HOUSE OF COMMONS

Public Accounts Committee

Oral evidence: Government Cyber Resilience, HC 643

Monday 10 March 2025

Ordered by the House of Commons to be published on 10 March 2025.

Watch the meeting

Members present: Sir Geoffrey Clifton-Brown (Chair); Mr Clive Betts; Mr Luke Charters; Rachel Gilmour; Chris Kane; and Sarah Olney.

Member from Public Administration and Constitutional Affairs Committee present: Lauren Edwards.

Gareth Davies, Comptroller and Auditor General, National Audit Office; Tom McDonald, Director, National Audit Office; Adrian Jenner, Director of Parliamentary Relations, National Audit Office; and David Fairbrother, Treasury Officer of Accounts, were in attendance.

Questions 1 to 83

Witnesses

I: Joanna Davinson, Interim Government Chief Digital Officer, Department for Science, Innovation & Technology; Vincent Devine, Government Chief Security Officer and Head of the Government Security Function, Cabinet Office; Cat Little, Chief Operating Officer for the Civil Service and Permanent Secretary to the Cabinet Office; and Bella Powell, Cyber Director, Government Security Group, Cabinet Office.

HOUSE OF COMMONS

Report by the Comptroller and Auditor General

Government Cyber Resilience (HC 546)

Examination of witnesses

Witnesses: Joanna Davinson, Vincent Devine, Cat Little and Bella Powell.

Q1 **Chair:** Good afternoon, everyone, and welcome to the Public Accounts Committee on Monday 10 March 2025. Cyber attack is one of the most serious risks facing the UK and can severely impact Government operations, public services and people's lives. The Government's cyber security strategy, published in 2022, noted a large gap between where Government's cyber resilience is and where it needs to be.

The cyber threat to Government is severe and evolving rapidly. The Government clearly need to keep pace with this threat, but ageing legacy IT systems and shortages of cyber skills create significant challenges, which we will examine today. We will look at how the Government understand the severity of the cyber threat that they face and how they can best achieve the aim of the strategy and build Government resilience to cyber attacks.

To help us with all that, we warmly welcome our witnesses. Cat Little, the permanent secretary and chief operating officer of the civil service, is a regular attender at this Committee and was appointed in 2024, following her previous role as second permanent secretary at the Treasury. Vincent Devine, head of the Government security function and Government chief security officer, was appointed in December 2021. Bella Powell, cyber director of the Government Security Group, joined the Cabinet Office in September 2022; I think it is your first appearance before this Committee, Bella, so a warm welcome to you. From the Department for Science, Innovation and Technology, we have Joanna Davinson; we saw you recently, Joanna, and you are welcome again. Joanna is the interim Government chief digital officer and was previously director general at the Central Digital and Data Office and head of the digital and data function.

A warm welcome also to Lauren Edwards MP, a member of the Public Administration and Constitutional Affairs Committee, which also does hearings in this space.

Without further ado, I will start with Cat Little. An awful lot of different organisations, groups and everything else are involved in the whole sphere of cyber. How do they all work with each other? Could the whole lot be streamlined?

Cat Little: Thank you very much for having us this afternoon.

The first thing to say is that this is an incredibly complex and team-based set of issues, so it is important that our national security teams, the intelligence community, our technology experts, Departments and our security experts work closely together. There are always questions about

what the best structure is, which I will say a little more about, but the most important thing is how we work together to make sure that the different experts are working as one team to manage the threat and respond.

When it comes to the different roles, the Cabinet Office is responsible overall for three big things: first, the policy and strategy setting; secondly, the functional standards that we expect people to apply; and thirdly, assurance. There are different roles for DSIT; I will not go into all the detail, but DSIT it is looking much more broadly at the technical expertise that we have. The National Cyber Security Centre is the lead for response and co-ordination and for making sure that it is independently advising Government on the threat and the assessment of the threat.

It is very easy to say, "Surely you can combine all these things and just do them all in one place." I am quite sceptical, in part because we need to have the right political oversight and ministerial accountability, which of course we cannot do with an arm's length body or through the UK intelligence community—that is not their direct function. Crucially, we need different expertise. This is so pervasive, across so much of what Government and the public sector do, that I do not think it right to assume that simple, streamlined governance is automatically the right answer.

Having said that, we have done a lot of work to make sure that our accountabilities, our responsibilities and our ways of working are as effective as possible. As you know, the recent machinery of government change, moving our digital and technology capability into DSIT, gave us a good opportunity to do that. I am sure that further questions will be asked constantly about structures, but ultimately that is a matter for the Prime Minister and for political colleagues.

Q2 **Chair:** I do not mind which of you answers this question. Imagine that I am the permanent secretary of a Department; it is a Monday morning, and my phone is red-hot. People are ringing me to say that their systems are acting in an odd way or not acting at all. Who do I ring?

Cat Little: Let me start, because this is not an unfamiliar situation, as you might imagine. We expect the security teams immediately to pick up the phone, probably to Bella, who will instigate an urgent response across GC3, the three parts of Government that need to be notified and to react. Bella should take it from there.

Bella Powell: I am happy to give a bit more detail on that. The cross-Government response to incidents of that type is set out in the national cyber incident management framework. That policy document essentially sets out the totality of Government's response to serious incidents of that type. The Government Security Group has a really important role to play within the Cabinet Office. We are responsible, through the GC3, the Government Cyber Coordination Centre, in partnership with the NCSC and the Government Digital Service, for helping Departments to respond to that type of incident. So the perm sec would commission their security team to get in touch with the Government Cyber Coordination Centre,

either directly, via the NCSC, or by going to GC3 directly. They will provide support to that organisation in immediate response.

The National Cyber Security Centre also has a critical role to play in providing broader technical advice, support and guidance, both to Government organisations and to that individual organisation in helping it to respond.

The national cyber incident management framework also sets out the process by which we would convene broader cross-Government governance as necessary. We have the Cobra process, which helps us to understand and to provide the cross-Government set of actions, including things like attribution, understanding how broader public sector organisations need to respond to an incident, how we understand the overall impact and how we co-ordinate across wider Government. So we have a really clear process in place, and we also have direct support to individual Departments for how they can respond.

Q3 **Chair:** Would every permanent secretary know what to do in that situation, absolutely backwards? They would—I see Cat Little nodding.

Cat Little: I am very confident of that, partly because I cannot think of a single Department that does not have cyber risk on its risk register, transparently set out, along with the protocols. We also have very expert security teams who would be advising permanent secretaries if there were any breach of this sort.

Joanna Davinson: All Departments have chief information officers, and generally the security teams are very well plugged into them. A permanent secretary who needed advice would, I imagine, go straight to their CIO, who would be able to guide them.

Q4 **Chair:** That is very helpful. I am going to direct this question to you, Vincent Devine, and ask you to tell us what you can in answer to it. How worried should we be about the cyber threat to the Government?

Vincent Devine: I think we should be extremely worried. The NAO Report sets that out very well; we have summarised the threat for the NAO. Over the last three years, the threat has grown and evolved. Our adversaries, who are both hostile states and criminals, have developed capability more rapidly than we expected. Their risk appetite has changed, particularly with some hostile states; I will not name names here. They have been more aggressive and more careless in their attacks than we had expected. Finally, the nature of the threat is evolving. We have been principally concerned in the past about the loss of Government information—classic espionage—or about cyber crime, which again is information based. We are now also worried about the risk of disruption of essential services. I think the fact that the threat has surprised us with its pace is underpinning most of the analysis in this Report.

Q5 **Chair:** What are some examples of cyber attacks? Very briefly, can you set out one or two things that are happening at the edges of this whole scene at the moment?

Bella Powell: Yes, I can absolutely give you some examples. If we think about the threat, we think about it in two broad categories: first, ransomware and data extortion, as Vincent has set out, and secondly, nation-state attack.

Ransomware and data extortion tends to be perpetrated by organised criminal groups. A great example that shows the impact that can be felt from that type of attack is the attack on the British Library that occurred in October 2023. The British Library is still recovering from that incident. Some 500,000 records were published on the dark web. Several terabytes of data were stolen.

The majority of the server estate was encrypted. It now estimates that it has cost between £6 million and £7 million—over 40% of its financial reserves—to respond to that. The British Library has also been incredibly transparent about its response to that attack, the role that the amount of legacy technology that it had played in its resilience levels and how that resulted in a greater impact, which is a challenge that is common to broader public sector organisations. That is a great example of the impact of ransomware and organised criminal activity.

On the nation-state front, we have two categories that we are particularly concerned about. With espionage, a really good example of the type of action we see is a campaign of activity by the Russian GRU that was called out by the National Cyber Security Centre last year. That was a campaign of espionage activity that included data exfiltration, website defacement and data leakage activity. It is a really clear insight into the scale of activity that is conducted by nation states for espionage.

Disruptive and destructive activity is an area of increasing concern for us. In February 2024, the NCSC and its international partners co-signed an advisory warning of activity by a group known as Volt Typhoon, a Chinese state-affiliated actor that has been identified as conducting pre-positioning activity on US critical national infrastructure, with the potential to escalate that to disruptive and destructive activity. That is a clear indicator of the scale of threat from Chinese state actors and their intent to disrupt essential services.

Q6 **Chair:** For public consciousness, can you give us an example of something that has really affected the public? It is one thing affecting the functioning of Government Departments, next steps agencies, arm's length bodies and so on, but can you tell us about something that has affected the public?

Bella Powell: The ransomware incident that impacted the Synnovis pathology lab is a great example of that. Although that was a component of the supply chain to the public sector, the direct impact on individuals was really quite substantial. More than 10,000 NHS appointments were disrupted and significant amounts of data were put at risk as a result of that incident. We have seen several examples of that ilk, whereby an incident has had a direct impact on a supply chain organisation—in some instances, several layers down the supply chain.

A couple of years ago, the incident affecting Hackney council had a direct impact on individuals within that area; several public services were disrupted for a period of months. Redcar and Cleveland council, similarly, suffered a quite significant impact as a result of a ransomware attack, which disrupted services to the local authority and to individuals in that area.

Q7 **Chris Kane:** Do you think it is seeping into the public consciousness? When we talk about cyber, it always strikes me that we are describing attacks from countries and talking about big deployments. Do you think this is getting into the public consciousness as much as it needs to?

Cat Little: I think it is, partly because we have seen cyber crime and cyber fraud increase significantly over the last five to 10 years. It is now one of the biggest categories of crime we are dealing with at large. It is not just the Government and the public sector; we are increasingly seeing an impact on other parts of the economy. Several banks have had challenges with cyber. All parts of our lives, whether they are public or state-run or in the private sector, are increasingly seeing the threats evolve and take place.

Q8 **Chris Kane:** Let us talk about the constantly evolving nature of this. What assurance can you give us that the Government are keeping up with and ultimately staying ahead of that growing and changing threat?

Cat Little: I will start, and then I will turn to Vincent and Bella. The first thing to say is that, as Vincent described, the threat has significantly evolved: it has become more sophisticated, and the circumstances have changed very rapidly. If I look back over the last few years, we already had a gap in our ability to respond. In order to keep pace, we are having to work twice or three times as hard to evolve and constantly be as on the front foot as possible, but my honest assessment is that there always will be a gap. No matter how quickly we close down our risks and mitigate them, our ability to keep up is increasingly a challenge. I would not want the Committee to think that we were not trying to close that gap, but we are running against the tide constantly.

The Chair commented on some of the challenges that make it particularly difficult in Government. The state of our legacy IT—the scale and complexity of it—is a very serious issue, as is our ability to recruit, retain and develop the right skills at the pace we would like. I am sure that we will come back to these topics.

I think we have a genuine challenge on how we keep pace. Our best effort is to keep evolving, to close that gap as much as we can, and to do it with the best possible value for money with taxpayer resources.

Vincent Devine: In a sense, we are in the kind of technology race with which colleagues in Defence will have been very familiar over the last 50 years. We cannot say to you that we have a plan; we have a set of proposals that will guarantee our security for the next five to 10 years, which we will need to keep evolving as our understanding of the threat develops.

I am sure that the threat will continue to grow. Our challenge is to ensure that the risk remains flat, at best, or reduces. It is about understanding the threat, developing responses and managing down the risk. That is what we aim to do. But we need to be very honest, as Cat said: we cannot offer you any assurance that we fully understand the future evolution of the threat or that we can always stay ahead of it. It is about mitigating it.

Bella Powell: The NAO Report rightly points out that at the moment we are not responding to the scale of the threat that we see. Our resilience levels are not sufficient to be able to respond to it. When we think about the evolution of the threat, that is why it is so important for us to focus on resilience as a concept.

The way we deal with an ever-evolving threat landscape, where we do not necessarily know how a threat actor is going to change, what new technology is going to be available or what new tactics, techniques and procedures might be employed, is to focus on layered controls and layered resilience. That is why the Government's cyber security strategy sets out a framework that is very closely tied to the NCSC cyber assessment framework and the resilience outcomes that are defined there.

If we can achieve that set of layered controls, even if the threat environment evolves, we will be able to have multiple layers: either we detect an issue and respond effectively to it or we have recovery plans in place if an attack is successful. Again, as the NAO Report sets out, we are not in a place where we are at those resilience levels right now, but that is why that resilience approach is so critical.

Q9 **Chris Kane:** My question was what assurance you can give that the Government can keep up or stay ahead. What I heard there is that staying ahead of the threat is nigh-on impossible, as is reacting to it, because you do not know what the threat will evolve into.

Let us park that for a minute and talk about keeping up with the threat as it is evolving. Are you in the race: not getting significantly behind, and not finding that those that would do us harm are pulling away? Are you in the race and keeping in the race?

Cat Little: Absolutely. Our National Cyber Security Centre is one of the most advanced organisations for understanding and assessing the threat. We work as part of a global community; we are not in isolation. We use all the best intelligence that we have to assess the evolution of the threat. The brilliant work of my colleagues here is to do everything we can to be agile in responding and mitigating, but fundamentally we are in the race. We are pretty good at what we do, but staying in the race and at the top of the pack is a constant challenge.

Q10 **Chris Kane:** Can I ask about AI? We are talking an awful lot about AI in pretty much every session at the moment, so let us spend a couple of minutes talking about AI and the cyber threat. I want to leave it as almost an open-ended question for comment from you. How is it impacting and what is your thinking around AI and cyber security at the moment?

Cat Little: One comment from me—the experts should add to this, particularly Joanna—is that ultimately AI is built on and utilising data on a technology stack, so fundamentally we need to make sure that the technology stack it sits on is secure, resilient and fixed forward to be ready for AI. A lot of this comes back to the conversations that we have been having about legacy IT, because if we are deploying AI on top of technology stacks that are not resilient and not secure, obviously we need to manage those vulnerabilities effectively. Joanna is our expert.

Joanna Davinson: AI presents an enormous opportunity, but it does also mean that we have to be very thoughtful about how we manage our technology risk. A key thing that we are now doing is looking at "secure by design". We have an approach to ensuring that all new technology development across Government is secure by design. That has a set of principles behind it on how you build security into new capabilities, as you create them. That is the key control that will enable us to ensure that, going forward, we have secure and resilient systems. The legacy issue is a whole other set of challenges that we need to deal with.

Q11 **Chris Kane:** I want to close that off very quickly, because we could spend forever talking about AI in every session that we do. I see AI being used to cure diseases, and it feels like AI is approaching things in a way that humans cannot. Are we headed to a world where the threat actors are going to be just setting AI loose to try to find weaknesses, and you are going to be setting AI loose to try to find the solutions? There is almost going to be a human hands-off approach, and that is a massive challenge and a massive change.

Vincent Devine: We have put our formal assessment of the impact of AI into the public domain. AI will not create new threats but will exacerbate the threats that are already out there. Our adversaries will be able to use that AI to probe our defences. They will be able to use AI to write coding to challenge them and to use it in other ways that damage Government, such as misinformation.

If we introduce AI wrongly, it will also create new vulnerabilities for us. I think we are pretty confident that we understand the risks and will not create those new vulnerabilities. Thirdly, we need to use AI as part of the defence. As our adversaries are using AI to probe us, we are developing ideas on how we can use AI to monitor, protect, detect and potentially hunt down attacks.

Chris Kane: Thank you. We could spend forever on this subject.

Chair: Between you, you have covered what is needed on AI, or for the moment anyway.

Q12 **Mr Betts:** I want to come on to the issue of making the skills and the challenges there, including not having enough skilled people to meet the challenges that Departments have. Today, *The Times* says there is going to be a recruitment push to double IT experts in the civil service. Given that we have had challenges in recruiting more IT experts for the last 10

years, and it has not been successful, why should we believe that the new attempt should be successful?

Cat Little: The first thing to say is that we have been successful in significantly expanding the number of technical and digital experts within Government, and I am sure Joanna will want to add to this. If you look at the size and scale of digital expertise in Government, we are now up to 23,000 people within our technical teams. That is a massive shift, so I would refute the suggestion that we have not been successful—that has been a massive endeavour for us.

Specifically on cyber skills, it is a challenge for the whole of the economy; this is not just a public sector or central Government issue. A couple of years ago, we published a report in Government that set out that there are large vacancies in the private sector, as well as in Government, so there are things that we need to do. One is grow more of our talent from within, and that is why we have our cyber fast stream and the tech track, which I talked about a couple of weeks ago and that is the doubling of our apprentices working in technology.

We have a new digital pay framework that is designed to be much more competitive and to attract people into Government based on the quality and the variety of the work that you get to do here. That is starting to have an impact. It is right that the Government are being ambitious and saying that we need to double the number. One in 10 is absolutely where we need to get to, and a combination of things will contribute to that being a realistic and necessary thing for us to do within the civil service.

Q13 **Mr Betts:** Coming back to your concern that I said you have not been successful, shall we say that you have not been fully successful? The Report that we have in front of us today identifies 751 cyber-security vacancies. There is a limit to the success at present, is there not?

Cat Little: We would like to be more successful. There are significant vacancies, particularly on cyber skills and particularly in the very high-end cyber skills that we need. That includes the skills required for penetration testing and some of the risk management work that we need to do. It saddens me that we are far too reliant on contractors and bringing in external expertise. What those vacancies are really showing is that we are filling the gaps through the use of expensive private sector expertise to come to help us deliver this work in Government. That is why it is so important that we build that talent and scale up our activity. Joanna should comment on this.

Joanna Davinson: I think you said it. The overall number of digital, data and technology professionals in the civil service has grown. We are now at nearly 6% across the whole civil service. It is not as much as we would like it to be, but as Cat says, we are really struggling with the very technical resources. That is a market problem: they are scarce in the private sector as well as in the public sector, so we are competing in a hot market for those skills. We have a range of initiatives to address that, particularly around our early talent approaches and how we are developing

the digital, data and technology pay framework to ensure that we can reward those very-hard-to-recruit skills at closer to market rate.

Q14 **Mr Betts:** There are 751 vacancies, some of which are filled by external agency workers and consultants coming in. Is that correct?

Cat Little: They are partly filled by external support, yes.

Q15 **Mr Betts:** How many vacancies have you got, then, that are literally vacant, with no one filling them?

Bella Powell: We will have to come back in writing.

Cat Little: We will just flick through this document to see if we have that data, but as you can imagine, every single week, we have different stats and different data on vacancies.

Q16 **Mr Betts:** Some idea would be helpful.

Cat Little: We can set that out.

Q17 **Mr Betts:** Why is there a gap at all? The NAO Report mentioned civil service recruitment procedures. If that is what it is, why have they not changed?

Cat Little: I will comment on civil service recruitment, and specifically on technology. The Committee has looked at this in multiple ways, andcivil service time to recruit has not been good enough. We had some data a couple of years ago that suggested that on average it took up to nine months to recruit some of the technology specialists that we needed. That was absolutely recognised at the time, and my central HR team has been relentlessly focused on reducing the time taken to recruit. We have been piloting different methods, different uses of technology and different ways of attracting people, so that we can shorten that time. We have just done a pilot in my Department where we have managed to get it down to two weeks. That is a fundamental thing for the whole civil service, not just for tech expertise.

Bella Powell: To come back to the previous point, we do not have the detailed information on the 700-odd roles that you defined—we can come back in writing on that—but the overarching statistic that really lays out the scale of the problem is that one in three cyber security roles across Government are currently either vacant or filled by a contractor. That gives a really clear view of the scale of the challenge.

Something we recognise we can be much better at doing is tapping into currently untapped pools of talent. The cyber security community and the digital and data community across Government is currently not a diverse community. Something like 20% of cyber security individuals are women, according to our current stats. It is not a diverse community right now. We can get much better at pulling into those broader pools of talent.

We have a really fantastic initiative that is being piloted for us this financial year by the Department for Work and Pensions. It builds on one of its initiatives: the Government Cyber Security Academy. That had

21,000 applications for essentially a reskilling programme for individuals coming from different careers and wanting a career in cyber. It also has excellent statistics on representation of diverse groups.

We can get much better at bringing in those broader pools of talent. That is one of the key levers for us in understanding how we can tackle the scale of our skills gap.

Q18 **Mr Betts:** I have a couple of follow-up questions. You mentioned one example, the Department for Work and Pensions. How far are you working across Government to try to address this, rather than letting each Department do its own recruitment in a very particular way?

Bella Powell: A number of central initiatives are already under way. Cat mentioned a number of them, including the DDaT pay framework, which is a cross-Government initiative, and the apprenticeships programmes, which we already have in place, and also the cyber fast stream.

The DWP academy is being run on behalf of the whole of Government, so the graduates from that programme will be deployed across Government. That is part of a broader approach that we are taking to step up our transformation across Government from a cyber perspective.

We are taking a much more interventionist approach from the centre as part of our response to our understanding of current resilience levels and to change the way that we deliver across Government. That also includes a new series of skills interventions, of which the cyber academy is one, which will help us to tackle the scale of the risk at the moment along with those skills gaps.

Q19 **Mr Betts:** Coming back to the point about civil service processes and procedures, is it really the case that historically the civil service has tried to recruit highly specialist, technically skilled staff with a very restricted pay regime because it does not want to enhance the pay of everybody, and that it will not do that just for the digital experts?

Cat Little: That is exactly why we have brought in a specific digital pay framework. I cannot tell you that it is matching what some of these experts would get in the private sector, but it is certainly much more competitive. The civil service has to be much more targeted and segmented in order to get the right specialists to come and join us. We cannot kid ourselves into thinking that people will join on the same salaries as the rest of Government.

Q20 **Mr Betts:** No doubt you will get headlines about some expert being paid more than the Prime Minister, but we will just have to live with that.

Cat Little: I can assure you that will need to be the case in order to attract them. At the moment, Joanna is on several recruitment panels for our most senior Government chief information officers. We have got to pay these people more. They are very scarce competitive salaries in a very hot market. If we are going to deliver on our ambitions, we need the leadership and the technical expertise there to do it.

Vincent Devine: It will still be significantly cheaper than using contractors, which is what we are driven to do. It will also be a cost saving in the longer term if we prevent some of the risks that we are talking about maturing.

Q21 **Chair:** Contrary to what many people think, the Committee is here to help the Government. So, while we are critical when the Government get things wrong, we should equally be complimentary when they get it right.

To upgrade you on what you said, paragraph 2.4 on page 24 of the NAO Report states that, "When GSG set up the cyber directorate, 32% of the roles it planned to recruit were vacant…By May 2024, this improved to around 12% of roles vacant." That was exactly in line with what you said, Cat, and it was a significant and welcome improvement at the centre. We are still obviously way down in some of the departmental roles.

Cat Little: If I could expand, this is all credit to Vincent, Bella and Joanna. We basically set up a whole new cyber directorate in the Cabinet Office and we are now at full complement. We have got some brilliant experts that we have been able to attract from all sorts of different backgrounds. Those people are doing a really tough job in very difficult circumstances.

In 2022, we had the tragic circumstances in Ukraine. The threat picture increased dramatically at the same time as we were trying to set up a new organisation and to get it set up for success. It is a real credit to Bella and my colleagues on this panel that we have been able to do that.

Chair: Indeed.

Q22 **Rachel Gilmour:** It is worth really noting what you just said about the cost in terms of it not just being about how much people get paid, but how much money you save in the long term. You cited the British Library, and the cost of 40% of its reserves, £6 million or £7 million. That is a drop in the ocean of what it would cost if there were any other cyber breaches. I think people have just got to grow up—and if there are members of the media listening to this, grow up.

Chair: Never understated, Rachel.

Rachel Gilmour: Never knowingly undersold.

Q23 **Mr Charters:** We have had a discussion about recruitment, and that is, of course, a key component to increasing the Government's capability across Whitehall. But we have also got to pivot existing civil servants' skills and time in terms of what they spend their day to day on.

Do you agree with the thesis that every hour a civil servant spends on photocopying and using a fax machine is an hour less that we could be using for productivity when it comes to our cyber defence?

Cat Little: I totally agree with that. Part of our work at the moment is to prioritise making the civil service—indeed, all of the public sector—much more productive and much more agile. People join the public sector because they want to make this country a better place, they want to serve

citizens and they want to deliver the very best outcomes for the people of this country.

Our own people get very frustrated when they are bogged down in bureaucracy and inefficiency, and they do not have the tools to do their job. So, given where we are coming from, we have got to invest in the right tools and services to deliver better services to citizens, but we have also got to upskill the public sector, which is partly about giving them the right technology—everything from issuing the right laptops to providing the right interoperability with other Government Departments. However, it is also about just saying that if you are spending your time filling in forms, trying to get permission to do sensible things, we have got to cut that sort of stuff out, because every hour should be spent with citizens on the frontline.

Q24 **Mr Charters:** Are you willing to lead by example, get rid of photocopiers in the Cabinet Office and go fully digital?

Cat Little: I am certainly taking on the challenge of doing much more digitally. Normally, I do not carry papers around with me; I do so for hearings like this one, but normally I just use my laptop. It really pains me to see huge amounts of paper copies being printed out when you could do these things digitally much more effectively.

Q25 **Mr Charters:** On fax, just before I move on—time for a moratorium on the use of fax across the entire public sector?

Cat Little: I am not sure if I can commit to that. By the way, I do not think I have ever used a fax machine; most of our staff do not even know what a fax machine is. I remember coming to the civil service and going to a legal body, and being told, "Oh, there's a microfiche over there", and I had never seen a microfiche before. It is absolutely right that we are using modern, 21st century technology and phasing out anything that does not increase productivity.

Q26 **Mr Charters:** Moving swiftly on, the Director of the NCSC, Dr Richard Horne, said in December of the cyber security risk: "The severity of the risk facing the UK is being widely underestimated". In those remarks, he was referring to the public and private sectors. Historically, do you think that Departments have underestimated the cyber risk?

Bella Powell: It is very reasonable to say that until recently we have not done a great job of making sure that leaders across Government have the right level of understanding of the scale of threat. We have made some significant changes in that, particularly over the last three years, ensuring that senior leaders across Government have a really clear picture of what the threat environment looks like. But probably more importantly, we have only recently started to give a really clear picture to senior leaders across Government of what we expect of them—what the required resilience levels are to be able to respond effectively to that threat.

So, as part of the Government's cyber security strategy, we have set very clear targets at cross-Government level for organisations to improve their

resilience levels. We have also codified those against the NCSC cyber assessment framework, but that is a recent improvement.

We launched GovAssure in April 2023 and that was the first time that we really set out those concrete objective requirements for Government Departments in terms of the resilience levels that they need to achieve to be able to respond effectively to threats. I think that part of the challenge is getting to a very concrete and measurable set of outcomes that permanent secretaries can prioritise appropriately, and I think we are in a much better space now as a result of that.

Q27 **Mr Charters:** So, you would freely admit that only until relatively recently did Departments accept and understand the risk from hostile states and so on?

Bella Powell: I think that is absolutely reasonable to state, but I think it is also worth noting that this environment has changed very rapidly, particularly over the last three years. We have seen a substantial escalation in threats. The technology environment has changed enormously and the Government's cyber security strategy is our response to that. But you are absolutely right: there has been quite significant work over the last three years to improve that position.

Q28 **Mr Charters:** I turn now to something in the NAO Report about leadership, which is on page 16. The summary there says that "accounting officers should: ensure that membership of their most senior decision-making board includes at least one digital leader with cyber expertise". I am sure you agree with that. Could you just comment on your own board in the Cabinet Office, permanent secretary? Do you feel as though you have got that level of expertise and that you are leading from the front?

Cat Little: Obviously, I very much agree with it. I actually currently do not have a full board in the Cabinet Office, because, as you may be aware, we are recruiting to a whole new set of non-executives. But we have mandated in our recruitment process that we are looking for at least one digital and tech expert to join our board, and we expect the same of every other Government Department.

Q29 **Mr Charters:** That is a perfect answer, thank you. I will turn to some of your leadership role with respect to other Departments. One of the most concerning cases was the Synnovis attack. I know you are not from the DHSC, but do you feel like Departments such as that are properly responding to some of the potential threat from state-based actors and hostile states? It is those sorts of NHS attacks that could affect my constituents in York.

Cat Little: Bella said a little about the increase in education and understanding. One of the first things that I did when I took on this post last year was to convene all the permanent secretaries together to talk about cyber risk. That was to make sure we all understood the sort of threats that were out there, but also to talk about our responsibilities, because, as you know, under our accountabilities, accounting officers and permanent secretaries are responsible for the overall control environment,

reporting, risk mitigation, and making sure that they have the right resources to take action, as well as, under the new GovAssure arrangements, making that they have a plan to close the gaps that we have identified.

I have also recently written to permanent secretaries, reminding them of their duties and the sorts of things we should do together to help to manage the risks. I very much believe that my permanent secretary colleagues not only understand the risks, but take it very seriously. As we get into the spending review, where choices have to be made about where you allocate scarce resources for technology, legacy IT, and managing cyber risk, it is the very top of Departments who are involved in those conversations.

Q30 **Mr Charters:** Finally, do you feel as though there is a growing risk from Russian cyber crime groups to our NHS?

Bella Powell: It is absolutely right to say that Russia poses a substantial risk, not just to health sector organisations, but more generally. We see Russia and China as both, from a nation state perspective, substantial risks. Russia tends to be an irresponsible actor, so the NCSC describes them in that context, and what that means in practice is that there may be significant impacts across a number of organisations from a UK perspective. I am happy to provide more detail in writing, if that is helpful.

Q31 **Chair:** Before I bring Lauren Edwards in, I would like to follow up on one of Luke's questions, perhaps for Cat Little and Joanna Davinson. We have discussed in this Committee many times before the need to have a chief digital data officer at a senior level in a Department. Surely, we should equally want a chief security officer or a chief cyber officer—whatever we would like to call them—at the same, senior level in a Department, and them talking to each other very closely about matters of procurement and security. Is this not a cultural change in all Departments and all Government next steps agencies that we are about? How will we do this?

Cat Little: I very much agree with the premise of that. I suppose—just before I hand over to Joanna—that there are very different scales and levels of threat in different Departments. One of the biggest challenges if you are a small Department is recruiting any cyber experts, because we tend to be able to recruit very top-end people into organisations such as the MOD and the Home Office, which are really exciting different environments to work in, but if you are a small policy Department, that is less appealing to quite a lot of people. The premise that we should have senior people accountable, at the very top end of the sort of expertise proportionate to the risk that a Department has, is absolutely right. The recent DSIT publication on the "State of digital government" set out the need to have a very senior CIO in every single Department as standard. Joanna should add to that.

Joanna Davinson: I think you've said it. The "State of digital government" report clearly showed that, although we have some Departments with chief information officers and chief security officers at

ExCo level, it is actually very few, so there is still work to be done with other Departments to ensure they have an accountable individual who has the experience and capability to advise the ExCo and the board on matters of information technology and security. That is one of the reasons why I am spending quite a lot of my time supporting Departments to interview for senior leaders across Government. It is really important that we get a good and consistent standard, in terms of the skills and capabilities of those individuals.

Q32 **Chair:** Can I challenge one tiny part of your answer, Cat Little? Small Departments such as DEFRA probably have not invested a lot in the past few years in legacy equipment, and therefore their likelihood of being subject to a cyber attack is greater, because it is easier to do. If even a small Department such as DEFRA seriously went down, it would inconvenience a lot of members of the public.

Cat Little: Absolutely. To clarify, I am saying that it is more challenging for smaller Departments to recruit. DEFRA is a good example: it has a second permanent secretary and a director general who are accountable and responsible for bringing together technology and cyber issues. My point is more that it should be proportionate to risk. Recruiting the chief information officers who we are trying to bring into Government is a challenge as it is. We have to be realistic about whether we can attract the very best cyber people and where we deploy them to have the maximum impact.

Q33 **Lauren Edwards:** Thank you very much for coming here today. Paragraph 4.9 of the NAO Report raises concerns about Departments being reluctant to share information about their cyber incidents with other parts of Government. A common theme I am discovering with Whitehall is that GDPR is almost used as a "Computer says no" response. Obviously, that is quite a challenge, particularly when you have a new Government that is very focused on its missions, a large number of which are obviously cross-departmental. It is particularly concerning for cyber incidents. As Bella mentioned, we have the example of the British Library being really transparent about theirs and all the lessons that were learned from that. There is obviously a bit of a concern that that is not happening in Whitehall, and that information is not being shared. Cat, what is the impact of Departments not sharing information about cyber incidents?

Cat Little: First, sharing data in a mission-led environment is essential, particularly for cyber, where we want to learn lessons, look at vulnerability, share best practice and work out what has gone wrong. We need that openness from a humble and sharing perspective.

There are sometimes good reasons why Departments are not able to provide that information or are concerned about reputational damage. It is our job in the centre, because generally we know what has happened, to really challenge those Departments on their risk appetite and help them to manage any risks or concerns that they are worried about.

This connects to one of our previous hearings about the culture and approach to data. We tend to take quite a risk-averse attitude. We will not learn or do our very best to get insight if we do not take a much more front-footed approach. The work that Joanna's Department is doing on the national data library and breaking down barriers to sharing data is absolutely essential.

Q34 **Chair:** Can I come in on the back of that? Sorry, Lauren. You are one of the most security-conscious parts of Government. Surely even if there were a reputational risk or a security issue, it is critical that the data and what happened is shared—we are not necessarily talking about publishing these incidents—with your Department.

Cat Little: I can only agree with you. Especially when we are trying to co-ordinate and respond to what could be a consolidated attack—quite often, one of our jobs is to work out whether there is a consolidated attack on different parts of Government—it is essential. Vincent and Bella have to live with this day to day.

Vincent Devine: I want to reassure you, first, that we obviously ensure that, if a vulnerability is exposed by the attack, we share that. If there is an impact beyond the Department on other Departments or individuals, we share that, too. But equally, we recognise that we would like to be more transparent in sharing incidents because there is both a lesson learned element for all Departments and a human element to permanent secretaries hearing how other permanent secretaries experience an incident. One of the most powerful meetings I have attended in this role was when a chief executive of one of our big companies got round a table with other chief executives and talked them through an incident that he—it was a "he"—had experienced. He talked about how real, dangerous and expensive it was for the company.

We absolutely agree; we should be more transparent. We are continuing to work on that. But I want to reassure you that we share immediately when there is a potential impact on either the systems or the people of another Department.

Bella Powell: On that point, the Government Cyber Coordination Centre is an initiative that we launched relatively recently, in September 2023. Through that joint initiative, we have made some strong progress, particularly on allowing ourselves as Government organisations to defend better as one, as opposed to in silos, and to share information more effectively across various organisations. The GT3 is effectively our operational response team. It draws in capability from across the National Cyber Security Centre, the Cabinet Office and the Government Digital Service and works with Departments to respond to threats, vulnerabilities and incidents. We have seen some great progress there, particularly in improving transparency, increasing the flow of information and being more data-driven in our response.

Q35 **Lauren Edwards:** That pre-empts one of my questions: what practical structures do you have in place to disseminate that kind of information?

The information about the co-ordination centre is helpful. How do you ensure that information is disseminated not just to permanent secretaries, but throughout the Departments?

Bella Powell: One of the most important components of the Government Cyber Coordination Centre is the communities it is built on. We have four strands of activity within the co-ordination centre: response to incidents, response to vulnerabilities, understanding of threats and building communities across Government. Part of the challenge for us has been being able to bring network defenders together in a context where they can share understanding and technical expertise and share information in response to an incident.

Those communities, and bringing together individuals who are at the coalface of responding to incidents, have been a priority for us. We are still in the early stages of making sure that we have the right collaboration platforms and dissemination mechanisms for individuals across Government to communicate effectively, but that has been a powerful step for us in bringing those individuals together. The intent is that GT3 is built by network defenders for network defenders to help them to collaborate more effectively.

Q36 **Lauren Edwards:** Cat, earlier you discussed the need for culture change, which I agree with. How are you trying to embed a culture, not just within the Cabinet Office but throughout Whitehall, where people are encouraged to come forward and learn from near misses, rather than seeing mistakes or breaches of cyber policy as part of a blame culture, which means that people do not raise them?

Cat Little: That is one of our biggest cultural priorities. As the Department that oversees inquiries policy in particular, we have tragically learned from a range of inquiries that we have to make it much easier for all our public sector staff to raise a flag when things do not look right or are not going well and to accept that we carry a lot of risk, and it is only right and proper that we talk about it openly when we make mistakes. When Government are responsible for so many things that could go wrong—by default, we are dealing with complex and difficult issues—it matters even more.

The tone starts from the top. I and the Chancellor of the Duchy of Lancaster have spoken openly in the Cabinet Office about the importance of testing, learning and accepting that we will fail and get things wrong, and that is okay—it is absolutely okay. I need every line manager in the civil service to have the backs of their staff on the frontline and to say, "Don't worry about it. We all make mistakes." As long as we learn and share what we will do differently, that is the most important thing. I often use this example: in my first eight weeks in this role I wrote to the Committee probably three times to apologise for something that my Department did and to set out what we were going to learn from it and do differently.

I should say to the Committee that, quite often, having to come and explain ourselves to Committees is a reason that people are worried about saying, "Something is wrong." They think they will be hauled in front of a Committee to be told off. The more that we can make it normal for us to correspond—to come and talk to you, to say that we have not got everything perfect, but also to explain what we are doing about it, and to create the conditions for that sort of culture—the better. But I think it is really hard because of the complexity and the scale of what the Government do.

Q37 **Lauren Edwards:** That is really helpful, particularly to have that leadership right from the top within the Cabinet Office. Do you think that has permeated through all the other Departments across Whitehall?

Cat Little: It is inconsistent—that is probably the straight answer—because your risk appetite for failure is very different depending on the environment you are working in and the services you offer. We are a very large, complex set of different organisations, so it will take a while for us to be able to say confidently that every member of the civil service is able to put their hand up, admit mistakes, learn from them and know that they are safe to do so. Obviously, our annual people survey and the pulse surveys that we run are critical in helping us to understand whether we are shifting the dial.

Q38 **Rachel Gilmour:** On what you just said, my party leader, Ed Davey, said exactly that to me when I signed a letter supporting the wealth tax—by accident—so I wholeheartedly endorse that kind of leadership.

As you have admitted, the timeline for some of your ambitions, particularly the 2025 one, is tight. What are the implications of the critical functions of the Government not being cyber resilient by the end of 2025, because we are not that far away?

Bella Powell: As the NAO Report quite rightly points out, the scale of risk to Government is currently extremely high. That is a result of both the resilience levels across Government, which are substantially lower than we had previously anticipated, and the escalating threat environment. The sum total is that we are at critical risk at the moment. We have also set out targets in the Government cyber security strategy for 2030. They are also very ambitious, but will be achievable if we are able to move further and faster to tackle the scale of the resilience challenges that we see.

Chair: Thank you very much, Rachel. We are going to take a short break now. The clock stands at 4.32 pm, so can we be back at 4.40? Just before we formally break, I will say that microphones will be on, so be careful what is said—I am sure you are careful, naturally.

Sitting suspended.

On resuming—

Chair: We will now resume our session on cyber-security. I call Chris Kane.

Q39 **Chris Kane:** I want to talk about GovAssure, so let me set the scene. Paragraph 2.8 of the NAO Report states: "In April 2023, GSG started agreeing with departments clear and risk-based cyber resilience outcomes that they needed to achieve. It did this by introducing an annual cyber security assurance scheme, known as GovAssure". Paragraph 3.2 states: "Between April 2023 and July 2024, 35 government organisations took part in the first year of GovAssure. They self-assessed the cyber resilience of 72 IT systems they considered to be critical to running their essential services. The Government Security Group (GSG) has not tried to establish how many critical IT systems there are across the government's digital estate, but it considers that the assessed systems will be a small proportion of these." That is my long-winded way of setting the scene. Where are you in that assessment of the cyber-security of the Government IT estate? Have you assessed it now, and can you assure us that the Government really know where they are vulnerable to attack?

Bella Powell: I am happy to cover that, and then I might pass to Joanna to talk in more detail about how we deal with legacy. We have two primary mechanisms for understanding the resilience of the Government IT systems. The first is GovAssure, which is our new cyber-security assurance scheme for Government. That is focused on the enduring technology estate—the technology estate that will be with us for some time. We also have the legacy IT register and the associated legacy risk framework, which focuses on legacy systems and the risk that they pose.

I will focus specifically on GovAssure. It is a new initiative that we launched in April 2023. Exactly as you described, 35 Government organisations took part in year one, and we had 72 critical systems assessed in that first year. We are now in year two, and we are covering a number of additional services as part of that, but we are still in the process of gathering that data. GovAssure is intended to be a rolling assurance process, so we will never be done with that process; the intent is that it gives us regular updates on resilience levels across Government and a regular and in-depth picture of what those resilience levels look like.

It is absolutely right to say that the number of systems that we have assessed in year one is a small component of the total estate and even of the critical systems across Government, but it is also designed to be representative; so each organisation involved in the process has gone through a process of scoping with my team to understand which systems should be assessed in year one. The intent behind that is to pick critical systems, including critical national infrastructure, but also systems that are representative of those organisations and the services that they deliver; so even though the results we have gathered in year one are across a small number of systems, we are able to infer a significant amount about the total resilience of Government.

I am happy to go into loads of detail on this, but I will try to keep it brief. We assess systems against the NCSC's cyber-assessment framework and although we do that at the system level, several of those controls give us a really good indication of how those organisations as a whole will operate.

We assess things such as asset management, risk management and governance, as well as some of the more detailed system-level controls.

GovAssure year one has given us a detailed understanding of how resilient those individual systems are and how they are measuring against outcomes. It has also given us an indication of the overall cyber-resilience and health of the organisations taking part. We will get further information as we go through years two and three and so on, but the level of granularity and the objectivity of that data is already an enormous step forward for us and gives us a much better picture of what current resilience levels look like in practice. I am happy to go into more detail on GovAssure, but I am also happy to hand over to Joanna on the legacy framework, if that is useful.

Chris Kane: We will cover legacy IT in a minute, so let us stick with GovAssure. It seems like a good idea and a good approach, but what I am trying to work out is this. If we assume that it is a good approach from year one, it is going to be an excellent approach from year x, but what is year x? When does it start to become a situation where you have a massive amount of data, you have everything assured and you know that you have a rolling programme that is working at full efficiency, and how will you increase the scale and pace to get there as quickly as you can?

Bella Powell: I should start by saying that the intent is not to assess every single system across Government through that process. GovAssure, as Departments will tell you, is an intensive process. We do a lot of data gathering: the Department is required to gather a lot of data and evidence against an individual system and answer a lot of supplementary questions about that system to enable us to assess it effectively. It would be disproportionate to do that across the entirety of the Government estate or even across a big swathe of it, but it is important that we continue to assess critical systems and get to critical mass.

Most important for us is to start to build up a clear picture of where we see the most systemic challenges across Government and how we identify the root causes of those. Success for GovAssure is not having assessed every single system across Government; it is helping us to diagnose where the most significant issues are, what the scale of resilience looks like in totality across Government, and how we can take action from a central perspective to tackle the scale of those resilience challenges.

We are already getting that data, so we are conducting root cause analysis right now on the challenges we see at departmental level. We already know that asset management, risk management and response planning are particularly challenging areas that Departments across Government are struggling with, so we are also targeting central activity on being able to tackle those risks and those particular vulnerabilities.

Response planning is a great example: there is low-hanging fruit there, so while we see that that is at a low level of maturity across Departments currently, it is also a relatively easy thing to focus on and scale up. That is one of our areas of focus, particularly as part of the next financial year.

Cat Little: May I add two very quick things? First, like all good assurance processes, it is important that it is targeted at risk and is proportionate. As Bella said, we are not trying to do 100% assurance; we are trying to target the most critical systems that we have in Government. I think that is right, and it is a normal approach to assurance. Secondly, the baseline for GovAssure will evolve. In the same way that the threat is evolving, the standards we expect to be testing Government Departments and critical infrastructure against will change; the goalposts will keep moving. It is quite a dynamic process. To respond to your top-level question, we will never get 100% assessment, but we will keep raising the bar and ensure that the areas that are of most risk to us are assessed on a regular basis.

Q40 **Chris Kane:** Can we explore that a little further? If these are critical systems, what is the barrier to doing more? I take the point that it is disproportionate to use all the resources to do assurance, but if these are critical functions, is it an issue of resource? Would you do more if you had more resource?

Bella Powell: There is a number of constraints on the process, and one of the most important is the amount of resource that we have at departmental level focused both on cyber-security and on service delivery. The GovAssure process requires departmental teams to conduct quite significant amounts of assessment activity. If we focus the entirety of those service delivery teams' efforts on assurance activity, they are less able to conduct patching or to design updates to those services. I am caricaturing, but it is a challenging balance for us to understand how much effort we need to focus on that really rigorous assurance process versus how much effort we allow teams to focus on broader cyber-security issues.

Q41 **Chris Kane:** I could understand if you took all the Government IT systems and said, "The following are critical and the rest are not," but what I think I am hearing is that while you are identifying what is critical, you are not assuring all the critical systems; which, by extension, means that the non-critical systems, which are still important and still vulnerable, are not being assessed at all. Striking the balance between the art of the possible and the art of the ideal—again, is it about resource? If you got more digital specialists and had more money, would you do more? I am trying to understand how you can have so much critical infrastructure but you are saying, "Well, we can't deal with that because we don't have the resource."

Cat Little: If I may, I will take a step back from GovAssure and go to what accounting officers are responsible for within their Departments. They are responsible for having the right controls and assurance over cyber risk.

To take my own Department, I am not using GovAssure as my only source of assurance. I have a dedicated set of cyber and technical experts who are preventing risk every single day, they are undertaking their own assessments—I have critical infrastructure within my own Department—and they are regularly doing their own work to assure themselves in what we would call the first line of defence in our assurance processes. What

Bella is describing is the second line of defence and what we are doing to consistently assure ourselves in the second line. GovAssure is not the total control environment, and nor should it be.

Q42 **Chris Kane:** I am a little confused. If you are comfortable that your responsible officers are giving you that level of assurance, why do we need GovAssure on top of that?

Cat Little: Because this is about consistency. Any good control environment has three layers of defence and every accounting officer has to take a view about what we want in each layer of defence. What we spotted a couple of years ago is that there was no strong second line of defence, objectively and consistently assuring cyber risk for Governments. What GovAssure is doing is providing that second line of assurance, where previously there would have been a weakness. Sorry, I do not want to teach you about assurance overall.

Chris Kane: I am enjoying the lesson.

Cat Little: What we are trying to do is build up layers of assurance proportionate to risk. It is important that permanent secretaries take a view, but when it comes to the second line, we want consistency and to be able to share best practice. That is what GovAssure is designed to do. You need the first, second and third lines. The NAO is a really good example of the third line—independent, external, objective assurance, which also provides us with a layer of defence.

Q43 **Chris Kane:** So GovAssure is not going to ramp up in terms of the scale and pace. It is at almost a fixed pace that you are comfortable with for what it does.

Cat Little: That is not quite right.

Bella Powell: As part of year two, we are already assessing a larger number of systems than we did in year one; I think about 100 assessments have already been submitted to us across Departments. So we are ramping up the number of systems that we are looking at, but we are not doing that in an exponential fashion.

It is also worth noting that with GovAssure we are driving the car and building it at the same time. We launched it in April ’23 following some early pilots with Departments. It was still an early-stage assurance process. There is much more that we can and need to do, particularly in the automation of the process and providing stronger support and guidance to Departments in implementing it, as well in the root cause analysis, to better understand the data that we are gathering from that process. It is by no means a finished or perfect product, but it is already starting to give us the outcomes we need in the understanding of resilience levels and of where we can take action.

Chair: Thank you. I think we need to ramp up the pace a little.

Q44 **Sarah Olney:** My understanding of the role of GovAssure is that when it came in in April 2023, it replaced a system in which Departments were

self-assessing their cyber resilience. My understanding from the Report is that the assessments done by GovAssure showed that until then Departments had been overestimating their readiness. First, did that come as a shock? Secondly, what did you do in response to that increased awareness of the lack of resilience?

Bella Powell: You are absolutely right in that characterisation. Previously, Departments assessed their adherence to the Government cyber security standard as part of the departmental security healthcheck. That was a self-assessed process; it was also against a prior standard, which required a much lower level of resilience, and it was much more prescriptive in terms of controls. What we have moved to with GovAssure are outcome-based requirements set against the NCSC cyber assessment framework. It is, therefore, absolutely right to say that we are holding Departments to a higher and more appropriate standard of resilience, but also that the levels of resilience that we see across Government are substantially lower than we had previously anticipated.

In the previous self-assessed returns, around a quarter of Departments assessed that they were able to meet the cyber standard. We now know that achievement of GovAssure resilience levels is substantially lower than that across Government organisations. We can also see that there are particular areas in which there are fundamental control failures across Government organisations—in asset management, risk management and response, as I called out earlier.

We have also seen—the NAO Report mentions this—that there is a difference between the initial self-assessment returns that the Departments conduct in the GovAssure process and the independent third-party assessments that are conducted afterward. So even throughout the GovAssure process, we are seeing the difference between a kind of self-assessment for an organisation and an independent assessment.

We have noticed that, where we have more mature organisations, where actually they are achieving a higher independently assessed score in GovAssure, they are also better at self-assessing, whereas the less mature organisations have a more substantial gap between their self-assessments and what comes back in the independent assessments. Therefore, the need for that independent assessment has also kind of been validated through the process.

You are also right in saying that it has been quite challenging to see the scale of resilience that we have actually achieved across Government. It is substantially lower than we had anticipated, and it means that we will need to take a fundamentally different approach to tackling cyber resilience levels if we are to meet the 2030 targets. That is something that we are doing.

Q45 **Sarah Olney:** Thank you. Mr Devine, the GovAssure process was only introduced in April 2023, which seems quite late given how much we have known about cyber risks in the last decade. Why has it taken such a long time to bring it in?

Vincent Devine: That is a fair question, although I am tempted to say that I arrived in January 2022. I do think that, if we are honest, we have probably woken up more slowly than we should have to the scale of the cyber risk. I think the Report captures that well. We were probably unrealistic in relying on self-assessment and the minimum cyber security standards.

I was pondering your question about whether we were surprised by the difference between the results of previous self-assessments and the results of GovAssure. I am genuinely trying to remember: I think we expected some difference, but probably not the scale of the difference that we saw, and we did not expect the difference between self-assessments against CAF and the independent assessments to be so great.

The short answer to your question is quite a long answer, and it goes back to something that kind of rolls right throughout the Report: despite recognising this in 2010 and starting to significantly invest money in 2016, in retrospect, we probably did not ramp up the Government response to cyber security, from assurance through to response, as quickly as we should have. Why? I think because we were not as alive to the threat as we should have been—we have already said that it evolved rapidly and that we should have seen it—and probably because we had not had the incidents ourselves or among our allies that really brought it to life for us in the way that we have over the last five years. That is not a good answer, but it is probably the true answer.

Q46 **Sarah Olney:** Do you think it was perhaps a mixture of naivety and lack of experience? The British Library example that you used was very compelling, but you were not aware of the threats until something like that happened. Was that perhaps due to a lack of intelligence coming from the people monitoring these threats more broadly?

Vincent Devine: Others will comment, but I think there is something about prioritisation. Government Departments have faced a lot of demands over the last 10 years. Probably we did not prioritise cyber security sufficiently, and it was not brought alive to us by serious incidents in the way that it has been in recent years. But others might want to say something, as that is very much a personal view.

Cat Little: It is really difficult to go back in time to our predecessors. I suppose, like with all good risk management, you manage risks as best you can until they become an issue, and when they become an issue and they are live—they are real—you step up your response. I think there is definitely something about how we have always known about the risks, but it was not until it became a real, live issue that the scale of what we were dealing with became clear and it needed a different sort of response.

Sarah Olney: Thank you.

Chair: We like candid answers in this Committee, so congratulations, both of you. We will go to my ever-patient deputy, Clive Betts.

Q47 **Mr Betts:** For a few more candid answers, maybe. GovAssure is a step

forward, as you have explained to us, away from the self-assessment, except that you have left behind out there, in the self-assessment process, with departmental responsibility, the worst systems—the legacy systems. Those are the ones where the risk is greatest, the threat is greatest and the security is least, but you are not dealing with them. Why?

Cat Little: Perhaps I can invite Joanna to set out what we are doing about legacy IT.

Joanna Davinson: As you say, there is a significant amount of legacy IT in the public sector estate. We know that because we have recently done a lot of research on that and produced our state of digital government report, which shows that about 28% of our IT estate, across the whole of the public sector, is classed as legacy. It is also true that historically we did not have a lot of information in the centre about our legacy technology and the risk that we carried.

About two years ago, we therefore introduced the legacy IT risk framework, which we have been working with Departments to implement, and which is really focused on central Government Departments and major agencies that have big IT estates. It will look at their legacy systems and classify them, to understand which of them—from the perspective of the likelihood and the impact of an issue happening—are red-rated as the riskiest of the systems. That is not just about cyber. It is also about their operational risk, just from technical failure, or their utility in terms of the ability to meet departmental objectives and actually deliver the service that Departments need.

What we know from the work that we have done so far is that, as of January—these numbers are actually an update on the ones in the NAO Report—we had assessed 319 legacy IT assets, and almost a quarter of those were red-rated. As with GovAssure, as we have gone through this process we have understood that we have quite a significant challenge out there in Departments.

We are continuing to look at that framework. We are now looking at work to expand that and to make it more consistent across all of Government, and also to align it better with GovAssure, so that we have a complete picture across both the legacy and the non-legacy estate.

Q48 **Mr Betts:** That poses one or two more questions. Have those 319 been assessed by you or by the Departments themselves?

Joanna Davinson: No, it is a joint effort between us and Departments. It is a set of questions that they answer, and we review that. We do some assurance on it, but you are right that it is a self-assessment, rather than a fully assured one in the way that GovAssure is.

Mr Betts: Right, so it is a halfway house approach.

Joanna Davinson: At the moment, yes.

Q49 **Mr Betts:** I have two further questions. Those 319 systems have been

assessed, but how many are there to be assessed?

Joanna Davinson: The really honest answer is that we do not know. I say that because when we did our state of digital government review, about 15% of the organisations that we spoke to did not know what their legacy IT was; they could not give us a view of it. There is a challenge there: the organisations that are responsible for legacy do not necessarily know themselves, in all cases, what the risks are in their estates. That was the whole purpose of creating the risk assessment framework: to shine a light and start to get information that enables us to challenge Departments to do the work to understand that.

Mr Betts: Not knowing the risk is one thing, but not knowing what the legacy systems are is another.

Joanna Davinson: I think they know their systems, but whether they have been assessed in respect of the level of risk that is carried from the sector—whether they qualify as legacy and what the risk is—is the thing that they do not necessarily understand.

Mr Betts: Do we know how many systems there are—whatever you call them—that have not yet been assessed?

Joanna Davinson: We do not have that data.

Mr Betts: Do Departments have that data?

Joanna Davinson: There is a real difference in the level of maturity in Departments in their understanding of their legacy assets. There is also quite a difference in the number that each organisation has. The research we did showed that in Departments the number classified as legacy varies between about 10% and 60% of the estate. Some understand their estates very well and have relatively low levels of legacy, whereas others have much higher quantities.

Mr Betts: We come back to the question: how many systems are there? That is back to the question of how many still need to be assessed. Surely Departments know how many systems there are.

Joanna Davinson: Not always. It depends. That information is not necessarily collated centrally in a way that is easy to access.

Cat Little: Just to expand on that, as we have discussed in this group several times, we have a large number of arm's length and public bodies, so when we say "departmental families", Departments have a very good grip on their external service-facing systems, on what is close to them, but what are less gripped is arm's length bodies, where we are reliant on—two or three layers down the departmental chain—what their understanding is and how they have assessed their IT.

As I think Joanna was about to go on to say, this is one of the challenges of sharing data in Government: we are constantly relying on layers of

information being fed back to us centrally so that we can take an overall view. I completely share your concerns: that gap is not acceptable.

Q50 **Mr Betts:** Should Departments not just be required to draw up a list, for a central register, of what systems there are? Arm's length bodies and others are ultimately accountable to Departments, so surely those Departments ought to know, if they are asked the question.

Joanna Davinson: Each Department will have a view on that, and they are not necessarily consistent: they may not hold the data in the same formats and will not necessarily have the same asset management systems to enable them to extract reports quickly to give us the information in a format that we can process. We need to fix that—I absolutely agree that we need to fix that. One of the core things that we are doing through, for example, our Secure by Design approach is to make sure that we have the right kind of information—that metadata—on what is contained within the estate, so that we can fix forward on that.

Q51 **Mr Betts:** What is your timetable for doing that? Do you have deadlines for the Department to respond to that quite important question?

Joanna Davinson: It is part of an ongoing process in how we work with Departments to understand what they have in their IT estates.

Mr Betts: This is quite a critical issue—the threat of a potential cyber attack that could be launched against a legacy system—and, to begin with, we do not yet know what the systems are. Should there not at least be a deadline for Departments to say, "This is the list of systems we have"? Then you can look at how long it will take to work through and do an assurance process on them.

Joanna Davinson: We continue to expand the number of systems that we are looking at, working with Departments. We are improving that information as we go, but it is not as simple as saying, "What is the list?"

Q52 **Mr Betts:** Why? We are laypeople; we are just asking questions about what seems to be an obvious issue. If we need to know what the problems are, we should begin by asking, "What are the systems we might have problems with?"

Joanna Davinson: We have asked that question of Departments, and we have had responses through our legacy risk framework, so we have that understanding. We continue to expand that to other organisations, but it is not a resource-free exercise.

Q53 **Mr Betts:** We are getting back to the issue. Do you not have the resources to enable you to push Departments to give you this information, or is it that Departments do not have the resources to assess what systems they have?

Joanna Davinson: It is a bit of both. We at the centre are expanding our capacity to work with Departments to understand better what they have and what their risks are; Departments are putting more effort into

understanding their estates and putting the systems in place to enable them to better understand their estates.

It is a little like where we got to with GovAssure. The balance is about how much resource we put into measuring things to understand risk at the individual asset level, versus whether we have enough information to understand that we have a problem, and whether we now start to triage what we do about it. We are asking how, from the centre, we can put the right mechanisms in place now so that we understand the issue that is out there and start to remediate it. Ultimately, what we need to do is remediate this problem—fix it. It is less about more and more measurement, and it is more about how we get the right mechanisms to put accountability in place to fix it.

Q54 **Mr Betts:** But you need to know what systems you have to fix before you start fixing them.

Joanna Davinson: If you had asked me that question two years ago, I would not have been able to tell you anything. We are actually now moving forward, in terms of understanding enough about the risk to start putting mechanisms in place to sort it out.

Q55 **Mr Betts:** You said that it was not just that you did not have enough resources to do everything, but that Departments do not have the resources either. Departments should have fully funded plans to fix their legacy IT systems, should they not?

Joanna Davinson: One of the things about legacy is that its visibility is not always in the Department. Often it is IT that has been developed and is being maintained and operated by third parties, so there is a very complex information chain from which to extract information about the estate. Systems are not necessarily single things; they are complex sets of components. There might be one part of the system that is a problem and other parts that are not. Trying to work through this and understand all that complexity, when the data is not in the Department or agency but in a third party, is part of the challenge.

Q56 **Mr Betts:** Is there not a worry that you have some very high-risk systems that have not been properly assessed, or that you do not even know are there? Data sharing has been encouraged in Government, but if you are data sharing from a system that has low protection, surely you can pass problems across to other parts of the IT world in Government.

Joanna Davinson: I think that that is probably less of a risk, because a lot of these legacy systems tend to be isolated. They are not networked in the way you might think of a modern system being; they tend to be sitting in towers in third-party data centres.

I would also say that not all legacy is necessarily a problem. Of the legacy that we have assessed, we have assessed getting on for a quarter of it as red-rated, so there is a large proportion of legacy that is not flashing red as a technical, resilience or cyber risk. It is not good, because it is

expensive to operate and is not necessarily delivering the quality of service that we need, but it is not an issue at this point.

Q57 **Mr Betts:** Let me come back to funding issues. If no one knows what the problems out there are or what systems might be problematic, how can Departments put in proper bids to the spending review? When they do, how can we be certain that they will spend the money on the issues that are challenging or a problem? Apparently, in the past, some money allocated for cyber-related issues has been spent on other things that suddenly become a priority for Departments.

Cat Little: What this part of our discussion really brings to light is that the Government, in a period of scarce resources, have to prioritise decisions based on risks and how much assurance is desired. It is for the Government to set their risk appetite, and to use that risk appetite and information to therefore allocate resources accordingly.

To be clear, it is not as if we have 100% lack of sight. As Joanna said, we have made huge progress in understanding the most significant issues that we have. Although it is not every single system, it is the vast majority. In the spending review, what we are doing differently from last time is running a zero-based review for technology, which is currently under way, to understand how every single £1 of spending is undertaken across the system. That is the first time that we have done a zero-based review on technology and how the money is spent, which will help us to answer some of the questions about where the money is going and what it is buying from a systems perspective.

The second thing is that we are using both GovAssure and our technical expertise on legacy IT to set out for Ministers the choices about risk and how much risk they want to buy out. That is the fundamental question. If you have x billion pounds available to fund people, resources and skills, to remediate legacy IT and to invest in new technology, how you use your allocative resource has to be risk-based and outcomes-based. The whole point of the spending review process is to bring outcomes and risks together so that Ministers can make a funding allocation choice. Experts in DSIT and in our cyber teams are embedded into the Treasury process. The Treasury is very reliant on our brilliant central experts to advise Ministers to make those choices, and that work is very live.

You said earlier that surely there are fully funded plans out there. That is not the case. You always have to make choices about how much funding you put in to buy new things, to manage the legacy systems and the risks you have and to build up skills. I do not that think I have ever seen a situation in which we have fully funded all those things to 100% possibility. It is an allocative choice.

Q58 **Chair:** You talk about priorities and the level of risk you are prepared to accept. The Government have to come up with a sum of money to remediate these legacy systems, but if you do not know what precisely is out there, how do you know where to make those priorities and risks?

We are coming to the year end for Departments. Would it not be

reasonable to ask all Departments and ALBs, at two months from their year end, to give you a list of where the legacy systems are? The legacy systems are not just, as we discussed, an entry point for cyber. As the British Library makes very clear, if a legacy system that is not supported is hacked, it is much more difficult to remediate afterwards, so this is a real priority, is it not?

Cat Little: It is a huge priority, and I do not want the Committee to think in any way that this is not one of our biggest priorities in Government. It has to be, because of all the opportunities and risks that we have discussed in several Committees now. It is a huge priority.

There is a choice whether the centre of Government, by which I mean DSIT and the Cabinet Office, should spend all our time trying to get 100% complete data, or whether we should get the balance on doing as much as we can and then relying on Departments. What we are choosing to do is say that we will get 80% or 90% there, but we really need Departments to own the risk, to tell us where there are gaps and to make sure that accounting officers have the support to set out the risks, to bid into the SR process and to come to us for help. That is a partnership. It has always been thus, and to some extent it will always be that way. It is my absolute hope that in the SR we will be able to do a much better job than we have done previously of elucidating those risks, having a proper conversation about prioritisation and buying out as much risk as we can afford.

Q59 **Chair:** We will move on, but I suspect that the laggards will always be laggards unless they are in some way pushed to do something about it.

Cat Little: I would not want you to think there is not a lot of pushing. There is a huge amount of pushing from Joanna and her teams, and from the Cabinet Office and the Treasury.

Q60 **Mr Charters:** Just to reiterate what we have heard, it is really disappointing that you do not seem to have a grip on where the legacy systems are across the arm's length bodies. These are not inconsequential organisations; they are bodies like the National Crime Agency, the CQC, the CPS and the Nuclear Decommissioning Authority. Would you set out to the Committee, perhaps at the Chair's advice, where there are gaps and who has not responded, and your view on whether there should be a better process for requisitioning this information?

Joanna Davinson: We can do that. If it is reassuring, I can say that some of the 29 organisations we have worked with to date on the legacy risk framework are arm's length bodies. We have targeted the ones that have the bigger IT estates. We are conscious that we need to prioritise in that direction, but we can write with more information.

Cat Little: I just want to clarify that it is not that we have not worked with all arm's length bodies; it is just that the complex supply chain arrangements and the fact that there are lots of different layers of accountability mean that it is harder to get right down into the depth of understanding of systems. I was just explaining the challenges. We definitely have lots of public bodies that we have worked with.

Q61 **Lauren Edwards:** My question follows on from that last discussion. Obviously, the legacy systems are quite an important gap. How are you managing supply chain risk across Whitehall? That would seem to be another vulnerability.

Vincent Devine: Going back to Mr Charters' question about Synnovis, that is a classic example of a risk that is in an ALB, in a supply chain. Those are two of our most difficult areas to manage. We are doing a great deal to try to improve our management of security in the supply chain, because we are aware that it is a vulnerability at the moment.

Bella Powell: You are absolutely right that supply chain security is a really complex area for us, particularly given the incidents we have seen impacting supply chains, and the direct impact that that has on public services.

We have taken a number of actions to date to improve how we manage security, particularly for our critical suppliers. That includes defining modular security schedules that can be included in contracts for Government organisations, to ensure that they are asking for the right things of their suppliers from a security perspective. We also work very closely with strategic suppliers to Government to ensure that we have a very open and partnering relationship with them—ensuring that, in the event of an incident, information is free-flowing and the relationship is positive, but that we are also holding them to the highest standards from an assurance perspective.

We can absolutely do more in that space, though. One of the things we will be focusing on in the next financial year, as part of taking a much more interventionist approach to cyber resilience, is ensuring that we have stronger supply chain assurance in place. We will also ensure that we are working in a much more targeted way with strategic suppliers to hold them to account and agree really clear objectives for how they can help Government to improve cyber-resilience levels, use their understanding of delivery across Government to identify critical gaps and, fundamentally, help us to transform.

The strategic partnership agreement with Microsoft is a great example of how that process will work. As part of that, we have defined very clear security objectives that we will be working on in partnership with Microsoft. The intent is that we use that as a forcing factor to improve resilience across Government organisations and use the collective expertise of that organisation to help us to drive up standards. Joanna might want to say something on the broader strategic partner relationships, from a security perspective.

Joanna Davinson: The Microsoft deal is a model that we want to try to roll out across our major suppliers. Thinking about the supply chain, as we roll out our secure-by-design approach, one of the key principles in that framework is ensuring that the technology partners we use have the right controls in place.

Q62 **Lauren Edwards:** That is really comforting. Is it the case, then, that all tendering or procurement requires a robust cyber defence from the supply chain partner?

Bella Powell: Yes. In terms of the security schedules we have set out, we have different schedules that are relevant to different types of contract. Departments are advised to use those as part of the contracting process to ensure that they have appropriate standards in place. Again, there is more that we can do in that space. We can ensure that they are applied more appropriately. We can give more support to Departments in the application, but that is absolutely the intent. There is a clear set of requirements in place for future contracts.

It is worth noting that those modular security schedules are not in place for pre-existing contracts. It is very much a process of fixing forward, and we also have a responsibility to help Departments manage the risk with their existing suppliers. But that has been a really positive step for us.

Q63 **Lauren Edwards:** Going back to the NAO Report, paragraph 2.12 talks about the Government Security Group and Departments lacking the time and resources to improve cyber-resilience outcomes following the conclusion of the first year of GovAssure, in July last year. It mentions that in November last year, "GSG had not commissioned progress updates from departments but planned to do so once departments had more opportunity to implement" their targeted improvement plans. Bella, what is your assessment that these Departments can and will implement their GovAssure improvement plans in the light of this?

Bella Powell: Let me clarify the process. We go through the assessment process for individual systems and then collectively agree a targeted improvement plan per system with each Department. At the time the Report was written, we had not commissioned updates, because we fully expect it to take six to 12 months, at a minimum, for Departments to be able to achieve a realistic change, particularly when we are talking about fundamental controls such as asset management and risk management.

I would absolutely say that the use of targeted improvement plans is a really important step forward to us. We have asked Departments to really focus on those targeted improvement plans as part of their engagement on the spending review to ensure that they are prioritising response to the vulnerabilities that have been identified in those reports, and that they are ensuring that that is a core part of their bids. Obviously, in many instances, response to those targeted improvement plans will be dependent on decisions made in the spending review, but we have made it very clear to Departments that that is the expectation, and that delivery of those plans is absolutely critical as part of achieving the outcomes that we set out for them.

We are also taking steps to strengthen the accountability frameworks that we have in place for Government organisations. The use of GovAssure results at the most senior levels of Government is something that we think is critical to ensure that Departments are prioritising investment in

targeted improvement plans and improving response. We now report on GovAssure results to the civil service boards as well as heads of Department, and we are also intending to strengthen that framework further. "A blueprint for modern digital government" sets out a commitment to changing our relationship with technology risk in the round, and to ensuring that there is clear accountability at perm sec level and downwards to understand and then respond to technology risks, including cyber risks. That is something that we will also be working on.

Q64 **Lauren Edwards:** Would you say you are confident that they will be implemented at this admittedly early stage?

Bella Powell: I am confident that they will be prioritised, but implementation will be subject to available funding and decisions in the spending review.

Q65 **Lauren Edwards:** So they are resource-contingent—thank you; that is helpful. One of the gaps for me was CBEST testing, which I know a bit about from my time at the Bank of England doing cyber-penetration testing with some of the very large financial companies that operate in the UK. It is a gold-standard system that allows companies to invite teams to come and test their cyber defences, and to be able to have that real-life example and then learn from any access that is given and anything that comes off the back of that.

It is not mentioned in the NAO Report, but I understand that the Government, in the light of that, created a similar system called GBEST back in 2018, which has been running annually since then. I really welcome that external testing of Whitehall's defences. That is really important and supplements a lot of the important work that we have been discussing. Can you tell us a bit more about that process? Admittedly, you cannot go into too much detail, but what can you tell us about that GBEST process? How does it interact with some of the other things that we have been discussing?

Bella Powell: I am happy to. The Government security red team sits as part of my team in the Cyber Directorate in the Cabinet Office. We conduct a rolling exercise of GBEST/GCASE, which is a slimmed-down version of a similar exercise from a cyber perspective, and also physical security red-teaming exercises on Government Departments. That is a core part of our assurance process.

The work that we do there involves essentially speaking to individual Departments. We have a rolling programme in which we focus on Departments that either have critical infrastructure or have not been tested for some time and have had particular challenges. We go through the process with them of scoping a red-teaming exercise, conducting it, assessing the outcomes and agreeing the actions that they need to take as a result.

We do two things with that. One is that we ensure that the Department is using that information as powerfully as possible. We find that it is incredibly helpful to use some real-life examples of how systems can be

compromised with the board of a Department, so that they really feel the pain of quite how vulnerable a particular organisation or system is. We also use that for tabletop exercising, which is a powerful mechanism to help boards understand scale of threat and vulnerability.

We also use that data as an input to our broader assurance process—so we look at all the GBEST and GCASE activities that we have conducted across Government and identify systemic vulnerabilities or issues with controls, which we also look at in comparison with our GovAssure results. That is an important part of our cross-Government assurance approach.

We also make sure that we get the best bang for buck by using the outcome of those individual assessments with Departments to help them to understand the scale of the problem. They are great for business cases as well; it is really great if you can say, "We have an exercise that proves that we have these vulnerabilities, and this is what would happen if an incident occurred."

Q66 **Lauren Edwards:** That is helpful. It sounds like the outcomes of those tests are then shared throughout Whitehall, so that lessons can be learned. Is that the case?

Bella Powell: The outcomes of the individual tests are not shared; they tend to stay with the individual Department. They often include very sensitive information about individual systems and components of the organisation. That stays with the organisation, unless it agrees with us that we can use it as part of a case study. But the anonymised results and the systemic issues and vulnerabilities that we identify are then shared as part of our wider assurance process with Government Departments.

Q67 **Chris Kane:** Can I ask about the move to make the public sector resilient by 2030? I think the Committee and the NAO Report note that the Government Security Group has the implementation plan for what it is going to do, but there is no strategy implementation plan that sets out what everybody else is going to do, who needs to do what, and who is going to do it. How can everyone become resilient by 2030 if that full plan is not in place?

Vincent Devine: Do you want to take that, Bella?

Bella Powell: I am happy to. As I think I have mentioned previously, the 2030 target is intentionally ambitious and will be enormously challenging to achieve—we should be clear about that—but it also sets a very clear target for Government Departments, their arm's length bodies and the wider public sector to achieve. It is important to recognise that in the Government cyber security strategy, we set a clear expectation for lead Government Departments, in particular, to understand and tackle the scale of risk for their core Department, their arm's length bodies and the parts of the public sector within their purview. The responsibility for that broader public sector lies with lead Government Departments.

We have seen a varying response to the strategy to date, but it is fair to say that we have seen some positive steps taken. For example, the

Department of Health and Social Care has set out a very clear cyber security strategy for health and social care that links directly to the Government's cyber security strategy. The Department has strengthened its assurance processes and put in place clear policies for broader public sector health and social care organisations to respond to. It has invested in common infrastructure around common services where appropriate, and it has seen commensurate positive steps in the overarching resilience of the health and social care sector.

The approach the Department has taken is one that we are very much looking at from the centre when we think about how we can drive change more effectively and achieve a step change in our approach. We would absolutely categorise the approach that it has taken as much more interventionist and much more focusing on what can be delivered from a central organisation in order to enact change. We would see that model as a particular case study of really positive change being made.

But it is right to say that the public sector is large and complex and that, if we want to achieve the 2030 target, we are going to need to take a fundamentally different approach. One of the things that we are looking at particularly for the next financial year—and as recognised by the NAO—is how we can change the systems of delivery across Government from a cyber perspective: how we can define a new target operating model that allows us to be much more interventionist from the centre, where that is appropriate. We are in the process of designing that model at the moment, and we are piloting some services this financial year to help us to deliver an early benefit and derisk that model.

We see particular value in strengthening accountability, and making sure that lead Government Departments and organisations across Government have a clear set of requirements for them to work to and for us to measure them against. We are also looking at the delivery of services at scale, and at examples where we can deliver a service once and well from the centre that allows us to make a material difference to the resilience of public sector organisations in the round.

An example that we are piloting this financial year is cross-Government vulnerability scanning, which is being delivered by colleagues in the Government Digital Service. That is a great example of a digital service that helps us to better understand the internet-facing vulnerabilities of a really broad range of organisations, not only giving us a better understanding of the scale of risk and the attack surface across Government but allowing us to help those organisations to respond better. We think that that model will be powerful in helping us drive broader public sector change, but it will be challenging to deliver.

Q68 **Chris Kane:** We are talking about the public sector and we are a United Kingdom, which has devolved nations, but the cyber threat does not recognise our internal borders. How are you working across the devolved nations to get this 2030 target? Are they included? Is there good co-operation and cross-working?

Bella Powell: We work really closely with the devolved Administrations. We have delivered a number of initiatives centrally that they have voluntarily adopted. GovAssure is a great example, where we have really strong uptake from the devolved Administrations. We see a real opportunity there for strong collaboration and for setting out a set of central initiatives—doing some heavy lifting—that can then be really powerful. So it has been a positive process so far.

Q69 **Chris Kane:** I suppose you can always get learning from the devolved nations, just as they can learn from the UK Government. As a Scottish MP, I am used to robust and ambitious targets being put in place and then not met. On the 2030 target, there is good evidence of what happens when Government Departments put in place targets that are so ambitious that they are never going to be met. Are you learning those lessons, about being realistic and robust? On the strategy implementation plan, are you being realistic, robust and learning from other parts of the United Kingdom, where an ambition sometimes just means that a reset is on the cards in two or three years, so there is a never-ending cycle of resets rather than delivery?

Vincent Devine: That goes back to something captured in your earlier question. To be clear, we fully agree with the Report's recommendation: to meet our 2030 target, we need a cross-Government implementation plan that will capture both what Bella's team propose to do and what Departments have committed to do. We will develop that plan once we see the outcome of the spending review.

I think the Report also emphasised that we need to put in place a much stronger monitoring and evaluation framework, and Bella's team are already working on that. We have absolutely learned the lessons of setting targets and allowing people to move towards them at their pace without understanding what they are doing. We will have a cross-Government implementation plan within six months, and a robust monitoring and evaluation framework to support that, so we will hopefully not fall into the trap that you talked about.

Q70 **Mr Betts:** How can you be sure that you are focusing on the right issues when you do not have full information about what is actually going on out there, in Departments and arm's length bodies?

Bella Powell: Let me go back to the engagement that we have with Departments. We work very closely with Departments to understand not only current resilience levels, but the challenges that they face on a day-to-day basis. We include them in governance for the delivery of the Government cyber security strategy, and work closely with their teams.

However, it is important to note that the work that we have focused on centrally—such as GovAssure and the Government Cyber Co-ordination Centre—has been to help us better measure and understand the scale of risks that we see across Government organisations, the challenges at departmental level, and how we can tackle them. Our focus on those central initiatives has been at the expense of defining, rolling out and co-

ordinating a cross-Government implementation plan that directly challenges Departments to deliver on their outcomes. But we absolutely have collaborated extremely closely with Departments and have put in place measures to allow us to understand the types of challenges that they are dealing with.

Q71 **Mr Betts:** When will the cross-Government implementation plan be in place?

Bella Powell: The NAO has included that as part of its recommendations, which we have absolutely accepted. Work is already under way to define that cross-Government implementation plan. I will double-check and write back to you, but I think we have committed to publishing that in summer 2025.

Cat Little: It needs to go alongside the spending review, for obvious reasons. We need to set out what we would ideally do so that Government can take choices. We can then set out a fully funded plan that will work.

Q72 **Mr Betts:** How far will that extend to the wider government—to local authorities and parts of the health service, given that hospital trusts are separate bodies with their own ways of developing and buying IT systems?

Bella Powell: The Government cyber security strategy covers Government and the public sector, as do those targets. The implementation plan will also be scoped to do exactly that. There will be a difference between how we set out requirements for central Government organisations and how we support lead Government Departments in the implementation of those targets within their sectors, but the scope will be the entirety of the public sector.

Mr Betts: We might come on to another question about the powers you might have over wider government, but that is a helpful initial answer.

Q73 **Mr Charters:** I was going to ask what changes at the centre of Government would help Departments with your leadership, but we have had some clear answers. Going back to arm's length bodies, how are you supporting their cyber resilience position from your position at the centre?

Cat Little: At a very high level, everything we are doing for central Government applies to our arm's length bodies. It is a bit of a cascade because we issue direction at top level. The departmental permanent secretary and senior leadership team are responsible for cascading that through the arm's length bodies that they sponsor and are responsible for. But everything we do should equally apply to arm's length bodies and to public bodies at large.

Q74 **Mr Charters:** Is that cascade effective?

Cat Little: It is going to be inconsistent by the nature of the different issues and risks we are dealing with. Part of why we have GovAssure and the work we are doing on legacy IT is to assure us on how consistently all parts of Government are responding to what we have asked them to do.

As I said earlier, there is always a balance between how much checking and policing you do and how much you have to place accountability into departmental hands. Everyone wants the centre to do more. I am a great believer that you have to have empowered, accountable people close to the frontline who can take proportionate decisions.

Q75 **Chair:** This is probably a question for you, Mr Devine. Are there any countries that do cyber prevention better than us from which we can learn lessons?

Vincent Devine: I think there probably are. I will ask Bella to come in because our team has been out speaking to some of them. It is worth noting—not in defence of where we are, but as a matter of fact—that most of our partners are facing the same challenges. They are all playing catch-up with threat; they are all playing catch-up with a risk that is beyond their appetite. I think the Report calls out the Australians—I am happy to do that on the record, in any case—who have put in place a number of interventions.

Q76 **Chair:** Yes, it does, in paragraph 2.23.

Vincent Devine: Some countries that face a particularly challenging cyber risk, for example some of our Baltic partners—the Estonians, for example—have learned a lot over recent years that they have put into their systems.

We speak to our Ukrainian counterparts—we are very lucky that our Ukrainian counterpart has come to our conference for the last two years—and they are in a particularly challenging environment. One of the advantages of that, and there are not many, is that they learn very quickly. They are evolving very quickly. There are a number of partners that we can learn from. Australia is the model. We see great similarities there and we want to learn the most from it. Bella, do you want to expand on that?

Bella Powell: I completely agree with that characterisation. While there are a number of international Governments from which we can learn an enormous amount, particularly those who are much more focused on digital adoption and have achieved a much greater rate of digital service adoption and public sector digitisation, our Five Eyes partners in particular are demonstrating an effective way of dealing with cyber resilience challenges.

Vincent has already mentioned Australia. Similarly, Canada has a helpful approach that we are drawing on as part of the work we are doing to reset our model for Government cyber resilience and define our new target operating model. The US and New Zealand have some helpful steps that we are drawing from.

We see two things that are particularly powerful, particularly for Canada and Australia. The first is a real focus on transparency and clear assurance of resilience levels across Government organisations. Our Australian counterparts publish on a regular basis the resilience levels that they see

across Government organisations. They found that that has been helpful in driving accountability across Government organisations.

Canada, Australia and other countries take a much more interventionist approach. In particular, they have taken on responsibility for the delivery of cyber services at scale, where it makes sense to do so from the centre. That has been enormously powerful.

Our colleagues in Canada in particular have taken really helpful steps in thinking about where they can deliver central capabilities and central services. That has an enormously powerful effect in helping them to understand the scale of risk that they see across Government, and it also helps them to respond more effectively to threats when they arise. We are absolutely looking to them as models of approach, and we are learning lessons from them as part of our more interventionist approach to cyber-resilience.

Q77 **Chair:** Let me take part of that answer. In this Committee, we are great believers in openness and transparency. Could we not follow the Australian model and publish a lot more on Departments' resilience so that we can see where the best exemplars are?

Bella Powell: First, the "State of digital government review" has recently been released by colleagues in DSIT, and I think it is a fantastic step forward in creating transparency around the scale of challenges our digital estate, particularly in legacy and in terms of the GovAssure results that we are seeing. There is absolutely more that we could do in that space. It is a challenging balance between ensuring that we are creating that transparency and also ensuring that we are not creating avenues for malicious actors to take further action against Government, but absolutely, we can explore that further.

Cat Little: Ultimately, that is a choice for the Government to make, given the very serious risks that you have to balance those choices against, but I think we would generally agree with you that transparency is a very good thing.

Q78 **Chair**: Sorry, these questions are a bit random—I am just sweeping up, really. Paragraph 2.18 of the NAO Report states: "the Cyber Government Security Centre (GSeC), which GSG funds, has needed to initiate contact with departments to raise awareness of its free cyber security consultancy services. This is because there is not a centrally coordinated way of communicating GSeC's offer to departments to ensure that they seek it out when they need it. This could limit departments' take-up of those services." I do not know anything about it, but it sounds as though that is an amazing offer. Could you not do more to promulgate that?

Bella Powell: We absolutely can. We work really closely with the Cyber GSeC, which is hosted in HMRC. We work very closely with it as an organisation to ensure that we are making the best use of the resources that it has available and also that we are matching it to Departments that have particular challenges.

One of the services that we have been piloting this financial year as part of our more interventionist approach is something called deployed cyber enablement teams. That is something that we have learned about from our Five Eyes partners. Essentially, what that is doing is deploying technical teams into Departments to tackle vulnerabilities where they may not have the skills or expertise to deliver on them or they just do not have the resources.

The Cyber GSeC will help us to deliver that during the next financial year. One thing we need to do much more effectively is provide a really clear strategy for how we can best use those resources, but absolutely, that is something that we are planning on.

Q79 **Chair:** I have a couple of technical questions. I am not a technical expert, I hasten to add, before I ask these questions, but I need to ask them because we have been given evidence about them.

The first one is from a Nigel D Cook. He says, referring to the Government's exclusively using Microsoft software: "The issue with such a "mono-culture"—this goes against what I would have thought, wearing my procurement hat—"is that a virus infection or software configuration issue…at the server/s quickly cascades across the "mono-culture" with resulting failure of the majority…user devices while individual desktops/laptops are re-configured and manually rebooted...This is what happened with the Crowdstrike" episode last year.

As a procurement person, one would want to get the best value for money, and the best value for money probably inevitably means Microsoft, but obviously there is the opposite case out there to deal with this sort of monocultural situation.

Cat Little: I have a couple of things to say; I am sure others will want to add to this from a technical point of view. I am not a technical expert either. What we are trying to do is weigh up the benefits of having large suppliers at scale, which include interoperability as well as value for money.

As someone from a Department not on a Microsoft platform, I can tell you that it is incredibly frustrating to have to constantly say, "I'm very sorry: I can't send you that document to work on because my system doesn't talk to your system." So we need to think about how we create the best environment for our staff to operate in and drive value for money. That has to be weighed up against the obvious risks that come with these large primes delivering quite a lot of our services.

Quite a lot of where we are is historical, not by design, so what we are trying to do is to maximise the economy of scale, maximise value for money and ensure that we are working with our supply chain to manage risk effectively and to increase interoperability at the same time. That is not straightforward.

Joanna Davinson: Just to add to that, CrowdStrike showed that this is not just about cyber. CrowdStrike was not a cyber incident; it was a

technical failure, and one of the things that it exposed was that actually we did not have a national focus for just technical resilience issues, rather than cyber issues.

It is very clear that if it is a cyber issue, it goes to the NCSC; that was less clear for a technical resilience issue. We fixed CrowdStrike, and one of the outcomes of that is that we have now identified the accountabilities within Government for dealing with those sorts of technical failures in the future. That sits in DSIT—in the Government Digital Service.

Q80 **Chair:** That is very important. We have also had some evidence from an organisation called the Open Cloud Coalition. They talk about the dominant cloud platforms. They say 60% of the UK Government and public IT systems operate on cloud services, and 80% of these rely on just two providers. They go on to say that if one of these providers accounts for 50% of UK Government services in a single region, a failure or outage could take down 30% of the public sector, highlighting the critical need for diversification and resilience. They particularly talk about the Cabinet Office's 2017 shift from cloud first to public cloud first. This comes back to what you were saying, Cat, about the dominance of certain players, but also the need to communicate between the different systems. How are you going to deal with those two competing issues?

Cat Little: The first thing to say is that this is not just a Government challenge. There are a small number of dominating cloud services out there; there is not a huge competitive market, with lots of different providers. We are not market shaping in our scale, so that is what the market has to offer us. Secondly, quite a lot of our legacy systems are operating off a very small number of cloud providers, and until you fix some of the legacy issues, it is very difficult to move off some of the cloud services that are there. But Joanna is the expert.

Joanna Davinson: I think Cat said that it is a market that has a small number of suppliers. We are quite concentrated on those suppliers, as is everybody. We are looking at how we ensure, on that issue around regional risk, that we work with our suppliers to ensure that we do not have too much of a concentration within a particular regional area. We are going to have to keep that constantly under review.

The positive thing, though, about cloud services and, actually, all the subscription-based services, which is where we are moving in terms of all our new digital development, is that it does build in continuous improvement, continuous maintenance; it reduces the risk of developing new legacy issues. These things are all a balance, but moving more into subscription-based services like cloud actually helps us to manage the legacy risk. From that perspective, it is our policy to move further—

Q81 **Chair:** I want to close the session, but you have raised a very important issue there. We have talked before about the move to subscription-based services—the need, when you are procuring, to procure something that is going to be updated constantly. Your Department now has responsibility for this through the CDDO.

We have discussed this before, but I would like to ask you again: how are you going to embed this culture into other Departments, particularly the Cabinet Office, that do commercial procurement, to make sure that this is always considered—for every single large contract that they procure?

Joanna Davinson: It is certainly part of our Secure by Design framework, in terms of ensuring that it is always considered in building new capabilities, but we are also, in the centre, creating more capability around modern or good technology management.

We have developed a community for chief technology officers across Government, and we are moving that Chief Technology Officer Council to be a design authority for Government. The chief technology officers of major Departments will set and assure the standard to ensure everybody implements against that need. That will ensure there is consideration of the need to continuously improve and resource to do that. Funding products and teams, not projects, is the shorthand for it. It is dependent on Departments making their allocative decisions around putting the right amount of money into protecting systems. The history that we have seen is that they build the thing but then don't maintain it.

Chair: Thank you very much. Last but by no means least, I call Lauren Edwards.

Q82 **Lauren Edwards:** Thank you very much, Chair. A question has come to me while we have been discussing this. There is obviously quite a big debate about work from home and the civil service. How do you ensure that when people are working from home, the cyber defences remain robust? How do you avoid having thousands of civil servants across the country sitting on default wi-fi router passwords?

Bella Powell: That is a really excellent question, and we particularly grappled with it as part of the response to covid. When we are fundamentally changing our mode of operations, how do we make sure we maintain appropriate defences and appropriate levels of resilience?

The first thing to note is that our approach has to be layered. The resilience requirements that we set out, as per the NCSC cyber assessment framework, do not rely on one control to maintain cyber resilience for a given organisation, an individual or the laptop they are using in any given scenarios. We have a series of controls that together give us an appropriate level of resilience. We also have to ensure that, when we are changing working practices, those controls change.

One of our most important defences is giving individuals the right guidance and support to make the right choices and ensure that they are doing their part in maintaining resilience levels. One of the things we have had to do as part of that fundamental shift in working is ensuring we are also giving the right guidance to individuals about how they can operate securely. We do that from a central perspective and support Departments in getting the right guidance to individuals. Departments really focus on that, and have done that as part of the fundamental shift in working.

Q83 **Lauren Edwards:** Thank you. Would you say that every civil servant has been given guidance about how to manage cyber risks when they are working from home?

Bella Powell: One of the things we do centrally is ensure there is good guidance available to Government organisations. Essentially, it is the responsibility of the individual Department to ensure that gets to every individual, but we provide really clear guidance and centralised training modules that are available on Civil Service Learning. We do everything we can from the centre, and then we support Departments in making sure that gets to individuals.

Chair: I thank Joanna Davinson very much for what you do in your Department. Cat Little, I thank you and your team. They work 24 hours a day to keep us safe in the electronic communications sphere. That is much appreciated.

This has been a good session, and we have covered a lot of ground. You are busy people; thank you very much indeed. An uncorrected transcript of this hearing will be published on the Committee's website in the coming days, and the Committee will consider the evidence you have provided us with in such detail and produce a Report with recommendations in due course.