House of Commons

Committee of Public Accounts

Cyber security in the UK

Ninety-Ninth Report of Session 2017–19

Report, together with formal minutes relating to the report

Ordered by the House of Commons to be printed 15 May 2019

HC 1745
Published on 5 June 2019
by authority of the House of Commons

The 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

Meg Hillier MP (*Labour (Co-op), Hackney South and Shoreditch*) (Chair)

Douglas Chapman MP (*Scottish National Party, Dunfermline and West Fife*)

Sir Geoffrey Clifton-Brown MP (*Conservative, The Cotswolds*)

Chris Davies MP (*Conservative, Brecon and Radnorshire*)

Chris Evans MP (*Labour (Co-op), Islwyn*)

Caroline Flint MP (*Labour, Don Valley*)

Robert Jenrick MP (*Conservative, Newark*)

Shabana Mahmood MP (*Labour, Birmingham, Ladywood*)

Nigel Mills MP (*Conservative, Amber Valley*)

Layla Moran MP (*Liberal Democrat, Oxford West and Abingdon*)

Stephen Morgan MP (*Labour, Portsmouth South*)

Anne Marie Morris MP (*Conservative, Newton Abbot*)

Bridget Phillipson MP (*Labour, Houghton and Sunderland South*)

Lee Rowley MP (*Conservative, North East Derbyshire*)

Gareth Snell MP (*Labour (Co-op), Stoke-on-Trent Central*)

Anne-Marie Trevelyan MP (*Conservative, Berwick-upon-Tweed*)

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

Committee reports are published on the Committee's website and in print by Order of the House.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

Committee staff

The current staff of the Committee are Richard Cooke (Clerk), Laura-Jane Tiley (Second Clerk), Hannah Wentworth (Chair Liaison), Ameet Chudasama (Senior Committee Assistant), Baris Tufekci (Committee Assistant), and Hajera Begum (Committee Support Assistant).

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 5776; the Committee's email address is pubaccom@parliament.uk.

You can follow the Committee on Twitter using @CommonsPAC.

Contents

Summary

The UK has one of the world's leading digital economies, designed to exploit the benefits of the internet, but this also makes it vulnerable to attack from hostile countries, criminal gangs and individuals. To counter this threat, and continue to support the UK's digital government and economy, since 2011 the Cabinet Office (the Department) has managed two, five-year national cyber security strategies. The Department is beginning to make progress in meeting the strategic outcomes of the current, 2016–2021 National Cyber Security Strategy after a poor start. However, a weak evidence base and the lack of a business case for the National Cyber Security Programme that helps to deliver the Strategy make it difficult for the Department to assess whether it will meet all its objectives by 2021. A lack of a business case also means it is unclear whether the money allocated at the start of the Programme was the right amount, making it more difficult to judge value for money. Digital technology and online services are fast-moving areas and constantly evolving, and we are concerned that consumers do not know how safe the websites or internet-enabled products they use are. There is clearly more that the government needs to do to make progress in this area.

Introduction

UK citizens and businesses increasingly operate online to deliver economic, social and other benefits, and the government aspires to be a world leader in digital economy and putting its services online. This makes the UK and its citizens more vulnerable to various risks when operating on the internet, collectively known as cyber-attacks. These attacks continue to increase and evolve. The government's view is that these risks can never be eliminated but can be managed to the extent that the opportunities provided by digital technology, such as reducing costs and improving services, outweigh the disadvantages.

Since 2010 government has taken a central lead in ensuring that the UK effectively manages its exposure to cyber risks. The Cabinet Office (the Department) has led this work, through successive National Cyber Security Strategies. The current National Cyber Security Strategy (the Strategy) runs from 2016 to 2021. It has a £1.9 billion budget. One part of delivering the Strategy is the National Cyber Security Programme (the Programme), which has a budget of £1.3 billion. The Strategy has 12 strategic outcomes. The Programme's objectives mirror these strategic outcomes. The Department currently assesses that one strategic outcome is on track to complete by March 2021. None of the remaining 11 strategic outcomes are currently due to be achieved by 2021, and the Department has 'low confidence' in the quality of the evidence that underpins the assessment of progress against many of these.

Conclusions and recommendations

1. **The UK is particularly vulnerable to the risk of cyber-attacks.** As one of the world's leading digital economies and global leader in putting government systems online, the UK is especially vulnerable to cyber-attacks. The National Cyber Security Centre (NCSC) has dealt with over 1,100 cyber security incidents since it was established in October 2016. The cyber-attack threat is evolving fast and becoming technically more complex, with the boundaries between state-orchestrated attacks and those of cyber criminals increasingly blurred. The government introduced a coordinated approach to cyber security in 2010 and has since published two, five-year strategies (National Cyber Security Strategy 2011–2016, and National Cyber Security Strategy 2016–2021). It has yet to set out its plans for its approach to cyber security after 2021. It needs to start planning now and develop a revised approach before the next Spending Review, which we understand should be announced as part of the 2019 autumn budget. Beyond 2021, the Department is expecting to put together a portfolio business case, rather than replicating its current approach of individual business cases for each of the 12 objectives of the Programme.

   Recommendation: ***The Department should ensure another long-term coordinated approach to cyber security is put in place well in advance of the current Strategy finishing in March 2021.***

2. **The Department cannot justify how its approach to cyber security is delivering value for money.** The £1.9 billion funding for the Strategy, including £1.3 billion for the Programme, was allocated via the 2015 Spending Review. The Department did not develop a business case for the Strategy or the Programme, although teams that manage each of the 12 objectives that make up the Programme do produce their own annual business cases. This means that the Department did not assess at the start whether £1.3 billion was the right amount needed to deliver the Programme and makes it more challenging to assess value for money. The Department acknowledges that it was not absolutely confident that the funding was at the right level, and that the estimated funding relied on a judgement about the resources required, the level of risk involved and the impact intended. It asserts that as its approach was cutting edge there was no existing approach or model for building a national cyber security strategy or programme on which the Department could base its assessment. The Department is nonetheless unable to explain what proportion of the overall Strategy the Programme itself is expected to deliver. In addition, a third (£169 million) of the Programme's planned funding for the first two years was either transferred or loaned to support other government national security priorities, such as counter-terrorism activities. Some £69 million of this funding will not be returned to the Programme, which seems at odds with the government's claim that cyber security is a priority.

   Recommendation: ***The Department should ensure that, to support any follow-on, long-term and coordinated approach to cyber security, it produces a properly costed business case.***

3. **The Department lacks the robust evidence base it needs to make informed decisions about cyber security.** The evidence base used to measure progress of the Strategy is weak. The Department has admitted that it has 'low confidence'

in the evidence used to assess progress against half of the Strategy's 12 strategic outcomes, and only has 'high confidence' in the evidence related to one strategic outcome—incident management. The Department did not conduct a robust 'lessons learnt' exercise to capture the evidence from the 2011–2016 National Cyber Security Strategy to help develop a baseline for the 2016–2021 National Cyber Security Strategy. Although the Department has been involved in aspects of cyber security for many years it often lacks evidence around the impact of its work; for example, on the demand for cyber skills. However, the Department has developed sufficient understanding in some areas to stop work where it is clear the desired impact has not been achieved. Its active cyber defence work is making good progress in generating evidence for future investments. Looking ahead, the Department is beginning work to ensure that it captures the relevant lessons from the current Strategy and hopes to develop a continuous process of learning rather than waiting until the Strategy ends in 2021.

Recommendation: ***The Department should write to the Committee by November 2019 setting out what progress it is making in using evidence-based decisions in prioritising cyber security work. This should include plans for undertaking a robust 'lessons learnt' exercise to capture all relevant evidence from the current Strategy and Programme to support any future approach to cyber security.***

4. **The Department has not been clear what the Strategy will actually deliver by 2021.** The Department asserts that it didn't intend to deliver all 12 strategic outcomes by the end of the Strategy in 2021, although it is unable to say how many it did intend to achieve. The evidence we heard suggests the Strategy committed to delivering 2 outcomes by 2021, although currently it is only on track to deliver a single strategic outcome, 'incident management'. The Department's 'low confidence' in the quality of the evidence underpinning the assessment of progress against many of the remaining 11 strategic outcomes gives us little confidence in the Department's progress up to 2021. Regarding the performance indicators for the Programme that support the Strategy, the Department is currently achieving only three of its 12 objectives. Unlike during the 2011–2016 National Cyber Security Strategy, the Department has not published any updates on progress since the current Strategy began, despite agreeing in the Strategy to report progress on an annual basis. It has committed to doing so in future and expects to produce its first report in May 2019.

Recommendation: ***When the Department publishes its costed plan in autumn 2019 for its future approach to cyber security it should also set out what the existing Strategy and Programme should deliver by March 2021, and the risks around those areas where it will not meet its strategic outcomes and objectives.***

5. **Government has not yet done enough to enhance cyber security throughout the economy and better protect consumers.** It is difficult for consumers to know whether the internet-enabled devices they buy or the companies they give their details to online are holding their information securely. For example, a trusted brand like British Airways was hacked in 2018, and the personal data of 380,000 customers was stolen. There is currently no 'traffic light' or 'kitemark' system to inform consumer choice on how cyber secure the products they buy are, unlike recognised standards in other areas—such as food safety. This is a difficult area for government to influence and regulate, although it has made some progress. For

example, the NCSC has promoted two-factor identification to make thefts of basic personal information less valuable to criminals on the open market. The NCSC has also worked with the Bank of England to build better cyber security standards. Rather than trying to impose a list of requirements on the banking sector, which may become rapidly outdated, the NCSC has provided technical advice to allow the Bank to best judge how to incorporate cyber security into its statutory mandate to promote financial stability. A similar approach could be developed to support other sectors of the economy, such as retail. Government also needs to involve larger organisations to make sure they realise the responsibility they have to encourage the smaller and more vulnerable companies that sit within their long supply chains to get their basic cyber security right. To help this process in 2018 NCSC published a guide specifically aimed at small and medium enterprises in an effort to get these organisations to improve their "basic hygiene" in terms of cyber security.

Recommendation: ***The Department should write to the Committee by November 2019, outlining how it intends to influence the different sectors in the economy—for example, retail—to provide consumers with information on their cyber resilience. As part of this it should outline how they intend to measure success in protecting consumers. This should also form part of its approach to cyber security after 2021.***

1 Delivering the National Cyber Security Strategy

1. On the basis of a report by the Comptroller and Auditor General, we took evidence from the Cabinet Office (the Department) about the progress of the 2016–2021 National Cyber Security Programme (the Programme).[1]

Introduction

2. The UK has one of the world's most open and most digital economies, making it vulnerable to attack from hostile counties, criminal gangs and individuals.[2] Their attempts to steal information, damage or disrupt these computer systems are called cyber-attacks and they continue to grow and evolve. The digital economy contributes a higher percentage to the UK's gross domestic product than in any other G20 country. There is growing digital connectivity across society; in 2018, 90% of UK households had digital access, compared with 77% in 2011. The risk of deliberate or accidental cyber incidents is heightened by the increasingly interconnected nature of networks, systems and devices in use by organisations and individuals. The government's view is that cyber risks can never be eliminated but can be managed to the extent that opportunities provided by digital technology, such as reducing costs and improving services, outweigh the disadvantages.[3]

3. In 2010, government decided that it needed centrally driven strategies and programmes to ensure the UK effectively manages its exposure to these risks.[4] The Cabinet Office is responsible for leading this work, through successive National Cyber Security Strategies, published in 2011 and 2016, and separate National Cyber Security Programmes designed to help deliver each strategy. The first programme had a budget of £860 million for the five-year period. Government departments and public bodies continue to remain responsible for safeguarding their own information.[5]

4. The current cross-government 2016–2021 National Cyber Security Strategy (the Strategy) has a budget of £1.9 billion. The Strategy is divided into three overarching themes—Defend, Deter and Develop, supported by International Action. These themes are divided into 12 strategic outcomes, ranging from developing cyber skills, managing and responding to cyber incidents and tackling cyber-crime. Specific departments are responsible for each of the 12 strategic outcomes. The Strategy includes £1.3 billion for the 2016–2021 National Cyber Security Programme (the Programme). Its objectives mirror those of the Strategy's strategic outcomes.[6]

The cyber threat

5. As one of the world's leading digital economies, and a global leader in putting government systems online, the UK is vulnerable to cyber-attacks.[7] At the time of our

[1] C&AG's Report, *Progress of the 2016–2021 National Cyber Security Programme*, Session 2017–19, HC 1988, 15 March 2019

[2] Q 82, C&AG's Report, para 1.8

[3] Q 65, C&AG's Report, paras 1–2

[4] Q82

[5] C&AG's Report, paras 3, 1.15–1.19

[6] Qq 82, 97, 106, C&AG's Report paras 4–6, Figure 1

[7] Qq 63–64, C&AG's Report, para 1

evidence session, the National Cyber Security Centre (NCSC) had dealt with over 1,100 cyber security incidents since it was established in 2016. The NCSC is the UK's technical authority on cyber security. It is responsible for understanding the cyber security environment; working with public and private sector organisations to improve their cyber security, responding to cyber security incidents and nurture and grow the UK's cyber security capability and provide leadership on critical national cyber security issues.[8] The NCSC told us that cyber-attacks are becoming more complex with the boundaries between state orchestrated attacks and those of cyber criminals becoming more blurred, criminal networks being used by state entities and the ability of some criminal networks to employ state resources.[9]

6. The Department explained that the government divides cyber threats into two types: strategic state actor threats and the more common and high-volume cyber-crime attacks. Part of the aim of the NCSC is to enable the country to be better equipped to deal with the low level, high volume cyber-crime attacks and can defend against them, so that cyber experts can concentrate on the high level, complex attacks which are more individual in nature.[10] The Department told us that it has built a free service that most NHS bodies and some local authorities use that allows them to scan for vulnerabilities on their networks, which tells them what is wrong and shows how to take basic precautions. Within local government around 4,000 vulnerabilities to cyber-attacks have been identified and fixed in the two years since the tool was introduced.[11]

7. The Department told us that the Spending Review of 2015 allocated £1.9 billion over five years for the Strategy and £1.3 billion of this for the Programme.[12] As the Department did not produce a business case for either of these allocations, it does not know if £1.3 billion is the right amount to deliver the Programme. The Department explained that the amount of money required for the Strategy and Programme was based on a judgement about the level of resources, the level of risk and the impact that a particular programme or strategy was trying to achieve that would lead it to an allocation. The Department also told us that as the UK was at the cutting edge of developing a cyber security strategy there was no model elsewhere in the world that showed what did and didn't work, therefore a judgement had to be made as to what should be included in the Programme. The Department could not explain in further detail how it how it arrived at the amount of money allocated and whether this was the right amount to deliver the Programme.[13]

8. Although cyber security is one of government's top priorities, the Department reprofiled Programme funding in its first two years. The Department explained that the Verify and Foxhound projects were given £69 million, and £100 million was loaned to counter-terrorism activities. It told us that around 50% of the £100 million was returned to the Programme by March 2019, with the remaining 50% expected to be returned in 2020–21. The Department told us that the reprofiling helped it to develop more innovative cyber security work, as it gave it the opportunity to test what would and wouldn't work. It similarly told us that this has meant, for example, that the active cyber defence element

[8] C&AGs Report, paras 1.19, 3.6
[9] Qq 65, 119
[10] Qq 65, 120
[11] Q67
[12] C&AG's Report, para 1.19, Q82
[13] Qq 82–86

of the Programme was given more money in the remaining years of the Programme—as during the financial reprofiling in the first two years it undertook pilot projects that showed which interventions worked.[14]

The lack of an evidence base

9. The Department acknowledged that it could have done more to understand the evidence base of the first National Cyber Security Programme which covered 2011–2016. The Department told us it conducted a 'lessons learnt' exercise, but admitted that with hindsight it could have been more robust than it was.[15] We asked how the Department could be confident that it was making the right decisions about levels of funding and priorities within the Programme without the evidence of what works that a robust lessons learned exercise would have provided.[16] The Department asserted that it had nonetheless learned some valuable lessons from the first programme, the main lesson being that government needed to be more interventionist, and as a result it changed its policy.[17] The Department told us that it had introduced a number of new and innovative projects at the beginning of the 2016–2021 Programme, and that there was continual testing by government of these projects of what worked and what didn't. It similarly told us that it had stopped projects that were not working and took the decision to invest more money into projects, such as active cyber defence, which were working.[18] However, as the National Audit Office observed, while some of the things that are being funded as part of the second cyber security programme are genuinely new and innovative, others are continuations of activities funded as part of the previous cyber security programme. The National Audit Office told us that it would therefore have expected the Department to have had a stronger evidence base for these areas in place to support the second Programme.[19]

10. We similarly asked the Department why it had taken it until 2018, halfway through the current Programme, to introduce a new performance framework. Prior to this, the individual departments that led each of the 12 strategic outcomes included within the Programme reported on progress. The Department told us that the evaluation of each outcome was originally carried out by individual departments to reflect the devolved funding arrangements for the Programme. However, the 2017 National Security Capability Review found that the centre of government needed to have a better overview of the Programme, so performance measurement was centralised in the Department. The Department acknowledged that there are still gaps in its evidence base and told us that it was working to fill these gaps.[20] It told us that there were some areas where there was no evidence for a certain approach to be taken and where a judgement call will need to be made. The Department provided the example of the establishment of the NCSC, for which there was no evidence that the unprecedented step of bringing the secret work of a body like the Government Communications Headquarters (GCHQ) into the open would work.[21] It nonetheless committed to collecting evidence of performance and lessons learned throughout the Programme, and confirmed that it would not wait until 2021 to

[14] Qq 86–89
[15] Qq 68–69, 77–78
[16] Q 105
[17] Qq 68–69
[18] Q86
[19] Q 105
[20] Qq 79–80, 106
[21] Qq 104–107

capture lessons from the current Programme and was already working to capture those lessons on an ongoing basis.[22] Although the Department set out in the Strategy that it would provide annual updates on the progress of the Strategy, is has so far not published any. The Department told us that it intends to start publishing progress reports, the first of which is due to be published in May 2019.[23]

[22] Qq 79–80, 106

[23] Qq 80–81, C&AG's Report para 2.16

2 Planning for the future

Delivery of the Programme to March 2021

11. The Department currently expects to meet just one of the 12 strategic outcomes in the current Strategy by 2021. We asked it to explain why this was the case if it considered that its current approach was working.[24] The Department explained that the Strategy recognised that not all the strategic outcomes would be achieved within its five year timescale, although it hoped it might achieve them all.[25] However, the National Audit Office found that two of the 12 strategic outcomes—'secure by design' and 'science and technology'—have specific objectives that should be met by 2021. The rest are open-ended. The Department explained that its performance measures for each of the outcomes in the Strategy related to the confidence it had in the evidence that the strategic outcome will be achieved, not the actual deliverability of the strategic outcomes.[26] The Department told us it currently has 'low confidence' in the evidence used to assess progress against half the Strategy's 12 strategic outcomes and it only has 'high confidence' in the evidence related to one strategic outcome—which is incident management. The Department acknowledged the weakness of this evidence base, but asserted that some areas of its work, particularly those there were more innovative, were very difficult to measure.[27] For example, it told us that it had a good evidence base for incident response as this is relatively easy to measure. It told us that there were other areas, such as improving the pipeline of cyber skills in the UK, where it will take a number of years for the Department to know whether its interventions in schools, for example, have been successfully delivered.[28]

12. Of the 12 objectives within the Programme, the Department told us that three were on track, and a further eight objectives had 80% or more of their projects on schedule. It told us that while one project had 73% of its projects on track, it was moving in the right direction.[29] We asked the Department how much of the Strategy the Programme was meant to be delivering. The Department explained that the Programme was meant to have a catalytic and transformative impact on both the public and private sector. However, it also told us that there were other projects outside the Programme that will also help deliver the Strategy, including money spent by government departments as part of their business-as-usual work to improve their IT and private sector initiatives and investment in their networks and systems.[30]

13. The Department is still considering its approach to cyber security after 2021, but expected to have a single, portfolio-based business case, rather than its current approach where each of the 12 strategic outcomes of the Strategy has its own, separate business case. The Department expects that it will focus on three elements: improving cyber resilience; continuing to build capability to deal with threats; and making sure that the UK is the safest place in the world to do business online.[31]

[24] Qq 97–101
[25] HM Government, *National Cyber Security Strategy 2016–2021*, p.69, Qq99–100
[26] Qq 101–102, C&AG Report, para 3.14
[27] Q76–77, 101
[28] Q103
[29] Q98
[30] Qq 98–99, 86
[31] Qq 109, 113–119

Protecting consumers

14. Consumers have no way of telling if the online sites they are using or the internet-enabled products they are buying are safe to operate or if companies are following best practice in building in cyber security.[32] For example, a trusted company like British Airways was hacked in 2018, and the personal data of 380,000 of customers was stolen.[33] The Department told us that government had made a range of guidance publicly available on its website covering common cyber security issues, such as the promotion of two-factor identification, where a user requires a second source to verify their identity in addition to a password; and the Cyber Essentials scheme run by the Department for Digital, Culture, Media and Sport that businesses can use. The Department explained that over the past 20 years the web economy has been based on consumers providing their personal data to organisations in return for a service.[34] The NCSC told us that cyber security was not thought of when internet-enabled products were being designed, and Western countries did not really understand the security requirement of evolving technology and is now paying for those mistakes.[35]

15. We asked the Department if there should be a mandatory certification scheme for organisations operating online with regards to cyber security standards. The Department told us that although there is a role for regulation, particularly within the critical national infrastructure sector, it is hard to draw up a list of organisations and specify what they must do as this becomes outdated quickly.[36] It suggested that a different model could be used, similar to the approach the Bank of England has adopted for banks, where it has worked with the NCSC to draw up technical standards that should be built into cyber security regulation by the Bank.[37] The Department also told us that there are some areas where private sector organisations will not invest, or where only government can intervene; for example, the NCSC intercepting spoof emails. In one year the NCSC collected half a billion spoof emails pretending to be HMRC, and these stopped appearing in peoples' inboxes. The NCSC told us that this method has been tested with commercial providers, such as retailers.[38]

16. The NCSC published a guide for SMEs in the 2018 budget, which set out the government's expectation about cyber security measures within these organisations. The Department explained that government does not expect SMEs should have the same defences as larger organisations, but that they should have in placed defences against cyber-attacks that are proportionate to the size of their organisation. However, the Department also pointed out that that many SMEs are in the supply chains of larger organisations and can be a point of entry for cyber hackers. The Department told us that it considered it the responsibility of larger organisations to encourage their supply chains to get basic cyber security right.[39]

17. The Department recognised that, as the internet is a global network, it needs to work closely with international partners when addressing cyber security. We asked the

[32] Qq 74–75
[33] *Forbes*, 'This Is How 380,000 British Airways Passengers Got Hacked'
[34] Qq 74–75
[35] Q 112
[36] Qq 121–122
[37] Q 122
[38] Q 91
[39] Q 123

Department if there were other countries we could learn from in terms of cyber security. It told us that there were not many reliable international indexes, although Canada has a good record in protecting its government networks. The NCSC told us that some countries, including Canada and Australia, are following the UK model. In addition, the NCSC told us that the UK also aims to encourage international organisations to adopt best practice in protecting their networks.[40] We asked the NCSC how it worked in the international arena as the internet is a global network. The NCSC told us that there are three ways of looking at this issue. The first is areas in which the UK can do something either by encouraging—or mandating, where possible—transnational companies to adopt segmented networks rather than flat ones. A flat network allows an attack on a network on one country to expand to other countries—as there is no segmentation of the network. The second is to make UK infrastructure a less attractive target for cyber-attacks by reducing the ability of hackers to operate from within the UK. The third way to work in the international arena to help combat cyber-attacks is to publish evidence of the interventions that the NCSC has made that work and hope that other countries will use them as well.[41]

18. While many of the cyber risks faced by the UK are from outside of Europe, we also heard of an increase in the number of cyber-attacks from within the European Union. We therefore asked the Department about the UK's relationship, and agreements in place, with organisations across Europe that currently help protect the UK from cyber-attacks. The Department told us that its response to the UK leaving the European Union in terms of cyber security will depend on whether the UK leaves with or without a withdrawal agreement in place.[42] It told us that if the UK left without a withdrawal agreement, the existing cyber security measures "will be severed", creating risks that it would have to mitigate against. If the UK leaves with an agreement, then these measures would form part of the agreement that had been reached, although the Department accepted that some areas, such as the UK's access to the second-generation Schengen Information System (SIS II), would require further negotiation as the EU does not yet have the legal instruments to extend capabilities to third countries.[43] The Department told us that the government would like to ensure that access to SIS II is available to the UK and that it would form part of the negotiation with the EU in the implementation period.[44] It told us, however, that it would expect to be able to agree this during the implementation period as "there is strong intent on both sides" to maintain existing access arrangements.

[40] Qq 124–127

[41] Q 127

[42] Q 128

[43] Q 132

[44] Qq 133–134

Formal Minutes

Wednesday 15 May 2019

Members present:

Meg Hillier, in the Chair

Sir Geoffrey Clifton-Brown	Chris Evans
Nigel Mills	Lee Rowley

Draft Report (*Cyber security in the UK*), proposed by the Chair, brought up and read.

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

Paragraphs 1 to 18 read and agreed to.

Introduction agreed to.

Conclusions and recommendations agreed to.

Summary agreed to.

Resolved, That the Report be the Ninety-ninth 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, in accordance with the provisions of Standing Order No. 134.

[Adjourned till Monday 20 May at 3:30pm

Witnesses

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

Monday 1 April 2019

Sir Mark Sedwill, Cabinet Secretary and Head of the UK Civil Service, and UK National Security Advisor, **Madeleine Alessandri**, Deputy National Security Advisor, Cabinet Office, and **Ciaran Martin**, Chief Executive, National Cyber Security Centre. Q1–134

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. The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

Session 2017–19

First Report	Tackling online VAT fraud and error	HC 312 (Cm 9549)
Second Report	Brexit and the future of Customs	HC 401 (Cm 9565)
Third Report	Hinkley Point C	HC 393 (Cm 9565)
Fourth Report	Clinical correspondence handling at NHS Shared Business Services	HC 396 (Cm 9575)
Fifth Report	Managing the costs of clinical negligence in hospital trusts	HC 397 (Cm 9575)
Sixth Report	The growing threat of online fraud	HC 399 (Cm 9575)
Seventh Report	Brexit and the UK border	HC 558 (Cm 9575)
Eighth Report	Mental health in prisons	HC 400 (Cm 9575) (Cm 9596)
Ninth Report	Sheffield to Rotherham tram-trains	HC 453 (Cm 9575)
Tenth Report	High Speed 2 Annual Report and Accounts	HC 454 (Cm 9575)
Eleventh Report	Homeless households	HC 462 (Cm 9575) (Cm 9618)
Twelfth Report	HMRC's Performance in 2016–17	HC 456 (Cm 9596)
Thirteenth Report	NHS continuing healthcare funding	HC 455 (Cm 9596)
Fourteenth Report	Delivering Carrier Strike	HC 394 (Cm 9596)
Fifteenth Report	Offender-monitoring tags	HC 458 (Cm 9596)
Sixteenth Report	Government borrowing and the Whole of Government Accounts	HC 463 (Cm 9596)
Seventeenth Report	Retaining and developing the teaching workforce	HC 460 (Cm 9596)
Eighteenth Report	Exiting the European Union	HC 467 (Cm 9596)

Nineteenth Report	Excess Votes 2016–17	HC 806 (Cm 9596)
Twentieth Report	Update on the Thameslink Programme	HC 466 (Cm 9618)
Twenty-First Report	The Nuclear Decommissioning Authority's Magnox	HC 461 (Cm 9618)
Twenty-Second Report	The monitoring, inspection and funding of Learndirect Ltd.	HC 875 (Cm 9618)
Twenty-Third Report	Alternative Higher Education Providers	HC 736 (Cm 9618)
Twenty-Fourth Report	Care Quality Commission: regulating health and social care	HC 468 (Cm 9618)
Twenty-Fifth Report	The sale of the Green Investment Bank	HC 468 (Cm 9618)
Twenty-Sixth Report	Governance and departmental oversight of the Greater Cambridge Greater Peterborough Local Enterprise Partnership	HC 896 (Cm 9618)
Twenty-Seventh Report	Government contracts for Community Rehabilitation Companies	HC 897 (Cm 9618)
Twenty-Eighth Report	Ministry of Defence: Acquisition and support of defence equipment	HC 724 (Cm 9618)
Twenty-Ninth Report	Sustainability and transformation in the NHS	HC 793 (Cm 9618)
Thirtieth Report	Academy schools' finances	HC 760 (Cm 9618)
Thirty-First Report	The future of the National Lottery	HC 898 (Cm 9643)
Thirty-Second Report	Cyber-attack on the NHS	HC 787 (Cm 9643)
Thirty-Third Report	Research and Development funding across government	HC 668 (Cm 9643)
Thirty-Fourth Report	Exiting the European Union: The Department for Business, Energy and Industrial Strategy	HC 687 (Cm 9643)
Thirty-Fifth Report	Rail franchising in the UK	HC 689 (Cm 9643)
Thirty-Sixth Report	Reducing modern slavery	HC 886 (Cm 9643)
Thirty-Seventh Report	Exiting the European Union: The Department for Environment, Food & Rural Affairs and the Department for International Trade	HC 699 (Cm 9643)
Thirty-Eighth Report	The adult social care workforce in England	HC 690 (Cm 9667)
Thirty-Ninth Report	The Defence Equipment Plan 2017–2027	HC 880 (Cm 9667)
Fortieth Report	Renewable Heat Incentive in Great Britain	HC 696 (Cm 9667)

Forty-First Report	Government risk assessments relating to Carillion	HC 1045 (Cm 9667)
Forty-Second Report	Modernising the Disclosure and Barring Service	HC 695 (Cm 9667)
Forty-Third Report	Clinical correspondence handling in the NHS	HC 929 (Cm 9702)
Forty-Fourth Report	Reducing emergency admissions	HC 795 (Cm 9702)
Forty-Fifth Report	The higher education market	HC 693 (Cm 9702)
Forty-Sixth Report	Private Finance Initiatives	HC 894 (Cm 9702)
Forty-Seventh Report	Delivering STEM skills for the economy	HC 691 (Cm 9702)
Forty-Eighth Report	Exiting the EU: The financial settlement	HC 973 (Cm 9702)
Forty-Ninth Report	Progress in tackling online VAT fraud	HC 1304 (Cm 9702)
Fiftieth Report	Financial sustainability of local authorities	HC 970 (Cm 9702)
Fifty-First Report	BBC commercial activities	HC 670 (Cm 9702)
Fifty-Second Report	Converting schools to academies	HC 697 (Cm 9702)
Fifty-Third Report	Ministry of Defence’s contract with Annington Property Limited	HC 974 (Cm 9702)
Fifty-Fourth Report	Visit to Washington DC	HC 1404 (Cm 9702)
Fifty-Fifth Report	Employment and Support Allowance	HC 975 (Cm 9702)
Fifty-Sixth Report	Transforming courts and tribunals	HC 976 (Cm 9702)
Fifty-Seventh Report	Supporting Primary Care Services: NHS England’s contract with Capita	HC 698 (Cm 9702)
Fifty-Eighth Report	Strategic Suppliers	HC 1031 (Cm 9702)
Fifty-Ninth Report	Skill shortages in the Armed Forces	HC 1027 (9740)
Sixtieth Report	Ofsted’s inspection of schools	HC1029 (Cm 9740)
Sixty-First Report	Ministry of Defence nuclear programme	HC 1028 (Cm 9740)
Sixty-Second Report	Price increases for generic medications	HC 1184 (Cm 9740)

Sixty-Third Report	Interface between health and social care	HC 1376 (Cm 9740)
Sixty-Fourth Report	Universal Credit	HC 1375 (Cp 18)
Sixty-Fifth Report	Nuclear Decommissioning Authority	HC 1375 (Cp 18)
Sixty-Sixth Report	HMRC’s performance in 2017–18	HC 1526 (Cp 18)
Sixty-Seventh Report	Financial Sustainability of police forces in England and Wales	HC 1513 (Cp 18)
Sixty-Eighth Report	Defra’s progress towards Brexit	HC 1514 (CP 18)
Sixty-Ninth Report	Sale of student loans	HC 1527 (Cp 56)
Seventieth Report	Department for Transport’s implementation of Brexit	HC 1657 (Cp 56)
Seventy-First Report	Department for Health and Social Care accounts	HC 1515 (Cp 56)
Seventy-Second Report	Mental health services for children and young people	HC 1593 (Cp 79)
Seventy-Third Report	Academy accounts and performance	HC 1597 (Cp 79)
Seventy-Fourth Report	Whole of Government accounts	HC 464 (Cp 79)
Seventy-Fifth Report	Pre-appointment hearing: preferred candidate for Comptroller and Auditor General	HC 1883 (Cp 79)
Seventy-Sixth Report	Local Government Spending	HC 1775 (Cp 79)
Seventy-Seventh Report	Defence Equipment Plan 2018–28	HC 1519 (Cp 79)
Seventy-Eighth Report	Improving Government planning and spending	HC 1596
Seventy-Ninth Report	Excess Votes 2017–18	HC 1931
Eightieth Report	Capita’s contracts with the Ministry of Defence	HC 1736
Eighty-First Report	Rail management and timetabling	HC 1793
Eighty-Second Report	Windrush generation and the Home Office	HC 1518
Eighty-Third Report	Clinical Commissioning Groups	HC 1740
Eighty-Fourth Report	Bank of England’s central services	HC 1739
Eighty-Fifth Report	Auditing local government	HC 1738

Eighty-Sixth Report	Brexit and the UK border: further progress review	HC 1942
Eighty-Seventh Report	Renewing the EastEnders set	HC 1737
Eighty-Eighth Report	Transforming children’s services	HC 1741
Eighty-Ninth Report	Public cost of decommissioning oil and gas infrastructure	HC 1742
Ninetieth Report	BBC and personal service companies	HC 1522
Ninety-First Report	NHS financial sustainability: progress review	HC 1743
Ninety-Second Report	Crossrail: progress review	HC 2004
Ninety-Third Report	Disclosure and Barring Service: progress review	HC 2006
Ninety-Fourth Report	Transforming rehabilitation: progress review	HC 1747
Ninety-Fifth Report	Accessing public services through the Government’s Verify digital system	HC 1748
Ninety-Sixth Report	Adult health screening	HC 1746
Ninety-Seventh Report	Local Government Governance and Accountability	HC 2077
Ninety-Eighth Report	The apprenticeships programme: progress review	HC 1749
First Special Report	Chair of the Public Accounts Committee’s Second Annual Report	HC 347
Second Special Report	Third Annual Report of the Chair of the Committee of Public Accounts	HC 1399