House of Commons

Committee of Public Accounts

Government cyber resilience

Twenty-Fourth Report of Session 2024–25 HC 643

Committee of Public Accounts

The Committee of Public Accounts is appointed by the House of Commons to examine "the accounts showing the appropriation of the sums granted by Parliament to meet the public expenditure, and of such other accounts laid before Parliament as the committee may think fit" (Standing Order No.148)

Current membership

Sir Geoffrey Clifton-Brown (Conservative; North Cotswolds) (Chair)

Mr Clive Betts (Labour; Sheffield South East)

Nesil Caliskan (Labour; Barking)

Mr Luke Charters (Labour; York Outer)

Anna Dixon (Labour; Shipley)

Peter Fortune (Conservative; Bromley and Biggin Hill)

Rachel Gilmour (Liberal Democrat; Tiverton and Minehead)

Sarah Green (Liberal Democrat; Chesham and Amersham)

Sarah Hall (Labour; Warrington South)

Lloyd Hatton (Labour; South Dorset)

Chris Kane (Labour; Stirling and Strathallan)

James Murray (Labour; Ealing North)

Sarah Olney (Liberal Democrat; Richmond Park)

Rebecca Paul (Conservative; Reigate)

Michael Payne (Labour; Gedling)

Oliver Ryan (Independent; Burnley)

Powers

Powers of the Committee of Public Accounts are set out in House of Commons Standing Orders, principally in SO No.148. These are available on the Internet via www.parliament.uk.

Publication

This Report, together with formal minutes relating to the report, was Ordered by the House of Commons, on 24 April 2025, to be printed.
It was published on 9 May 2025 by authority of the House of Commons.

Committee reports are published on the Committee's website at www.parliament.uk/pac and in print by Order of the House.

Contacts

All correspondence should be addressed to the Clerk of the Committee of Public Accounts, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 8480; the Committee's email address is pubaccom@parliament.uk. You can follow the Committee on X (formerly Twitter) using @CommonsPAC.

Contents

Summary

The severity and nature of the cyber threat to the government has evolved more rapidly than the Cabinet Office anticipated. There is now a substantial gap between the threat and the government's ability to respond. Cyber attackers are already disrupting public services, and will continue to do so without significant improvements to government's resilience. New technologies, such as AI, are showing why government must be able to react quicker.

Government has been unwilling to pay the salaries necessary to hire the experienced and skilled people it desperately needs to manage its cyber security effectively. Commendably, government has increased its digital workforce to 23,000 people. However, one in three cyber security roles remain either vacant or filled by expensive contractors. Experience suggests government will need to be realistic about how many of the best people it can recruit and retain. This includes the need for departments to have digital and security leaders on their most senior boards. Many departments have not understood the severity of the cyber threat or done enough to prioritise cyber security.

It is positive that the Cabinet Office is now independently verifying the resilience of departments' 'critical' IT systems. However, this has shown that departments' cyber resilience is lower than expected and has fundamental weaknesses. We find it alarming that risky 'legacy' IT systems, which the Department for Science, Technology and Innovation (DSIT) estimated make up 28% of the public sector's IT estate, have not undergone a similarly independent assessment. We recognise that the size and complexity of the public sector, and its supply chains, make it challenging for government to manage cyber risk. However, it is unacceptable that the centre of government does not know how many legacy IT systems exist in government and therefore cannot manage the associated cyber risks.

Looking forward, the Cabinet Office will not meet its target for government to be cyber resilient by the end of 2025. The Cabinet Office is aware that helping the wider public sector be cyber resilient by 2030 will require government to take a fundamentally different approach. It needs to strike the right balance between supporting departments, holding departments to account, and doing more from the centre of government. We are glad the Cabinet Office is learning from the valuable experience of our international partners, and look forward to greater transparency about government's performance, as it continues working to tackle this urgent issue.

Introduction

Cyber attack is one of the most serious risks to the UK and the Government's resilience. The government defines cyber resilience as "the ability of an organisation to maintain the delivery of its key functions and services and ensure the protection of its data, despite adverse cyber security events". government's digital estate is vast, complex and diverse. Departments, arm's–length bodies and their partners use a wide range of IT systems to provide public services. Ageing and outdated IT systems, known as 'legacy', increase the cyber risk to government. The cyber threat comes from individuals, groups or organisations, including hostile states and financially motivated cyber criminals, that have malicious intent to cause harm to digital devices or systems. Cyber attacks increasingly threaten the government's ability to safeguard national security and run public services.

The Government Security Group (GSG) in the Cabinet Office is responsible for leading the implementation of the *Government Cyber Security Strategy*: 2022–2030 ('the Strategy') and supporting government departments to improve their cyber resilience. GSG works closely with the Government Digital Service (GDS) in the Department for Science, Innovation and Skills (DSIT). Departments are responsible for their own cyber resilience and for ensuring their sectors and arm's–length bodies meet strategic resilience targets. The National Cyber Security Centre (NCSC) provides technical advice, support and guidance. In the 2021 Spending Review, the government announced it would invest £2.6 billion in cyber, of which it allocated £1.3 billion to departments for cyber security and legacy IT remediation.

Conclusions and recommendations

1. **Government has not kept up with the severe and rapidly evolving cyber threat.** Government's adversaries, both hostile states and criminals, have developed their capability faster than government expected. Government is concerned by the growing intent of hostile states to disrupt public services and critical national infrastructure. Ransomware attacks by criminal groups are prolific and recovery from attacks is costly. For example, the British Library's response to its October 2023 attack has cost around £7 million so far. Cyber attacks have devastating effects on people's lives. In June 2024, the cyber attack on a supplier of NHS pathology services (Synnovis) in south–east London led to two NHS foundation trusts postponing over 10,000 appointments. The UK is part of an accelerating "technology race". New technologies, such as AI, are both a threat and an opportunity for cyber security. Government will need to keep updating its plans in response to this ever–changing threat and technology landscape. However, government has not been as alive to the cyber threat as it should have been. As the Cabinet Office acknowledges, there is now a significant gap between the threat and government's response to it.

   RECOMMENDATION
   In one year's time, the Cabinet Office should write to the Committee setting out their assessment of: how the cyber risk to government has continued to change; how government's approach has evolved in response; and the extent to which the gap between the cyber threat and government's cyber resilience has grown or reduced.

2. **There is a longstanding shortage in government of the experienced, technical cyber skills required.** Skilled cyber security professionals are scarce and in high demand nationally and globally. As this Committee has frequently reported over the years, government finds it hard to compete with the private sector for the best talent, in part because it has not been willing to pay market–rate salaries. The Cabinet Office reports that government has successfully expanded its digital, data and technology profession to 23,000 people, which represents 6% of the total civil service, and it wants to further expand this to 10%. However, significant vacancies remain, particularly for expert cyber skills. Right now, one in three cyber

security roles in central government are vacant or filled by expensive contractors. In addition, civil service recruitment processes, which can take up to nine months, are not quick enough. The Cabinet Office and DSIT are intervening to address these issues, including by increasing the amount departments can pay cyber professionals. If government paid higher, market–rate salaries, it would save money over the longer term compared to using contractors, especially if it helps to reduce risk. The Cabinet Office noted it could do better at improving diversity in government's cyber security community. Only 20% of cyber security professionals in government are women.

RECOMMENDATION
Following the conclusion of the 2025 Spending Review, the Cabinet Office should set out: how many of the estimated cyber vacancies in government that its central interventions will fill; and how it will support departments' plans to fill the remaining gaps in their workforces.

3. **Departments have not done enough to prioritise cyber security, meaning that government's cyber resilience is far from where it needs to be.** Accounting officers are responsible for protecting the security of their organisations. Until recently, the Cabinet Office had not given departments a clear picture of the cyber threat and what they should do about it. Departments have underestimated the severity of the threat, and their funding and prioritisation decisions have not reflected the urgency of the issue. All departments must ensure their senior management and decision–making boards include senior and expert digital and security leaders. The Cabinet Office has mandated that its own board has at least one digital expert and it now expects all other departments to do the same. The British Library has set a good example by sharing the lessons it learned from the ransomware attack it suffered. However, there is not a good enough culture across government whereby departments openly share learning and information from cyber incidents with each other. The Cabinet Office assured us that the new Government Cyber Coordination Centre is increasing the flow of data across government and helping it to better 'defend as one'.

RECOMMENDATION
The Cabinet Office should set out how it is supporting accounting officers to: improve accountability by appointing an appropriately experienced and expert Chief Information Officer and Chief Security Officer at senior management and board–level; include cyber resilience in departmental plans and activities; and create a strong cyber security culture in their organisations.

4. **Government still has substantial gaps in its understanding of how resilient its IT estate is to cyber attack.** In July 2024, GovAssure's assessment of 72 critical IT systems across 35 organisations, identified that government cyber resilience was substantially lower than the Cabinet Office expected. Departments had multiple fundamental control failures, including in risk management and response planning. The GovAssure scheme collects data about departments' 'critical' IT systems to assess their cyber resilience. This is a clear improvement compared with the previous reliance on departments' optimistic self–assessments, but government should have collected reliable data sooner. We recognise the need to balance effort between assurance and frontline security, but there is also scope for GovAssure to assess more systems, faster. Separately, DSIT's understanding of Government's 'legacy' IT assets relies on self–assessments by departments. By January 2025, 28 public sector organisations had identified 319 legacy systems in use across government, rating around 25% as 'red' because there was a high likelihood and impact of risks occurring. However, DSIT does not know how many legacy systems there are in total. Departments need to make a more complete and reliable assessment of their legacy systems so that government can take informed decisions about funding, prioritisation and risk.

RECOMMENDATION
The Cabinet Office should set out: what proportion of critical and legacy IT systems it has assessed so far; the optimal scale and frequency of assessment activity needed; a deadline for when this will be achieved by; and how it will prevent departments from diverting funding away from this activity.

5. **The scale and diversity of government's supply chains, and the size of the public sector, makes it significantly harder for government to manage cyber risk.** The Cabinet Office expects departments to understand and tackle the cyber risk to their arm's–length bodies and the wider public sector that they are responsible for. Departments should work closely with the Cabinet Office, in particular the Government Security Group, in assuring this risk as arm's–length bodies may be an entry point for cyber attackers. Departments have not always met this expectation because of insufficient funding, staff, and oversight mechanisms. Lessons can be learned from the Department of Health and Social Care, which has begun to improve the resilience of its sector by putting in place a cyber security strategy, strengthening assurance processes, investing in common services, and setting clear policies. Departments also need to understand and manage the risks to security from their supply chains, which can be vulnerable to adversaries seeking to gain access to or disrupt government networks. The ransomware attack on Synnovis is an example of a supply

chain attack that had serious consequences for individuals and disrupted services. The Cabinet Office says it is giving departments text to include in contracts so that suppliers put appropriate cyber security measures in place, and that it plans to work with strategic suppliers to help improve government's resilience.

RECOMMENDATION
The Cabinet Office should secure clear assurance from departments that they understand and are effectively managing the cyber risk from their arm's–length bodies and supply chains.

6. **Government's work to date has not been sufficient to make it resilient to cyber attack by 2025, and meeting its 2030 aim to make the wider public sector cyber resilient will require a fundamentally different approach.** The Cabinet Office's focus on implementing its initiatives, such as GovAssure, has been at the expense of it coordinating a cross–government plan that challenges departments to meet their cyber resilience targets. The cyber risk to government is now extremely high and the Cabinet Office does not expect to meet its aim for "government's critical functions to be significantly hardened to cyber attack by 2025". Its aim for the whole of government and the wider public sector to be "resilient to known vulnerabilities and attack methods no later than 2030" is very ambitious. This is only achievable if government moves further and faster than it has before. The Cabinet Office assured us it is planning to take a fundamentally different approach for how it operates in future. It is reassuring that the Cabinet Office is learning from the experience of Australia, Canada and other international governments as it designs its new approach to improving government's cyber security and resilience. We would welcome the greater transparency on public sector resilience levels that the Australian Government has used successfully to improve accountability.

RECOMMENDATION
Following the conclusion of the 2025 Spending Review, the Cabinet Office should set out what levers and instruments the centre of government will use to take a fundamentally different approach to cyber resilience.

1 The challenge of cyber resilience in Government

Introduction

1. On the basis of a report by the Comptroller and Auditor General, we took evidence from the Cabinet Office and the Department for Science, Innovation and Technology (DSIT) on the cyber resilience of Government.[1]

2. Cyber attack is one of the most serious risks to the UK and the Government's overall resilience. The COVID–19 pandemic highlighted that the UK needed to strengthen its national resilience and prepare for future emergencies. The government defines cyber resilience as "the ability of an organisation to maintain the delivery of its key functions and services and ensure the protection of its data, despite adverse cyber security events".[2]

3. The need for government to improve its cyber resilience is becoming more urgent in an increasingly digital world. The last decade has seen rapid growth in government's digital ambitions, and the number of devices and IT systems that connect people, organisations and businesses globally. Government's digital estate is vast, complex and diverse. Departments, arm's–length bodies and their partners use a wide range of IT systems and technology to provide public services. Ageing and outdated IT systems, known as 'legacy', increase the government's exposure to cyber attack. This is because their creators no longer update or support their use, few people have the skills to maintain them, and they have known vulnerabilities.[3]

4. The cyber threat to government comes from individuals, groups or organisations that have malicious intent to cause harm to digital devices or systems. These include hostile states, who use cyber intrusions to carry out espionage or disruptive activities, and financially motivated cyber criminals or groups. Cyber attacks increasingly threaten the government's ability to safeguard national security and run public services.[4]

1 C&AG's Report, Government cyber resilience, Session 2024–25, HC 546, 29 January 2025
2 C&AG's Report, paras 1, 1.2–1.3
3 C&AG's Report, para 2
4 C&AG's Report, para 2

5. In January 2022, the Cabinet Office published the *Government Cyber Security Strategy: 2022–2030* ('the Strategy') which, for the first time, set out the challenges facing Government cyber security and a vision for improving it. The Government Security Group (GSG) in the Cabinet Office leads the government's security function, including cyber security. It is responsible for leading implementation of the Strategy and supporting departments to improve their cyber resilience. GSG works closely with the National Cyber Security Centre (NCSC), the UK's technical authority on cyber security, which provides technical advice, support and guidance on cyber security. GSG also works with the Government Digital Service (GDS) in DSIT, which leads government's digital and data function.[5]

6. Departments are responsible for their own cyber resilience and meeting the security standards set by GSG. They also are responsible for ensuring their sectors and arm's–length bodies meet strategic resilience targets. In the 2021 Spending Review, the government announced it would invest £2.6 billion in cyber, of which it allocated £1.3 billion to departments for cyber security and legacy IT remediation.[6]

The cyber threat

7. The Cabinet Office told us that we should be extremely worried by the rapidly evolving cyber threat, which is the most sophisticated it has ever been. It explained that over the last three years, government's adversaries, which include nation states and organised criminal groups, have developed their 'capabilities' more rapidly than it expected.[7]

8. The Cabinet Office highlighted concerns about nation states' intent to conduct espionage and disrupt essential services.[8] It described a campaign of espionage by Russian military intelligence that involved stealing and leaking data, and defacing websites. The Cabinet Office considered disruptive cyber attacks to be an increasing risk. It gave the example of Volt Typhoon, a Chinese state–affiliated group, which had targeted US critical national infrastructure with the intention of disrupting essential services.[9]

9. Organised criminal groups use ransomware and data extortion to make money.[10] They do this by stealing and encrypting victims' data and then demanding a ransom or threatening to the leak the data. In October 2023,

5 Q 2; C&AG's Report, paras 4, 6
6 C&AG's Report, paras 6, 22
7 Q 4
8 Qq 4–5
9 Q 5
10 Q 5

the British Library suffered a ransomware attack, which it was still recovering from a year after the attack.[11] The cyber attackers encrypted most of the British Library's servers, leaked around 500,000 records and stole several terabytes of data. The Cabinet Office told us that responding to the attack cost the British Library between £6 million and £7 million.[12] We asked the Cabinet Office for an example of a cyber attack that had affected the public. The Cabinet Office pointed to the June 2024 ransomware attack on Synnovis, a supplier of NHS pathology services, which led to two NHS foundation trusts postponing more than 10,000 appointments and put a significant amount of data at risk. Ransomware attacks on Hackney, and Redcar and Cleveland councils, have also disrupted public services.[13]

10. Both the cyber threat and government's cyber security are continuing to evolve as technology develops.[14] The Cabinet Office described this to us as a "technology race" that required government to adapt its approach constantly.[15] We asked how government thought artificial intelligence (AI) would affect cyber security. The witnesses argued that AI was a huge opportunity, but that it needed to be introduced securely. The Cabinet Office's assessment was that adversaries were already using AI to probe its cyber defences.[16]

11. We pressed the Cabinet Office on what assurance it could give us that government was keeping up with the cyber threat.[17] The Cabinet Office's assessment was that there was already a gap in government's ability to respond and that this might always be the case. It suggested the best approach may be continuously managing and mitigating the risk as far as possible, in a way that is value for money. The Cabinet Office stressed the importance of resilience, so that even if government does not detect an incident it is still able to respond and recover effectively. The Cabinet Office acknowledged that government's current cyber resilience levels were not good enough to do this.[18]

Cyber skills

12. For more than a decade, skilled cyber security professionals have been in short supply and high demand nationally and globally. Government has not paid market–rate salaries for digital and cyber skills, which has been

11 C&AG's Report, paras 1.7, 1.10
12 Q 5
13 Q 6
14 C&AG's Report, para 12
15 Q 8
16 Qq 10–11
17 Qq 8–9
18 Q 8

a significant barrier to recruitment and retention.[19] This Committee has often reported on how this shortfall of digital skills has affected the work of government.[20] The Cabinet Office and DSIT told us that they have made progress by significantly expanding the civil service's digital, data and technology profession. They stated this included 23,000 people, which was around 6% of the total civil service, and that they aimed to increase this to 10%.[21] In correspondence provided after our evidence session, the Cabinet Office explained that this would involve replacing 7,000 contractors and consultancy employees with civil servants, which it claimed could result in annual savings of up to £500 million.[22]

13. In 2023–24, one in three cyber security roles in central government were vacant or filled by expensive contractors, and the proportion of vacancies in several departments' cyber security teams was more than 50%.[23] The Cabinet Office accepted that there were significant cyber–skill vacancies and set out the actions it was taking to address the shortfall.[24] These included a cyber 'fast stream' and a 'TechTrack' apprenticeship programme to develop more talent within government. The Cabinet Office also told us about a new digital pay framework, which it had designed to allow departments to pay higher salaries to cyber professionals.[25] In its letter to us, the Cabinet Office clarified that, for the first time since 2016, it was increasing the maximum amount that departments could pay civil servants in technical roles below the senior civil service grade, by £15,000. This means cyber professionals in government could earn up to £110,000 per annum.[26] We pushed the Cabinet Office on government's reluctance to pay market–rate salaries. The Cabinet Office agreed that paying higher salaries would still be cheaper than using contractors and could save money over the longer term, if it helped to reduce risk.[27]

---

19 C&AG's Report, para 4.15

20 For example: Committee of Public Accounts, Defence Digital, Thirty–Sixth Report of Session 2022–23, HC 727, 3 February 2023; Committee of Public Accounts, BBC Digital, Forty–Sixth Report of Session 2022–23, HC 736, 28 April 2023; Committee of Public Accounts, Digital transformation of the NHS, Eighth Report of Session 2022–23, HC 223, 30 June 2023

21 Qq 12–13

22 Letter from the Civil Service Chief Operation Officer and Cabinet Office Permanent Secretary relating to the oral evidence session held on 10 March 2025 on Government Cyber Resilience, 24 March 2025

23 C&AG's Report, para 4.15

24 Q 13

25 Q 12

26 Letter from the Civil Service Chief Operation Officer and Cabinet Office Permanent Secretary relating to the oral evidence session held on 10 March 2025 on Government Cyber Resilience, 24 March 2025

27 Qq 19–20

14. We asked the Cabinet Office why civil service recruitment processes remained a barrier. The Cabinet Office noted data suggesting it took on average nine months to recruit technology specialists. The Cabinet Office described this as not being good enough and said that it was trying different ways of shortening the time it takes to recruit. The Cabinet Office raised that it could also do much more to make government's cyber security community more diverse. The Cabinet Office's statistics showed that only around 20% of government's cyber security community were women.[28]

15. Recruitment is fragmented across government, with some departments developing their own cyber recruitment and training programmes based on their needs.[29] We queried how the Cabinet Office was working across Government, rather than letting each department train and recruit in its own way. The Cabinet Office told us that it was planning a new series of interventions. These included the Department for Work and Pension's (DWP) cyber academy, which is reskilling civil servants who want a career in cyber. The Cabinet Office reassured us that DWP is running its cyber academy on behalf of the whole of government, so graduates would be deployed across government.[30]

Departments' responsibilities for cyber resilience

16. Accounting officers in departments are responsible for protecting the security of their organisations and managing their department's cyber risk, but they have not taken sufficient ownership of this responsibility. Often, membership of departments' most senior boards does not include a digital expert.[31] Some departments have been reluctant to share information about their cyber incidents with other parts of government. When departments are transparent about their cyber incidents, other organisations can learn from them and improve their own cyber resilience. In the 2021 Spending Review, the Government announced it would invest £2.6 billion in cyber and 'legacy' IT, of which it gave £1.3 billion to departments. Some departments have significantly reduced the scope of their cyber security improvement programmes to fund other priorities.[32]

17. We asked the Cabinet Office if departments have underestimated the cyber risk. It told us that until recently it had not done enough to ensure leaders across government understood the cyber threat, but that it had made

28 Q 17
29 C&AG's Report, para 4.16
30 Qq 17–18
31 C&AG's Report, para 4.2–4.4
32 C&AG's Report, para 4.9–4.12

significant improvements in the last three years.[33] These included bringing all the permanent secretaries together to discuss their responsibilities for cyber risk and writing to them to remind them of their duties.[34] We suggested to the Cabinet Office that all departments needed to have a Chief Security Officer operating at senior levels. The Cabinet Office agreed that government should have senior people accountable and there was a need to have a very senior Chief Information Officer in every single department as standard.[35] We asked the Cabinet Office if its senior board had a digital expert and it explained that it was recruiting new non–executive members and that these would include at least one digital expert. The Cabinet Office expected every department to do the same.[36] The Cabinet Office reassured us that as part of the 2025 Spending Review, government was undertaking a comprehensive review of its technology budget and how it is spent.[37]

18. We asked the Cabinet Office what the impact was when departments did not share information about their cyber incidents. The Cabinet Office agreed that sharing data is essential to learn lessons, understand vulnerabilities, share best practice and work out what has gone wrong. The Cabinet Office reassured us that if departments find any vulnerabilities that could affect other parts of government, it shares these immediately. The Cabinet Office accepted that departments could be cautious and concerned about reputational damage, but noted there may also be good reasons to not share data. The Cabinet Office told us it wants to increase transparency and that its role is to challenge departments on how much they share and help manage their concerns.[38] When we asked the Cabinet Office what it was doing to promote a culture of learning from mistakes and near misses, it responded that this was one of its biggest cultural priorities.[39]

19. We asked the Cabinet Office what structures it had in place to share information about cyber security with permanent secretaries and throughout departments.[40] The Cabinet Office told us that it had launched the Government Cyber Coordination Centre (GC3) in September 2023, and that this had helped government share information more effectively. The GC3 brings together people from the National Cyber Security Centre,

33 Q 26
34 Q 29
35 Q 31
36 Q 28
37 Q 57
38 Qq 33–34
39 Q 36
40 Q 35

the Cabinet Office, and the Government Digital Service.[41] The Cabinet Office added that GC3 was in its early stages, but was starting to build communities of cyber practitioners across government.[42]

41 Q 34; C&AG's Report, para 2.16

42 Q 35

2 Improving Government's cyber resilience

Resilience of the IT estate

20. In 2023, the Cabinet Office launched 'GovAssure', a cyber security assurance scheme, as part of its strategy to improve government organisations' cyber resilience. Before GovAssure, departments self–assessed their performance against minimum cyber standards set by the Cabinet Office.[43] In the period April 2023 to July 2024, 35 departments took part in the first year of GovAssure and assessed 72 IT systems, of which independent reviewers verified 58. The GovAssure data showed that there were significant gaps in departments' cyber resilience, including low levels of maturity across asset management, protective monitoring, and response planning.[44]

21. The Cabinet Office told us that GovAssure would run continually to give regular updates on government's resilience. Although the systems assessed so far are a small part of government's IT estate, the Cabinet Office argued that they were representative of organisations and services. As a result, the Cabinet Office said it could infer from the GovAssure results what the overall state of government's cyber resilience was.[45]

22. The Cabinet Office told us that cyber resilience was substantially lower than it had expected following departments' previous self–assessments. It had found that the organisations that GovAssure's independent reviewers had scored poorly were the most over–optimistic in their self–assessments.[46] We challenged the Cabinet Office on why it had not introduced GovAssure sooner. The Cabinet Office acknowledged that it had probably been unrealistic to rely on self–assessment and that it had not been sufficiently alert to the threat, until incidents brought it to life.[47]

23. We asked the Cabinet Office how it would increase the scale and pace of GovAssure to assess the cyber resilience of all of government's critical systems. The Cabinet Office explained that it did not plan to assess 100%

43 C&AG's Report, paras 14, 15
44 C&AG's Report, para 19
45 Q 39
46 Q 44
47 Q 45

of critical systems through GovAssure.[48] This was because GovAssure was one part of a wider system of assurance, which included department's own cyber experts as the "first line of defence". The Cabinet Office said that it had designed GovAssure to bring consistency and share best practice, but that government must balance its effort between assurance and frontline cyber security.[49] We asked if that meant the Cabinet Office was happy with the current scale and pace of GovAssure. The Cabinet Office told us it wanted to increase the number of systems it assessed and it needed to make GovAssure quicker and easier to complete for departments.[50]

24. Many of government's IT systems are 'legacy', because they are ageing and outdated but still in use. The government estimated that it used nearly half of its £4.7 billion IT expenditure in 2019 to keep legacy systems running. Risks to public services posed by legacy technology have built up over many years.[51] In 2023, the Government Digital Service published a legacy IT risk assessment framework. It has used this to collect data from some departments about the legacy systems they own, the risks they present, and plans to remediate them.[52]

25. We challenged DSIT and the Cabinet Office on why they were not identifying and fixing legacy IT systems, where the risk is greatest and security lowest. DSIT told us that before 2023 the centre of government did not have much information about legacy IT but this was improving. DSIT data showed that around 28% of the public sector's IT estate was legacy. Twenty–eight public sector organisations had identified 319 legacy systems and self–assessed almost 25% of these as 'red' for risk.[53] DSIT said it wanted to expand this work and better align it with GovAssure.[54] We asked how many legacy assets there were in total across government. DSIT told us it did not know, and that 15% of organisations it had spoken to, as part of the *State of digital government review,* also did not know the what the situation was for their own legacy IT.[55]

26. We pressed DSIT and the Cabinet Office on why Government's understanding of its legacy IT was so limited. They told us that the amount of legacy systems, and understanding of them, varied between departments. They said this was because information about legacy systems

48 Q 39
49 Qq 41–42
50 Q 43
51 C&AG's Report, para 1.3
52 C&AG's Report, para 3.5
53 Q 47; Letter from the Civil Service Chief Operation Officer and Cabinet Office Permanent Secretary relating to the oral evidence session held on 10 March 2025 on Government Cyber Resilience, 24 March 2025
54 Q 47
55 Q 49; Department for Science, Innovation & Technology, State of digital government review, January 2025

was not easy to access and was spread across arm's-length and other public bodies. The Cabinet Office agreed there was an unacceptable gap in knowledge about government's legacy IT.[56] We asked why departments could not provide a list of the systems they have. We heard that data were in different formats across departments and poor asset management meant departments could not easily collate this data.[57] DSIT told us that departments and the centre of government had limited resource to understand and fix legacy systems.[58]

27. We queried how government could manage the risk from legacy systems, make informed bids for funding to fix them, or prevent departments reprioritising this funding, if it did not know what systems it had.[59] The Cabinet Office told us that legacy systems were one of its biggest priorities, but that departments needed to own the risk.[60] DSIT claimed that many of these legacy systems were likely to be isolated from networks and, although expensive to run, were not flashing 'red' as a risk.[61] DSIT also told us that moving to subscription-based services, such as cloud platforms, helps government to manage the risks posed by legacy IT.[62]

Managing suppliers and the wider public sector

28. Departments, arm's-length bodies and their partners use a wide range of IT systems and technology to provide public services.[63] The *Government Cyber Security Strategy: 2022–2030* ('the Strategy') set out that government departments' cyber responsibilities included ensuring their arm's-length bodies and wider public sector meet resilience targets. In April 2024, the Cabinet Office reported it could not be confident that departments were meeting these responsibilities. Departments reported that they did not have enough funding, people, or oversight to understand and improve resilience across their sectors.[64]

29. The Cabinet Office confirmed to us that lead government departments were responsible for understanding and tackling cyber risk across the wider public sector. While recognising that departments' response to the Strategy

56 Q 49
57 Qq 50–51
58 Q 53
59 Qq 54, 57–58
60 Q 58
61 Q 56
62 Q 80
63 C&AG's Report, para 11
64 C&AG's Report, para 4.5; The Cabinet Office, Government Cyber Security Strategy: 2022–2030, January 2022

had been "varying", the Cabinet Office focused on the Department of Health and Social Care (DHSC) as a positive example. It told us that DHSC had set a clear cyber security strategy for health and social care that linked to the Cabinet Office's own strategy. The Cabinet Office said that by strengthening assurance processes, putting in place policies, and investing in common services, DHSC had started to improve its sector's resilience.[65]

30. We asked the Cabinet Office how Government managed the cyber security of its supply chain. The Cabinet Office told us that managing supply chain risk was complex and difficult. Government's supply chain has been the source of incidents with serious consequences for individuals, such as the ransomware attack on the supplier of NHS pathology services, Synnovis. The Cabinet Office set out to us the actions it was taking improve its management of supply chain risk. It was creating schedules that departments could include in future contracts to ensure they were asking their suppliers for the right security measures. The Cabinet Office planned to work with strategic suppliers in 2025–26 to agree objectives for how they will help government improve its cyber resilience. DSIT and the Cabinet Office cited the example of a partnership agreement with Microsoft.[66]

31. Based on written evidence, we asked the Cabinet Office about the advantages and disadvantages of relying on a few strategic suppliers.[67] The Cabinet Office acknowledged that trying to maximise value for money and interoperability while managing the risks was not straightforward. DSIT added that this was not just a cyber security issue. In July 2024, the major global IT outage resulting from a Crowdstrike software update on Microsoft systems caused significant impacts around the world.[68] Regarding competition concerns in the markets for cloud services, the Cabinet Office told us that this was not just a government challenge. Many organisations were using the two suppliers that dominated the market. DSIT reassured us that it was working to prevent government services to regions of the UK becoming too concentrated on a single supplier.[69]

Meeting the 2025 and 2030 targets

32. The Cabinet Office has prioritised implementing its central initiatives, such as GovAssure. However, it has not put robust arrangements in place to oversee how departments are implementing the Strategy, such

65 Q 67
66 Q 61
67 Q 79; GCR0004, Written evidence submitted by Nigel D Cook; GCR0007, Written evidence submitted by The Open Cloud Coalition
68 Hansard, CrowdStrike: IT Outage, 22 July 2024
69 Q 80

as a cross–Government plan or performance framework.[70] The National Audit Office (NAO) concluded that government would not meet its aim for "government's critical functions to be significantly hardened to cyber attack by 2025". The Cabinet Office's aim for the whole of government and the wider public sector to be "resilient to known vulnerabilities and attack methods no later than 2030" is ambitious.[71] In April 2024, ministers expressed support for the Cabinet Office to be more directive and provide departments with more centralised capability and support.[72] The Cabinet Office assured us that it was working across the devolved administrations to meet its cyber resilience aims for the whole of government.[73]

33. We asked the Cabinet Office how it intended to meet its target for 2030. The Cabinet Office was clear that the target would be challenging to meet. To do so, it told us that government would need to take a fundamentally different approach to cyber security. The Cabinet Office was designing this new approach, which it said would focus on what the centre of government could do to bring about change. Its plans included strengthening accountability, setting requirements for departments and measuring their performance against them, and providing services "once and well" from the centre of government to the public sector. The Cabinet Office gave the example of cross–Government vulnerability scanning, which the Government Digital Service was testing.[74]

34. We challenged the Cabinet Office on whether its plans were realistic. The Cabinet Office told us it had accepted the NAO's recommendation that it needed a cross–Government implementation plan and a stronger monitoring and evaluation framework.[75] It said these would be ready in the summer of 2025, after the Spending Review concluded.[76] We asked the Cabinet Office how it knew which were the right issues to focus on if it lacked oversight of departments' activities. The Cabinet Office clarified that it was working closely with departments, including through GovAssure and the GC3, which has helped it better understand and measure department's risks and challenges.[77]

35. We asked if there were any countries that manage cyber security effectively that the UK should learn from. The Cabinet Office told us that most of the UK's international partners were also trying to catch up with the

70 C&AG's Report, paras 2.5, 2.20–2.21
71 C&AG's Report, paras 16, 25; The Cabinet Office, Government Cyber Security Strategy: 2022–2030, January 2022
72 C&AG's Report, para 2.22
73 Q 68
74 Q 67
75 Q 69
76 Q 71
77 Q 70

fast–moving threat.[78] The UK could learn a lot from other international governments, including Canada and Australia, which have done more from the centre of government and have focused on transparency and assurance. The Cabinet Office told us that its counterparts in Australia regularly publish the resilience levels of government organisations and have found this improves accountability. The Canadian centre of government provides services and capabilities to the rest of government, which lets it understand and respond to risk more effectively. The Cabinet Office said it was learning from these approaches as it designs the UK Government's new approach to cyber security.[79]

78 Q 75
79 Q 76

Formal minutes

Thursday 24 April 2025

Members present

Sir Geoffrey Clifton-Brown, in the Chair

Mr Clive Betts

Anna Dixon

Sarah Hall

Michael Payne

Oliver Ryan

Government cyber resilience

Draft Report (*Government cyber resilience*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 35 read and agreed to.

Summary agreed to.

Introduction agreed to.

Conclusions and recommendations agreed to.

Resolved, That the Report be the Twenty-Fourth Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available (Standing Order No. 134).

Adjournment

Adjourned till Monday 28 April 3 p.m.

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Monday 10 March 2025

Cat Little, Permanent Secretary, Cabinet Office, Chief Operating Officer, Civil Service; **Vincent Devine**, Government Chief Security Officer and Head of the Government Security Function, Cabinet Office; **Bella Powell**, Cyber Director, Government Security Group, Cabinet Office; **Joanna Davinson**, interim Government Chief Digital Officer, Cabinet Office Q1-83

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

GCR numbers are generated by the evidence processing system and so may not be complete.

1	Cartwright, Professor Edward (Professor of Economics, De Montfort University); Cartwright, Dr Anna and Seifert, Dr Jacob (Lecturer in Economics, University of Leicester)	GCR0005
2	Cook, Mr Nigel D	GCR0004
3	Dresner, Professor Daniel (Professor of Cyber Security, The University of Manchester)	GCR0001
4	Information Commissioner's Office	GCR0002
5	Institute of Corporate Resilience (IoCR); and Cyber Security and Business Resilience policy centre (CSBR)	GCR0003
6	Surrey Centre for Cyber Security	GCR0006
7	The Open Cloud Coalition (OCC)	GCR0007

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website.

Session 2024–25

Number	Title	Reference
23rd	The cost of the tax system	HC 645
22nd	Government's support for biomass	HC 715
21st	Fixing NHS Dentistry	HC 648
20th	DCMS management of COVID-19 loans	HC 364
19th	Energy Bills Support	HC 511
18th	Use of AI in Government	HC 356
17th	The Remediation of Dangerous Cladding	HC 362
16th	Whole of Government Accounts 2022-23	HC 367
15th	Prison estate capacity	HC 366
14th	Public charge points for electric vehicles	HC 512
13th	Improving educational outcomes for disadvantaged children	HC 365
12th	Crown Court backlogs	HC 348
11th	Excess votes 2023-24	HC 719
10th	HS2: Update following the Northern leg cancellation	HC 357
9th	Tax evasion in the retail sector	HC 355
8th	Carbon Capture, Usage and Storage	HC 351
7th	Asylum accommodation: Home Office acquisition of former HMP Northeye	HC 361
6th	DWP Customer Service and Accounts 2023-24	HC 354
5th	NHS financial sustainability	HC 350
4th	Tackling homelessness	HC 352
3rd	HMRC Customer Service and Accounts	HC 347

Number	Title	Reference
2nd	Condition and maintenance of Local Roads in England	HC 349
1st	Support for children and young people with special educational needs	HC 353