan, which you say will come a little later in the year, very carefully. We will probably want to see you again, to see how you are progressing with that, next year. Thank you again.