House of Commons
Science and Technology Committee

Digital Government

Eighteenth Report of Session 2017–19

Report, together with formal minutes relating to the report

Ordered by the House of Commons to be printed 3 July 2019

HC 1455
Published on 10 July 2019
by authority of the House of Commons

Science and Technology Committee

The Science and Technology Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Government Office for Science and associated public bodies.

Current membership

Norman Lamb MP (*Liberal Democrat, North Norfolk*) (Chair)

Vicky Ford MP (*Conservative, Chelmsford*)

Bill Grant MP (*Conservative, Ayr, Carrick and Cumnock*)

Mr Sam Gyimah MP (*Conservative, East Surrey)*

Darren Jones MP (*Labour, Bristol North West*)

Liz Kendall MP (*Labour, Leicester West*)

Stephen Metcalfe MP (*Conservative, South Basildon and East Thurrock*)

Carol Monaghan MP (*Scottish National Party, Glasgow North West*)

Damien Moore MP (*Conservative, Southport*)

Graham Stringer MP (*Labour, Blackley and Broughton*)

Martin Whitfield MP (*Labour, East Lothian*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO. No. 152. These are available on the internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website at www.parliament.uk/science 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: Danielle Nash (Clerk), Zoë Grünewald (Second Clerk), Dr Harry Beeson (Committee Specialist), Jocelyn Hickey (Committee Specialist), Sonia Draper (Senior Committee Assistant), Julie Storey (Committee Assistant), and Joe Williams (Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Science and Technology Committee, House of Commons, London SW1A 0AA. The telephone number for general inquiries is: 020 7219 2793; the Committee's e-mail address is: scitechcom@parliament.uk.

You can follow the Committee on Twitter using @CommonsSTC.

Contents

Summary

In 2011, the UK Government created the Government Digital Service (GDS) to sit within the Cabinet Office. It was created to implement the then Government's "digital by default" strategy. The core purposes of GDS were to: save money; centralise information via a single website; and improve the user experience of Government. In 2017, the UK Government announced its intentions to transform its operations in the *Government Transformation Strategy*, which sought to use technology to transform Government, making it more responsive to change and the needs of citizens, and putting more power into the hands of the citizen.

The UK Government has consistently been placed in the top five in the United Nations e-Government survey. In 2016 the UK was ranked number one in this survey, but fell to fourth behind Denmark, Australia and South Korea in 2018. In our inquiry we heard concerns that the UK had lost momentum in its digitisation agenda.

The UK Government can learn from other international examples of best practice, such as Estonia where citizens have a single unique identifier. We conclude that single unique identifiers for citizens can transform the efficiency and transparency of Government services. We welcome the Government's announcement in June 2019 that it will consult shortly on digital identity. While we recognise that in the UK there are concerns about some of the features of a single unique identifier, as demonstrated by the public reaction to the 2006 Identity Card Act, we believe that the Government should recognise the value of consistent identity verification. The Government should facilitate a national debate on single unique identifiers for citizens to use for accessing public services along with the right of the citizen to know exactly what the Government is doing with their data.

We find in this Report that data-sharing is key to ensuring that digital Government can be transformative. It enables departments to work together to produce efficient public services that work for the citizen, thus improving the citizen-Government relationship. We welcome the Government commencing phase one of developing its National Data Strategy. DCMS should conduct an audit of data-sharing amongst Government departments to see where best practice is taking place, and identify which departments are particularly siloed. This audit should be completed and published in advance of the National Data Strategy being published in Winter 2020.

We welcome the steps that the Government has taken to enhance public trust in data use, including the establishment of the Centre for Data Ethics and Innovation. However, we are concerned that the Government might be taking an overly-cautious approach and second-guessing citizens' views on how their data should be used. DCMS should ensure that the Centre for Data Ethics and Innovation annually assesses public opinion on Government data use. This review should start in summer 2019 and should aim to report by Spring 2020.

Leadership of the digital Government agenda and a loss of momentum were recurrent themes within our evidence. We conclude that political leadership in digitisation has been lacking in recent years since Francis Maude ceased being Minister for the Cabinet Office. This, coupled with the departure of senior Civil Service figures in

GDS, has resulted in a slowing in the Government's digital momentum, as evidenced by other countries overtaking the UK in international rankings. To address this issue, we propose that the Government should introduce a ministerial digital champion in every department by the end of 2019 who has responsibility for using innovation and digitisation to transform the way their department operates.

Concern was also raised about the role of GDS. Although GDS made good progress in its early years on standards and platforms that applied across Government, we heard how GDS has "lost its way somewhat" and its purpose is now less clear. GDS's purpose should be twofold: to provide advice to departments when needed, but also to devise and enforce minimum standards to be applied consistently across Government digital services. Departments, with the relevant capacity, should retain the ability to develop platforms and software.

In April 2018 responsibility for data policy and governance was moved to DCMS from the Cabinet Office/Government Digital Service. It is too early to tell if the move of data policy to DCMS presents a challenge or an enhancement for Government digitisation. We urge the Government to keep under review whether DCMS should be the lead department for open data and data ethics, governance and sharing and set out whether DCMS requires any additional powers to drive data reform across Government. If it does not deem this necessary it should set out why.

Further, we heard that legacy systems present a significant barrier to effective Government transformation and digitisation. We acknowledge the attempts of the Government, its predecessors and individual departments to produce guidance and to deal with legacy issues. However, the same issues frequently recur, suggesting that the Government and GDS's advice has not been fully implemented. We acknowledge that there is a significant cost attached to the replacement of legacy systems, which the Treasury must resource adequately. We recommend that GDS conduct an audit of all legacy systems across Government, including where they are based, what actions to take, the expected cost of such action and the resulting timescales. GDS's framework of retain (do nothing), retire (drop), re-host (lift and shift), repurchase (shop and drop), re-platform (life and shape) should be used to determine what actions to take with each legacy system. The audit should assess which approach is most realistic but 'retain' should not be used widely as the proposed action in the long-term as there is clear evidence that the legacy system issue is going to increase over time and there are challenges with regard to the skills for supporting such systems.

Responsibility in Government for cyber security policy is spread between departments to ensure checks and balances are in place, but we are concerned that this may result in a lack of accountability for specific incidents. We support the 2018 recommendation of our colleagues on the Joint Committee on the National Security Strategy that there should be a Minister for Cyber Security.

Shortage of digital skills is an issue that affects the digital workforce in both the public and private sector. The Government, including GDS, has made good attempts to tackle the digital skills shortage, through academies, creating job roles and considering progression pay. Nonetheless, more action is needed. The Government should publish a strategy by mid-2020, covering how it intends to make digital skills sustainable.

Another factor which impacts the Government's ability to transform is procurement. The Government has introduced initiatives, such as G-Cloud, the Digital Marketplace and the GovTech Catalyst Fund, to try and open up digital/IT procurements to a broader pool of bidders. These have helped to partially overcome some barriers involved in procurement, including engagement with SMEs. However, further innovation in procurement is needed to encourage involvement from start-ups and SMEs so that their strengths can be drawn on to enable transformation. In this Report we recommend several actions, including:

- The Crown Commercial Service consulting on the accessibility of the current Government technology procurement framework; and
- An increase to the funding available through the GovTech Catalyst Fund.

1 Introduction

Digital Government in the UK

1. The UK Government Digital Service (GDS) was created in March 2011 to sit within the Cabinet Office. It was created to implement the then Government's "digital by default" strategy, which had been proposed by the 2010 Report *Directgov Strategic Review*, requested by the Permanent Secretary of Government Communications and the Digital Champion's team.[1] Martha Lane Fox, the Government Digital Champion (2009–2013) and co-founder of lastminute.com, used that Report to inform her review of DirectGov. Her accompanying letter to the Report, *Directgov 2010 and beyond: revolution not evolution*, recommended a "radical overhaul" of the Government's online services to make it fit for purpose of the requirements of the citizen and the State.[2] The core purposes of GDS, as set out in the 2012 Cabinet Office Report *Government Digital Strategy*, were to:

- "save money";
- centralise information via a single website; and
- improve the user experience of Government.[3]

The Government Digital Service (GDS) is just one part of the UK's digital Government ecosystem. Another big component is the Government's website, GOV.UK. The public sector information website, GOV.UK, was formally launched in October 2012, officially replacing Directgov and Business Link, as the new online platform for Government departments and public bodies. Now, all 25 ministerial and 20 non-ministerial departments, as well as 406 other public sector organisations, such as the Council for Science and Technology, make use of GOV.UK.[4]

2. In 2017, the UK Government announced its intentions to transform its operations in the *Government Transformation Strategy*, which sought to:

- "transform Government through technology";
- create a "responsive State that can change at pace and at scale"; and
- transform "the relationship between citizens and the State - putting more power in the hands of citizens and being more responsive to their needs."[5]

The benefits that the Government could achieve for the citizen with this new approach were:

- Coherent and accessible services for citizens and businesses;
- Immediacy of service provision;
- Saving of public money and increased efficiency of service provision;

[1] Transform, Directgov Strategic Review, (September 2010)
[2] Martha Lane Fox, Directgov 2010 and beyond: revolution not evolution, (October 2010)
[3] Cabinet Office, Government Digital Strategy, (November 2012)
[4] GOV.UK, "Departments, agencies and public bodies", accessed 3 July 2019
[5] The Cabinet Office, Government Transformation Strategy, February 2017

- Improving the trust between the citizen and the State; and
- Enhanced security of data.[6]

In this Report we will consider the extent to which these aims have been achieved.

How does the UK digital Government perform internationally?

3. In 2018, the Organisation for Economic Co-operation and Development (OECD) emphasised the importance of Governments across the world harnessing digital technologies in order to adjust to the "changing expectations and needs" of modern societies.[7] In practice, meaning that their services were digital by design, data-driven, user-driven and proactive in policy making.[8] They set out the power of digital to transform Government services and to put the citizen at the heart of what the Government does:

> This transformation requires governments to take a user-driven approach, empowering citizens and business to interact and collaborate with the public sector to determine and address their own needs.[9]

4. The UK Government has generally been placed in the top five in the United Nations e-Government survey, in which three qualities are measured:

- the adequacy of telecommunication infrastructure;
- the ability of human resources to promote and use Information Communication Technology; and
- the availability of online services and content.[10]

In 2016 the UK was ranked number one in this survey, but fell to fourth behind Denmark, Australia and South Korea in 2018. This decline in rankings was anticipated in a March 2017 NAO Report, *Digital Transformation in Governmen*t, which identified areas where progress had slowed. For example, it attributed the low uptake of GOV Verify by departments to an overall slower adoption of Government services.[11] This issue will be explored further at paragraph 20. Further, in June 2017, a Report from the Institute for Government, an independent think tank looking at how to make the Government more effective, found that "the spread of new digital services for the public had been slower than planned" and that a cyber-attack that hit the NHS demonstrated "the fragility of some of the systems being used in the public sector".[12] Consequently, we decided to launch an inquiry to assess the extent to which UK digital Government had resulted in transformative change; saved public money; increased trust between the citizen and the state; and optimised service delivery to citizens.

[6] The Cabinet Office, Government Transformation Strategy, February 2017

[7] OECD, "Executive summary", Digital Government Review of Morocco: Laying the Foundations for the Digital Transformation of the Public Sector in Morocco, July 2018, p 11

[8] OECD, "Strengthening Digital Governments" OECD Going Digital Policy Note, 2018

[9] OECD, "Executive summary", in Digital Government Review of Morocco: Laying the Foundations for the Digital Transformation of the Public Sector in Morocco, July 2018, p 11

[10] United Nations, "e-Government Survey 2018", July 2018

[11] National Audit Office, "Digital transformation in Government", (March 2017), p 11

[12] Institute for Government, "Improving the management of digital government", (March 2017), p 2

Our inquiry

5. We launched a call for written submissions in July 2018. We sought submissions that addressed the following terms of reference:

- The progress of Government digital services, the areas where further development is particularly needed, and how well the UK compares with other countries.
- How well Government digital services are protected from cyber attacks.
- How well the Government Digital Service (GDS) has helped spread the use of digital services across Government, including promoting the use of new technologies and uses of data.
- The digital skills capacity in Government departments and agencies, to be able to deliver effective digital services to the public and businesses.
- How well the Government and its agencies deploy their datasets to maximise their value for money, effectiveness and delivery of digital services.
- The extent to which Government datasets are made available to private-sector and academic service developers, and how well its 'open data' arrangements are operating.
- The implications and opportunities for GDS arising from Brexit, including areas where the nature of digital services may have to change.
- The implications for GDS following the move of its data policy and governance functions from the Cabinet Office to the Department for Digital, Culture, Media and Sport.

6. We received 30 written submissions from a variety of sources, including Government departments, members of the public, technology companies, universities and data rights groups. We held four oral evidence sessions, including evidence from the then Director General of the Government Digital Service, Ministers, academics and technology experts from the private sector. The evidence that we received is available on our website.

7. In addition, we held a roundtable event with GovTech small-medium enterprises and start-ups (see Annex one), where we heard their perspectives and experiences of Government technology procurement frameworks. We had been hoping to visit Estonia but due to the uncertainty of UK parliamentary business in the Spring, this was not possible. Instead, the Chair had a private meeting with the Estonian Ambassador and a representative from the e-Estonia showroom to discuss Estonian digital successes (see Annex two). The Chair also met with HMRC's Chief Digital and Information Officer, Jacky Wright, to discuss the work that HMRC had undertaken to digitise (see Annex three). To further assist with our inquiry, we appointed Dr Jerry Fishenden, visiting Professor at the University of Surrey, as a Specialist Adviser for this inquiry.[13] We are grateful to all those who contributed to our inquiry.

[13] Dr Jerry Fishenden declared his interests on Tuesday 13 November 2018

Aims of this Report

8. In this Report we make recommendations relating to what the Government should do to ensure that it takes full advantage of the opportunities that arise from digitisation. Specifically:

- In Chapter 2, we outline a rationale for our understanding of digitisation, and present the case study of Estonia, as an example of a State that has transformed its relationship with the citizens through the use of technology, as well as drawing lessons and recommendations for the UK Government from the Estonian digital Government model.
- In Chapter 3, we consider the extent to which the Government has successfully employed digital levers of transformation, including data and innovative technologies.
- In Chapter 4, we assess the cultural challenges to digitisation, specifically leadership and momentum.
- In Chapter 5, we explore the technical challenges of legacy systems and security in digitisation.
- Finally, in Chapter 6, we analyse the institutional challenges of procurement frameworks and digital skills in Government.

2 Government digitisation

9. This Chapter sets out the concept and purpose of digitisation, as well as the success of the Government to date in transforming through technology. Further, this Chapter sets out the Estonian digital Government model and highlights what the UK Government could learn from it.

Transformation through digitisation

10. In the *Government Transformation Strategy*, published in 2017, the Government set out three goals for how it intended to use technology and digitisation to improve Government:

- To "transform Government through technology";
- To create a "responsive State that can change at pace and at scale"; and
- To transform "the relationship between citizens and the State - putting more power in the hands of citizens and being more responsive to their needs."[14]

11. We took our definition of digitisation from a 2018 report from the Institute for Government (IfG), *The hidden obstacles to government digital transformation*.[15] In its report, the IfG made the distinction between digital transformation and digital programmes, where digital programmes "mainly focus on improving citizen's website experience", whilst digital transformation meant "more profound shifts in the way government departments operate and even with reshaping operating models across departmental boundaries when there are benefits for citizens from joining up services."[16] This difference is in the end-to-end digitisation of services, as opposed to front-end optimisation.

12. This view was also shared by technology transformation consultancy company, PUBLIC, who explained that digital was understood by the public sector and the Government as "deep internal departmental change, and a core shift in how public bodies operate".[17] As such, PUBLIC viewed technology as a disruptive method for entering a new era of Government, transforming both policy and delivery of services to create "smarter governments around the world."[18]

13. This view was also shared by the Minister for Implementation, Oliver Dowden MP. When asked how he would characterise digital, he explained that digital "is not somebody taking something that is produced digitally, printing it out, processing it and then sending someone an email at the end" but that the challenge is how we ensure "end to end digitisation".[19] This understanding of digital is similar to the IfG definition of digitisation, as going beyond online platforms to using digital to transform the way departments operate.

[14] The Cabinet Office, "Government Transformation Strategy", (February 2017), p 21

[15] Institute for Government, "The hidden obstacles to government digital transformation" (October 2018)

[16] Institute for Government, "The hidden obstacles to government digital transformation" (October 2018), p 5

[17] PUBLIC (DIG0027) para 11

[18] PUBLIC (DIG0027) para 2

[19] Q396

14. The Government defined a "digital transaction" as "those lodged by a customer through a digital channel. Once received some of these transactions are processed automatically whilst others require manual intervention and subsequently incur greater costs."[20]As such, when assessing the evidence of the Performance Dashboard, a tool that records which services are online and their level of take-up, it did not distinguish services which had delivered against the Minister's ambition of "end-to-end digitisation", nor did it distinguish services, as per our preferred definition, that were digitised in a way that transformed how these service were delivered.[21] It simply recorded services for which an element of the process was digital, which could involve downloading, completing and printing the form to submit, or, in the case of the second most used 'digital service' on the list, the Home Office arrangements for passenger arrival at the UK border, simply a publication of the number of people entering the UK.[22] Further, much of the data on the dashboard no longer seems to be updated, despite section 10 of the GDS Service Standard, last updated in 2017, which advocated the publication of such data: "publishing performance data means that you're being transparent about the success of services funded by public money. And people can make comparisons between different government services".[23]

15. **The open-ended definition of "digital" has meant that it is hard to assess the full scale of any progress that the UK Government has made with its digitisation agenda. We believe that Government digitisation should be defined as transforming how services are delivered so that the relationship between the citizen and the State is enhanced.** ***The Government should adopt this definition and set out metrics of success. Departments and associated Agencies should be required to publicly report against these metrics on an annual basis, starting from the financial year 2020/21, highlighting areas of success and areas for improvement. The Cabinet Office should be responsible for overseeing departments' action plans in response to this annual publication.***

Levers for digitisation

16. What this definition of digitisation means in practice is a matter of debate. Though we did not put the IfG definition of digitisation to our witnesses, the themes in the evidence can be related to this definition. For example, the evidence, including that from Deloitte, the Cabinet Office and Mr David Moss, explained how data could be used to join up Government departments, saving money and time, and producing a better experience for the citizen through the joining up of data sets and creating a more efficient and comprehensive profile for departments to work from.[24] We also heard that the efficient use of data was a major feature of the Estonian digital Government model, an issue that we will be explored in greater detail in this Chapter.

17. Much of the evidence also explained how innovative technologies could be used to enable transformation. We heard from the Alan Turing Institute and Deloitte, for example, about how Artificial Intelligence could be used to transform specific services so they were faster and more efficient.[25] The Minister for the Cabinet Office also explained ways in

[20] GOV.UK, "Land registry: searches of whole register", accessed 3 July 2019
[21] GOV.UK, "Performance", accessed 3 July 2019
[22] GOV.UK, "Passenger arrivals at the UK border", accessed 3 July 2019
[23] GOV.UK, "Service Standard", accessed 3 July 2019
[24] Deloitte LLP (DIG0014); Cabinet Office (DIG0023); Mr David Moss (DIG0013)
[25] The Alan Turing Institute (DIG0005) para 5; Deloitte LLP (DIG0014) para 31

which the Government's GovTech Catalyst programme had used innovative technologies to solve policy delivery issues, such as cutting congestion and tackling rural isolation and loneliness.[26] Innovative technologies will be explored in further detail in Chapter 3.

Progress

18. As set out at paragraph 1, the beginning of the digital transformation period was characterised by the creation of the Government Digital Service in 2011, on the back of the Martha Lane Fox review. The first blogpost once GDS had launched set out its priorities and explained that GDS would become the new centre for digital Government in the UK, championing a culture of digital throughout Government that put the user first and delivered cheaper, more efficient services.[27]

19. A former Deputy Director of GDS, Tom Loosemore, told us that the aims of digitisation during the establishment of GDS were improving service delivery, and improving communications between citizens and the Government.[28] This was demonstrated by the creation of the "Government as a Platform" concept in 2013. This can be illustrated by the creation of a host of technology products that departments could use, which would ease interactions between departments and the citizen, and standardise delivery across Government. These shared platforms included GOV.UK Pay, GOV.UK Notify, GOV.UK Platform as a Service, GOV.UK Registers, GOV.UK Verify.[29]

20. The Cabinet Office explained that these platforms had been successful: "adoption of these platforms has increased substantially over the past year, and it is expected to accelerate further over the coming years".[30] The Institute for Government (IfG) also pointed to the growth in use of GOV Pay and GOV Notify, and praised the successes of GOV.UK as a central Government website, becoming an international exemplar across the world.[31] However, the IfG was critical of GOV.UK Registers and GOV.UK Verify as there had been a lack of incentives for departments and citizens alike to use Verify, and that Registers had lacked strategic focus on getting the basic data infrastructure right.[32] Further, the Public Accounts Committee concluded in 2019 that Verify had been unsuccessfully implemented, was badly designed, and had technical difficulties that lacked the necessary departmental and leadership buy-in.[33] GlobalData and Mr David Durant, both explained that Government as a Platform had failed to reach its full potential due to an absence of leadership and political will.[34] We explore further challenges of leadership in Chapter 4.

[26] Cabinet Office (DIG0023) para 59

[27] GDS, "Introducing the Government Digital Service", March 2011

[28] Q7

[29] A secure way to pay for Government services online; a way for service teams across Government to keep people updated by sending text messages, emails or letters; hosting for services on a Government cloud platform so departments aren't duplicating digital infrastructure; helping Government design and build services on consistent data infrastructure; a secure way for citizens to prove their identity to Government online.

[30] Cabinet Office (DIG0023) para 30

[31] Institute for Government, Digital, "Whitehall Monitor 2019" (2019)

[32] Institute for Government, Digital, "Whitehall Monitor 2019" (2019)

[33] Public Accounts Committee, Ninety-Fifth Report of Session 2017–19, Accessing public services through the Government's Verify digital system, HC 1748, paras 1–6

[34] GlobalData Public Sector (DIG0024) para 2; Mr David Durant (DIG0020) para 7

21. In addition to Government as a Platform, GDS published the *Government Digital Strategy* in 2012, which set out the Government's plans to improve digital capabilities throughout Government, increase the number of citizens using online services and make sure Government services were consistent and coherent, using common standards and platforms across departments. The aim of this was to create a more consistent experience of Government for the citizen. A 2017 NAO report, *Digital transformation in Government,* emphasised the success of GDS in doing this, particularly in its creation GOV.UK as a centralised Government website, as well as its spreading of common standards and guidance across departments.[35]

The Government-citizen relationship

22. According to the OECD (Organisation for Economic Co-operation and Development), digitising Government not only improves service delivery and public sector efficiency, but it can also give rise to new forms of public engagement and collaborative relationships, moving from "citizen-centric" approaches to "citizen-driven" approaches.[36] The OECD explained in 2014 in *Recommendation of the Council on Digital Government Strategies*, that if digital technologies were harnessed they could strengthen the relationship between the citizen and the State; they advocated that governments could and should use technology to strengthen citizen trust, and create more agile, resilient and forward-looking public institutions that performed better and more responsively for the citizen.[37] Evidence from Professor Helen Kennedy referenced the importance of citizen trust in ensuring that digital Government was utilised to its full potential, due to the need for efficient and transparent use of citizen data for better services.[38]

23. Estonia's approach to data and citizen identification was an area that we recognised as a useful case study for our inquiry. Estonia operates a "consent" model in its utilisation of citizen data, where citizens are fully informed about how their data is being used by the Government. Every citizen in Estonia has a profile of basic personal data that allows them to interact with the Government quickly without incurring the inconvenience and cost of contacting multiple Government departments. Citizens can access all the data the Government holds on them through a State portal using an identity card and they can make updates and corrections. The Personal Data Protection Act in Estonia created a framework that allowed people control over their data, such as restricting who could view it. It fostered a consent model.[39] This meant that certain sensitive personal information, such as ethnicity, State of residence and sexuality, could only be viewed by a government department if the citizen had given consent. This consent could also be conditional on circumstance. For example, a citizen could change whether a department could view their data or information at any time. Sam Smith, representing medConfidential, said that it was wrong to call the Estonian model a "consent" model, and in fact it should be regarded as a transparency model.[40] He explained that this was because being able to access Government services did not equate to true consent because it was a conditional on

[35] National Audit Office, "Digital transformation in Government", (March 2017), para 15

[36] OECD, " Recommendation of the Council on Digital Government Strategies" (July 2014), para 2

[37] OECD, " Recommendation of the Council on Digital Government Strategies" (July 2014), para 7

[38] Q111

[39] Personal Data Protection Act 2007, RT I 2007, 24, 127

[40] Q 107

sharing one's data. However, the Minister for Digital and the Creative Industries, Margot James MP, told us that both the Estonian model and GDPR did equate to consent models, as they were "opt-in" systems, and such consent was given.[41]

24. Under the Estonian model, the Government has implemented a comprehensive electronic ID system, covering 94% of the population. It was recognised by the World Bank as one of the most advanced digital States in the world according to a Digital Dividends Report from 2015.[42] Peter Herlihy, who worked on Digital Strategy at GDS in 2013, called Estonia "the most joined up digital government in the world".[43] Estonia's use of single unique identifiers, in the form of electronic ID Cards has allowed citizens to interact efficiently and directly with the Government. Citizens could verify their identity securely in a matter of seconds to access a range of Government services, including e-Banking, libraries, medical records, tax history, e-Prescriptions, i-Voting and digital signatures.[44] Dr Helen Margetts, representing the Alan Turing Institute, told us that "the key problem the UK has" is the lack of unique digital identifiers, and that one of the good things about Estonia's system was its use of these unique identifiers and secure data interchanges between registries.[45] Peter Wells from the Open Data Institute encouraged caution at the prospect of single unique identifiers, explaining that he did not believe it was necessary for some departments to be able to access all his data, including that which was irrelevant to the department's purpose.[46] Discussion on single digital identifiers will be explored in more detail at paragraph 29.

25. Whether the UK can learn lessons from Estonia is arguably called into question by the most recent UN e-Government ranking, which measured the use of ICT to deliver public services. In this, the UK came fourth behind Denmark, Australia and the Republic of Korea, whilst Estonia came sixteenth.[47] However, in an academic paper published by witness Helen Margetts from the Alan Turing Institute, she explained that e-Government rankings may not necessarily give a true indication of the most advanced and exemplary digital States:

> E-government rankings are well known for their methodological weaknesses and inconsistencies and Estonia's place in international rankings has not reflected the country's reputation […] these rankings include many other elements outside eGovernment (such as business and innovation environment) and when public services or infrastructure are singled out, Estonia has consistently done well in indicators like the 'social impact of ICTs in public services', as in the World Economic Forum network readiness index.[48]

26. Further, there are questions surrounding the feasibility of the UK in producing a similar system of data-sharing to that of Estonia. A number of witnesses, including SAS and Deloitte, pointed out that the UK faced a barrier of societal distrust of the Government's

[41] Q436
[42] e.Estonia.com, "e-Estonia: the epic story of the e-State", (2018), p 14
[43] Peter Herlihy, "'Government as a data model': what I learned in Estonia", Government Digital Service, (October 2013)
[44] e.Estonia.com, "e-Estonia: the epic story of the e-State", p.18
[45] Q 276
[46] Q 277
[47] United Nations, "e-Government Survey 2018", July 2018
[48] Helen Margetts and Andre Naumann, "Government as a Platform: What can Estonia show the world?", Oxford Institute, (2017), p 7

use of data.[49] The written submission from SAS (Statistical Analysis System), a software suite for advanced analytics, suggested that part of the reason that UK citizens had minimal trust in the Government was due to "nervousness" from citizens about the way governments were using their personal data.[50] Similarly, Deloitte explained:

> The UK has a history of societal aversion to "big state" government. According to Deloitte's Global Mobile Consumer Survey, 80% of respondents are concerned or fairly concerned about sharing their data. This limits the UK's ability to move quickly on cross-cutting digital transformation, such as across the health and social care sector.[51]

27. The recent results from the Edelman Trust Barometer mirror the concerns of Deloitte and SAS. The Edelman Trust Barometer measures levels of citizens trust across different countries annually. In its 2019 study, the Barometer highlighted a flatline trend on the trust of citizens in the UK, with 44% of the public identifying the Government as the "most broken institution".[52] The Barometer further highlighted that the UK had some of the lowest scoring levels of trust internationally at 43%, behind Germany (44%), France (44%), US (49%), Italy (46%), Australia (48%), and many others with similar political systems.[53] In addition to this, a 2017 study by the UK Information Commissioner's Office revealed that less than half (49%) of Britons trusted the Government with storing their personal data.[54]

28. However, many witnesses, such as Helen Kennedy from the University of Sheffield and Sam Smith from medConfidential pointed out that rather than a lack of trust being seen as a barrier to the UK implementing data intensive transformation as Estonia had, a push for transformative digitisation could be seen as a means to improve the Government-citizen relationship and levels of trust. Helen Kennedy, viewed the transparent use of a data as a means for the Government's ability to improve relations.[55] Further, Sam Smith argued that the UK could learn valuable lessons from Estonia in enhancing trust between the citizen and the Government, as when Estonia built its digital State in the 1990s, the populace had a "fear of the State", and the solution was for the Government to say "the State will be able to do a number of things, but you will be able to see anything that the State does with access to your data."[56] UKCloud also pointed to the benefits that further data transparency would provide.[57]

Single unique identifiers

29. As previously explained at paragraph 24, one particular way in which Estonia transformed the relationship between the citizen and State was through the use of a single unique identifier. In practice, this meant that citizens could access Government services quickly and securely, through an ID card that gave individuals and departments access to all their citizens' personal information. Some of the written submissions we

[49] SAS (DIG0015) para 4
[50] SAS (DIG0015) para 4
[51] Deloitte LLP (DIG0014) para 10
[52] Edelman, "EDELMAN TRUST BAROMETER 2019 – A DISUNITED KINGDOM" (2019), p 2
[53] Edelman, "The 2019 Edelman Trust Barometer: Global Report", (2019), p 6
[54] ICO "ICO survey shows most UK citizens don't trust organisations with their data" (November 2017)
[55] Qq89–91
[56] Q100
[57] UKCloud Ltd (DIG0008) para 5

received such as those from GlobalData, Helen Margetts from the Alan Turing Institute and 360Giving were supportive of the suggestion of having a single unique identifier in the UK.[58] GlobalData, a global data analytics company, explained that "whilst ID cards were a political hot-potato, a single digital identity for each citizen could have provided the foundations for better data-sharing and faster transformation".[59] Further, 360Giving advocated that the Government should adopt single unique identifiers for organisations and processes across key datasets to produce more efficient, cost-effective use of data.[60] Dr Helen Margetts also spoke in favour of digital identifiers as a means of improving public services and making datasets more accessible, stating that "less is more in the case of digital identifiers, and reviving the idea of data registries and a digital identifier is something to think about."[61]

30. However, some evidence, including from medConfidential, was cautious about the use of single unique identifiers, which, in effect, was akin to the implementation of ID cards.[62] medConfidential, for example, was concerned about the prospect of identity cards for citizens, calling it one of the "worst traditions" of the Government, during 2001 to 2010.[63] Though ID cards and single unique identifiers are not identical, it is important to note how the centralisation of data and worries over access to it have concerned the public in the past. In May 2018, a YouGov survey revealed that 57% of the British public would support the reintroduction of ID cards.[64] However, when the original Identity Card Act 2006 was repealed, it showed that support for the Bill from the public had decreased as time had gone by. A poll by the ICM indicated that between 2003 and 2006, public support for ID cards had dropped from 61% to 46%.[65]

31. The 2006 Identity Card Act was repealed in 2010. In 2005, the then Joint Committee on Human Rights questioned the compatibility of the Bill with the European Convention on Human Rights, specifically with regard to Article 8 (the right to respect for private life) and Article 14 (the right to non-discrimination).[66] In 2004, Richard Thomas from the Information Commissioner's Office explained that ID cards could result in the UK's "sleepwalk[ing] into a surveillance society".[67] The then Home Affairs Committee in 2008 expressed concern that ID cards could be subject to "function creep", and that citizens would not have a say over how their data was being shared and with whom, if further functions were to develop incrementally.[68]

32. Former GDS employee, Mr David Durant, recognised the political controversy surrounding ID Cards, but recommended an approach to single unique identifiers where citizen data would be treated in a similar way to the Estonian system.[69] This would mean that key data fields would not be centrally stored, but just duplicated across departments to reduce the security risks and ethical concerns surrounding centralisation. Further, the

[58] GlobalData Public Sector (DIG0024) para 13; Q276; 360Giving (DIG0019) para 7
[59] GlobalData Public Sector (DIG0024) para 13
[60] 360Giving (DIG0019)
[61] Q276
[62] medConfidential (DIG0028) para 70
[63] medConfidential (DIG0028) para 70
[64] Matthew Smith, "Majority of Brits support introducing ID cards", YouGov, (2012)
[65] ICM, "ID Card Survey", (2006)
[66] Joint Committee on Human Rights, Eight Report of the Session 2004–2005, Scrutiny: Fourth Progress Report, HC 388, p 3
[67] BBC, "Britain is 'surveillance society'" (November 2006),
[68] Home Affairs Committee, Fourth Report of the Session 2003–2004, Identity Cards, HC130-I, para 152–159
[69] Mr David Durant (DIG0020) para 10

Estonian system enshrined transparency, whereby citizens had a legal right to see who had accessed their data and for what reasons.[70] In the meeting between our Chair and Estonian officials in March 2019, the Estonian representatives disputed the view that a single unique identifier raised ethical concerns (see annex two). Instead, they argued that citizens' data being used across Government departments, with little transparency over who had accessed it and why, and without the citizen being aware of the use of their data, such as in the UK system, was a bigger civil liberties issue due to the lack of transparency and accountability. The Estonian citizen has a unique identifier but that means they can see exactly what the Government is doing with their data. The Estonian representatives explained that the civil liberties argument was more nuanced than some might claim.

Despite concern among some groups of witnesses, a shift in approach in the UK Government's position seems on the horizon. The Minister for Digital and the Creative industries, for example, implied support for a universal digital ID in a recent interview with *The Daily Telegraph* in 2019:

> I think there are advantages of a universally acclaimed digital ID system which nowhere in the world has yet. There is a great prize to be won once the technology and the public's confidence are reconciled.[71]

33. On 11 June 2019, DCMS and the Cabinet Office announced their intentions to launch a consultation on digital identify verification in the coming weeks. The following actions were set out:

- "A consultation to be issued in the coming weeks on how to deliver the effective organisation of the digital identity market."
- "The creation of a new Digital Identity Unit, which is a collaboration between DCMS and Cabinet Office. The Unit will help bring the public and private sector together, ensure the adoption of interoperable standards, specification and schemes, and deliver on the outcome of the consultation."
- The start of engagement on the commercial framework for using digital identities from the private sector for the period from April 2020 to ensure the continued delivery of public services."[72]

34. **Single unique identifiers for citizens can transform the efficiency and transparency of Government services. We welcome the Government's announcement in June 2019 that it will consult shortly on digital identity. While we recognise that in the UK there are concerns about some of the features of a single unique identifier, as demonstrated by the public reaction to the 2006 Identity Card Act, we believe that the Government should recognise the value of consistent identity verification.** ***The Government should facilitate a national debate on single unique identifiers for citizens to use for accessing public services along with the right of the citizen to know exactly what the Government is doing with their data.***

[70] Peter Herlihy, "'Government as a data model': what I learned in Estonia", Government Digital Service, (October 2013)

[71] "UK should 'get over' privacy fears and embrace tech-based ID, says digital minister", The Telegraph, 9 December 2018

[72] "Minister confirms government ambition on digital identity", Cabinet Office press release 2019, 11 June 2019

Social inclusion

35. In this Chapter so far, we have mainly focused on the positives of digitisation for the Government-citizen relationship. However, we did receive concerns that a move to "digital" could result in a two-tier set of public services that might, for example, worsen the citizen-State relationship for some, specifically those who were not able to use digital channels as easily, such as some disabled or elderly people. For example, Policy Connect argued that Government services should still be accessible for those who have a disability who might be less able to access these services digitally. They explained that as "the ONS found that while 90% of all adults in the UK have used the internet recently, 20% of disabled adults had never used the internet".[73] In comparison, 8.4% of all adults had never used the internet in 2018.[74] Tom Loosemore, a former Deputy Director of GDS, expressed a concern that some senior Government staff, specifically at the Department for Work and Pensions, might have "wilfully" misunderstood what was meant by digital by default, including hiding other means of contacting the department, such as phone numbers, from its websites:

> Digital by default did not mean online only. It did not mean hiding other channels and making them rubbish, so that people were forced to use the online channel. Personally, I think that that is lamentable.[75]

We put these allegations to Simon McKinnon, the interim Chief Digital Officer at DWP, when he appeared before us. He refuted the allegation that DWP would try and hide phone numbers, stating that citizens were only requested to use online services for "economic reasons", and that the department would always provide alternative means of contact.[76] This point was reinforced in a joint letter to the Chair of the Committee, from the Minister for Digital and the Creative Industries and the Minister for Implementation, which explained that the Government intended to keep the relationship between citizen and Government as accessible to those who were not able to access the internet as it was to those who could use the internet. Libraries was one of the means suggested to do this.[77]

36. **While we believe it is important for the Government to make its services end-to-end digital, it must do this in such a way that it includes access to public services for those who are not digitally connected.** ***The Government must ensure that public spaces with digital access, such as libraries, are maintained. The Government should also ensure that those who are not digitally connected have alternative ways of accessing services, for example, by using the phone or having assistance to use digital services, and those alternatives are properly promoted.***

[73] Policy Connect (DIG0011) para 2

[74] Office for National Statistics, "Internet users, UK: 2018, 31 May 2018

[75] Q27

[76] Q333

[77] Department for Digital, Culture, Media and Sport and the Cabinet Office (DIG0032) p 3

3 Levers for transformation

37. This Chapter sets out the progress that the Government has made so far in utilising data and technology to enable transformation.

Public sector data-sharing

38. The *Government Transformation Strategy*, published in 2017, emphasised how and why the joining up of data across the Government and its Agencies was key to transforming the operations of Government:

> Delivering public services more effectively and efficiently requires joining together data from multiple public sector bodies [...] The convenience and cost-effectiveness of these digital services are felt by individual citizens and society as a whole. They would not be possible without the ability to share data securely within government.[78]

Similarly, the British Computing Society emphasised that data-sharing and its underlying infrastructure were vital aspects of digital Government as well as a means of better policy delivery.[79]

39. We heard that the utilisation of data for better public services could, in turn, improve the relationship between the citizen and the State, a key theme of digitisation (see paragraph 22). Professor Weerakkody told us that there was a lot of data out there, that if utilised properly by the Government, would benefit the citizen, providing them with more information that would positively affect their day-to-day life, such as in the case of a citizen who may be moving house and want to look up information and data about schools, transport, environment and healthcare in the local area.[80] Further, Joel Bellman representing Deloitte and Councillor Peter Fleming representing the Local Government Association, gave us further examples of how the good use of data by the Government could create more efficient public services that in turn improved the quality of life for citizens.[81] Joel Bellman, for example, explained that, in the London Borough of Barking and Dagenham, he had seen how local datasets had influenced policy decisions that fulfilled their social imperatives, while Councillor Peter Fleming explained that in his area, Sevenoaks Town & St. John's, the data on deprivation levels influenced where the Council spent money.[82]

40. The Cabinet Office was positive about the Government's data-sharing infrastructure. It explained that GDS was continuing to make services seamless for users through its expansion of the availability of GOV.UK Registers, as discussed in the previous Chapter.[83] SAS, a software analytics company, explained that GDS had undertaken work on data infrastructure and standards already which had made major progress in "joining up the machinery of government".[84] Similarly, Deloitte explained that GDS had been successful in creating services (such as GOV.UK Registers and GOV.UK Design System) which teams

[78] The Cabinet Office, Government Transformation Strategy, (February 2017), p 47

[79] BCS, The Chartered Institute for IT (DIG0016) para 4.3

[80] Q94

[81] Q165

[82] Qq167–168

[83] Cabinet Office (DIG0023) para 67

[84] SAS (DIG0015)

across Government could use to assist the sharing of data.[85] Tom Smith representing the Office for National Statistics was also positive about the contribution that GDS had made initially to the Government data-sharing landscape: "one great success of GDS was enabling, facilitating and supporting a step change in the technical expertise and capability within Government."[86]

41. In addition, the *Government Transformation Strategy* (2017) outlined further action that the Government had taken to improve data-sharing:

- Opening up Government data and Government services internally and externally through the use of Application Programming Interfaces (APIs) (definition in footnote).[87]
- Building a national data infrastructure of registers and ensuring they were secure and available to the public, such as a country register and the prison estate register;
- Transforming the way that Government's data is stored and managed; and
- Exiting large single supplier and multi-year IT contracts.[88]

42. In 2017, GDS carried out research on how Government services were developed and found that there was variation between departments, often with silos between different areas and professions.[89] As such, and in response to the *Government Transformation Strategy*, GDS set out a commitment to "build services that run seamlessly across government".[90] Since then, GDS and the Cabinet Office have implemented infrastructure to promote data-sharing across departments.[91] For example, the Cabinet Office highlighted to us API technical data standards that were released in February 2018, noting that these standards had helped departments to open up data for re-use in a consistent way.[92] This had been a significant recommendation made in the Martha Lane Fox review, which led to GDS's creation, (see paragraph 1 for further detail on the Martha Lane Fox review). These standards included:

- Enabling access to a whole dataset in bulk;
- Having appropriate responses to data requests;
- Authorising APIs to be used by other departments; and
- Keeping local dataset copies up-to-date.[93]

[85] Deloitte LLP (DIG0014) p 7

[86] Q146

[87] An application programming interface (API) is a set of subroutine definitions, communication protocols, and tools for building software. API makes it easier to develop a computer program by providing all the building blocks, which are then put together by the programmer.

[88] The Cabinet Office, Government Transformation Strategy, (February 2017) p 49

[89] Tom Wynne-Morgan and Will Harmer, "How cross-government communities can support cross-government services", GDS Blog, 8 January 2018

[90] The Cabinet Office, Government Transformation Strategy, (February 2017) p 5

[91] Cabinet Office (DIG0023) para 33

[92] Cabinet Office (DIG0023) para 33

[93] Martha Lane Fox, Directgov 2010 and beyond: revolution not evolution, (October 2010)

The Government Digital Service also told us that it was prioritising "making better use of Government data" as part of its workstreams, but little additional evidence was provided about how they planned to do this.[94]

43. As discussed in the previous Chapter, Estonia was highlighted to us as an example of a State that had made good use of citizen data to transform the way in which the two interacted. Estonia utilised a system known as the X-Road to ensure that data was shared securely between departments, but without a reliance on a centralised database.[95] The X-Road is a system of registries whereby each register has an owner, usually a department or team within a department, who is responsible for the data. In order for the citizen to access this data, they provide a single unique identifier (we discussed the theme of single unique identifiers at paragraph 29). In turn, the citizen's data is encrypted and every time a person accesses it, including the citizen or the Estonian government, a digital footprint of that activity is left so that people can see who has accessed that data. In a book published by e-Estonia, a group that presents the way in which the Estonian government had facilitated electronic interactions between the citizen and the State for global policy makers, they summarised the benefits of the X-Road:

> The X-Road is a critical tool, one of the key ingredients in e-Estonia's infrastructure that connects all the decentralised components of the system together. It's the environment that allows the nation's various e-services and databases, in both the public and private sector, to link up and operate in harmony no matter what platform they are being used on.[96]

44. The Alan Turing Institute, the national institute for data science and artificial intelligence, suggested that GDS had taken steps to emulate features of the X-Road in the Government as a Platform (GaaP) approach: "where each data variable is the responsibility of one agency alone, and there is a mechanism of secure data interchange between registries, X-Road".[97] However, David Durant, a former employee for GDS, told us that GOV.UK Registers received minimal support from the rest of Government and, as such, progress stalled.[98] Further, a report from the National Audit Office in 2017 and a 2018 Report from Reform, a think tank working to reform Westminster, both concluded that, though progress had been made, further work on the necessary infrastructure was required so that data could be shared across the public sector for optimum results.[99] The Government has taken other steps in this area too. For example, in January 2019, GDS launched the "data revolution"—a public call for thoughts and ideas on how the Government could create "a strong practical movement in central government focusing on the applied experience of data for better services".[100] In the blogpost that announced this, GDS identified five key areas in which the Government needed to make distinct progress to better its data-sharing practices. These were:

[94] Cabinet Office (DIG0034) p 13

[95] E-Estonia, Interoperability Services, accessed 25 June 2019

[96] "e-Estonia: the epic story of the e-State", pp 18–19

[97] The Alan Turing Institute (DIG0005) para 3

[98] Mr David Durant (DIG0020) para 7

[99] National Audit Office, Digital transformation in Government, (March 2017), para 22; Sarah Timmis et al, "Sharing the benefits How to use data effectively in the public sector", Reform, (August 2018), p 37

[100] Kit Collingwood and Robin Linacre, "Help us start a data revolution for Government", Government Digital Service January 2019

- Making sure data is fit for purpose and stored appropriately by the Government;
- Ensuring the right skills in both leadership and lower down, so that data skills gaps are appropriately addressed;
- Ensuring funding teams to work across department boundaries;
- Building shared guidance and standards to ensure all data custodians and guardians are connected whilst maintaining autonomy; and
- Sharing data through open but secure collaboration.[101]

45. In July 2018, DCMS announced its intentions to launch a National Data Strategy, "to unlock the power of data in the UK economy and Government, while building public confidence in its use."[102] The Office for National Statistics and 360Giving explained that the National Data Strategy also had a key role to play in the future good use of data.[103] While this has not yet been published the Government has begun the process of developing the strategy. In June 2019, the Government announced the first phase of this strategy, which was a call for evidence to underpin the strategy itself. The final strategy is expected late next year.

46. **Data-sharing is key to ensuring that digital Government can be transformative. It enables departments to work together to produce efficient public services that work for the citizen, thus improving the citizen-Government relationship. We welcome that the Government has commenced phase one of developing its National Data Strategy.** ***As part of this process to inform the content of the National Data Strategy, DCMS should conduct an audit of data-sharing amongst Government departments to see where best practice is taking place, and identify which departments are particularly siloed. Further, the audit should also determine to what extent the initial recommendations by Martha Lane Fox were adopted. This audit should be completed and published in advance of the National Data Strategy being published in Winter 2020 so that its findings can inform the National Data Strategy.***

Culture and leadership

47. As mentioned at paragraph 38, the relationship between departments and the processes within departments are key to maximising the use of data across Government. Further, Tom Loosemore, a former Deputy Director of GDS, identified that, as departments improved their own expertise, there remained a need for a central driving force, such as a data advisory board, to ensure cross-government collaboration.[104] The creation of a 'Data Advisory Board' was mentioned by the Office for National Statistics, DCMS and the Cabinet Office as having the potential to remedy data related challenges and to ensure that use of data had the appropriate leadership and governance across Government.[105] Such a Board was set up earlier this year, as a result of the *Government Transformation Strategy*.[106]

[101] Kit Collingwood and Robin Linacre, "Help us start a data revolution for Government", Government Digital Service, January 2019

[102] Department for Digital, Culture, Media and Sport, "National Data Strategy open call for evidence", June 2019

[103] 360Giving (DIG0019) p 1; Office for National Statistics (DIG0012), p 6

[104] Q149

[105] Department for Digital, Culture, Media and Sport (DIG0031); Office for National Statistics (DIG0012); Cabinet Office (DIG0023)

[106] The Cabinet Office, "Government Transformation Strategy", (February 2017), p 10

The Board's terms of reference explain that it is "the senior public sector board responsible for driving the better use of data in government and addressing any gaps and barriers preventing it."[107] The Board has met but membership and the minutes of meetings are not a matter of public record.

48. Additionally, the *Government Transformation Strategy* in 2017 set out a plan to appoint a cross-Government Chief Data Officer to oversee data governance across departments.[108] However, as of yet this role still remains unfilled. Mr David Durant, a former employee of GDS, and techUK, both emphasised the importance of appointing a Chief Data Officer to ensure that data was given the appropriate leadership and direction it required.[109]

49. The issue of leadership in data policy was highlighted by other witnesses, including Councillor Peter Fleming from the Local Government Association, who suggested that work was still needed to join up projects across Government departments. Not doing so, he explained, could result in the citizen's experience of Government being "confused, contradictory and complicated".[110] This view was shared by Deloitte, who explained that some departments only saw "as far as their own perimeters".[111] Deloitte elaborated that this issue existed due to the complex design of Government: the "relatively complex governmental design" presented a large barrier to digital change and collaboration, meaning that systems were entrenched in departments, and "countries with fewer levels of Government and more centralised structures are better able to drive change across government silos".[112]

50. **We welcome the Government's establishment of a Data Advisory Board. However, at present its membership, agenda and decisions are not a matter of public record. *In response to this Report, the Government should set out how it will make the work of the Data Advisory Board more transparent. It should make public its membership, agenda and a summary of its decisions. If the Government decide that it is not possible to make the Board more transparent then it should set out its reasons why.***

51. **It is disappointing that the Government has not appointed a Chief Data Officer, some time after it committed to do so in the 2017 Government Transformation Strategy. *The Government should appoint a Chief Data Officer by the end of 2019.***

Innovative technologies

52. Another major lever of digital Government transformation is technological innovation. This was defined by the Government as "new technologies that do not currently have a critical mass, but which may have the potential to disrupt industries or generate significant savings".[113] This had been prioritised as a key theme for Government, and appeared as a major commitment in the *Government Transformation Strategy.*[114] PUBLIC, a technology

[107] Department for Digital, Culture, Media and Sport, "Terms of Reference for the Data Advisory Board", January 2019

[108] The Cabinet Office, "Government Transformation Strategy", (February 2017), p 10

[109] Mr David Durant (DIG0020), para 5.1; techUK (DIG0022) para 20

[110] Local Government Association (DIG0018) para 4.4

[111] Deloitte LLP (DIG0014) p 8

[112] Deloitte LLP (DIG0014) p 2

[113] Government Digital Service, " Technology innovation in government survey", August 2018

[114] The Cabinet Office, "Government Transformation Strategy", (February 2017), p 63

consultancy company for the public sector, told us that "the UK has an extraordinary opportunity" to seize the emerging market of innovative technology, where the GovTech market could reach up to £20bn.[115]

53. In 2017, the then Director General of GDS, Kevin Cunnington, commissioned a review into the Government's use of innovative technology.[116] This review concluded that GDS was in a good position to support BEIS and DCMS in achieving the Government's ambition of becoming a world leader in artificial intelligence (AI) through the adoption of emerging technologies to transform public services.[117] Many of the written submissions we received highlighted the potential uses of artificial intelligence in future Government services. For example, SAS, an analytics and software company explained the economic benefits of AI for the Government:

> It has been estimated that Artificial Intelligence (AI) alone could add an additional USD $814 billion (£630bn) to the UK economy by 2035, increasing the annual growth rate of GVA from 2.5 to 3.9%. As such, Government like other constituents in the UK has a massive amount to gain from using data-enabled technologies such as analytics and AI.[118]

54. Further, we heard how the adoption of new innovative technologies, such as AI, had an important role to play in improving the relationship between the citizen and the State, a key benefit of digitisation (as outlined at paragraph 17). PUBLIC explained that, by the Government utilising innovative technologies, it could also transform and improve how it delivered services for citizens, another key theme of digitisation: innovative technologies could "offer a better service to citizens, both in terms of service delivery and taxpayer money, and Government can ensure equitable, high-quality provision of services".[119]

55. Further, evidence from the Cabinet Office and the Minister for Implementation, Oliver Dowden MP, set out the Government's use of the GovTech Catalyst programme to develop technological innovation to solve public policy issues.[120] The GovTech Catalyst programme is "a 3-year programme that funds private-sector innovators to solve public-sector operational service and policy delivery challenges across the UK".[121] Though the Catalyst is fairly new, the Cabinet Office set out its current and future plans for the programme: "GovTech expects to launch a total of 15 competitions to solve public-sector challenges over 3 rounds and has announced the first 10 challenges selected for funding".[122] We were told by the Cabinet Office that GovTech Catalyst programme funding has helped to tackle public policy issues, such as rural isolation and traffic management, through innovative technologies such as artificial intelligence.[123]

[115] PUBLIC (DIG0027) p 1

[116] Government Digital Service, " Technology innovation in government survey", August 2018

[117] Government Digital Service, " Technology innovation in government survey", August 2018

[118] SAS (DIG0015) para 4.1.2

[119] PUBLIC (DIG0027) p 5

[120] Cabinet Office (DIG0023) para 56–60; Q394

[121] Cabinet Office (DIG0023) para 56

[122] Cabinet Office (DIG0023), para 58

[123] Cabinet Office (DIG0023), para 59

Leadership in innovative technology

56. Evidence that these technologies were important to digital Government was compelling. However, we also received evidence explaining the importance of leadership in promoting these technologies. Deloitte, for example, suggested that GDS had a key role to play in encouraging departments to adopt new technologies as "forms of artificial intelligence technologies [could] improve the speed of decision-making in areas such as welfare, tax and criminal justice".[124] Nonetheless, the Alan Turing Institute warned that a lack of central leadership in developing and utilising innovative technology in Government could cause smaller departments to fall behind, as "without a concerted and centralised effort, a two-tier system is emerging".[125]

57. In March 2018, the Government announced the creation of the Government Office for AI as part of the commitments made in the AI Sector Deal. The Office for AI is jointly led by DCMS and BEIS and committed to making AI work for society, supporting its uptake across sectors and helping to ensure the development of skills and investment.[126]

58. However, Helen Margetts representing the Alan Turing Institute noted that although the Government had made progress in introducing and committing to innovative technologies, there was a general lack of enthusiasm in the Government's overall approach to them.[127] This view was supported by Daniel Korski, representing PUBLIC, who said that the "Government have to be much more willing to try out, pilot and experiment with new technologies".[128] Further, Deloitte also argued that, without central leadership, departments may inadvertently duplicate work and the implementation of specific technologies, and that "in the promotion of new technologies, the public genuinely needs advocacy for "Government as one entity"".[129]

59. The Minister for Digital and the Creative Industries, Margot James MP, told us that the publication of the National Data Strategy would help to advance the Government's commitment to innovative technology, by helping to clarify the opportunities that data presented. Further, in a speech at the Government ICT conference in January 2019, the Minister for Implementation, Oliver Dowden MP, set out his commitment to ensuring that innovation would become "standard practice" in the public sector, and that the Government should become "an intelligent and coordinated buyer of emerging technologies".[130]

60. The Government made further commitments on taking advantage of AI and data-intensive technologies in its Industrial Strategy White Paper, which set out AI and data use as one of its four "Grand Challenges". Further, in a recent announcement on the first phase of the National Data Strategy, the Government emphasised the value of data for Government innovation.[131]

[124] Deloitte LLP (DIG0014), p 8

[125] The Alan Turing Institute (DIG0005), para 9

[126] Office for Artificial Intelligence, "About Us", accessed 25 June 2019

[127] Q269

[128] Q271

[129] Deloitte LLP (DIG0014), p 8

[130] Oliver Dowden CBE MP, "Oliver Dowden CBE MP - speech at the government ICT conference 2019", Cabinet Office, 23 January 2019

[131] Department for Business, Energy and Industrial Strategy and Department for Digital, Culture, Media and Sport, "AI Sector Deal", 21 May 2019

61. **The Government has made positive commitments to artificial intelligence and harnessing its value for transformation. It is too early to assess to what extent the National Data Strategy and Industrial Strategy will impact the Government's use of innovative technologies. We are concerned, however, that a lack of central leadership for the use of AI and other innovative technologies in Government services may result in inconsistent deployment across departments.**

62. ***The Government should make the Government Office for AI responsible, as a central body, for leading on ensuring that all departments take advantage of the transformative benefits that Artificial Intelligence and other innovative technologies offer.***

Ethics of data use

63. One concern raised with us, for example by Helen Margetts, representing the Alan Turing Institute, was related to the ethical implications of new technologies, specifically in terms of the use of the data that underpinned them.[132] Concerns were raised about how the Government might misuse or fail to appropriately mitigate the risks surrounding the technology's associated datasets—for example, the Legal Education Foundation, a charity promoting the rule of law, raised concerns relating to data bias and transparency in decision-making algorithms, which could result in flawed decision-making and policies.[133]

64. Further, Helen Margetts and Daniel Korski both explained that in order for the Government to fully take advantage of the benefits that innovative technologies had to offer, it needed to clean up the quality of data.[134] Helen Margetts raised concern that it would be risky to start adopting data-intensive technologies without ensuring that the data infrastructure that underpinned them was as accurate and usable as possible.[135] Peter Wells representing the Open Data Institute shared this view.[136] Peter Wells specifically highlighted the need to "build data infrastructure through delivering real practical services by solving problems, always thinking of what other unintended uses you might be making it available for".[137]

65. Our predecessor Committee was concerned too that as many of these technologies relied on the presence of automated decisions, transparency around the decision-making process and the provenance of data was vital to their ethical and accurate use.[138] In its Report, *Big Data Dilemma*, published in 2016, our predecessor Committee concluded that "distrust arising from concerns about privacy and security is often well founded and must be resolved by industry and Government if the full value of big data is to be realised."[139] In the Government response to this Report it agreed with the Committee's conclusion. Further, when our predecessor Committee called on the Government to establish a Council of Data Science Ethics to address "the growing legal and ethical challenges associated with balancing privacy, anonymisation, security and public benefit" when

[132] Qq288–289

[133] The Legal Education Foundation (DIG0029) para 32

[134] Q219, Q294

[135] Q266

[136] Q272

[137] Q293

[138] Science and Technology Committee, Fourth Report of the Session 2015–16, *The big data dilemma,* HC 468

[139] Science and Technology Committee, Fourth Report of the Session 2015–16, *The big data dilemma,* HC 468, para 60

using data, the Government agreed.[140] In the Government Response, published in April 2016, the Government agreed with the Committee's recommendation on independence of oversight and undertook to "consider how a Council for Data Science Ethics should be established".[141] It took nearly two years for the Government to establish the Centre for Data Ethics and Innovation (CDEI). The CDEI agreed to submit an annual report to the Secretary of State, as per the recommendation from the Government, that he or she would lay before Parliament annually. The Government Response also outlined the CDEI's commitment to publishing an overarching assessment of data use and the governance landscape, including any recommendations it has made and the steps the government has taken to implement them, in order to ensure the Government was making the best and most transparent use of data, to maintain citizen trust and better the quality of public services.[142]

66. However, since that Report, concerns have continued to be raised that the Government has not taken all the appropriate action to mitigate ethical concerns. For example, medConfidential explained that "until citizens see how their data is used, and algorithms run from the data satisfy the standards of judicial review, the only mistakes that get fixed will be the mistakes with a high political profile".[143] Further, the Legal Education Foundation expressed concern that the Government's use of personal citizen data might not be entirely transparent: "when Government decisions are made about individuals' rights using data processing, it can be hard for an individual to know whether their data were accurate or processed correctly".[144]

67. Nonetheless, the Government has taken action in recent years. For example, it established a number of arms-length bodies to help advise on mitigating the ethical risks of data technology, such as the Office for AI, the Centre for Data Ethics and Innovation, and the Alan Turing Institute. Since this inquiry commenced, the Centre for Data Ethics announced that it would be dedicating a quarter of its workstream resource to a review of algorithmic bias in public services.[145] This work is due to be completed by March 2020. There have also been a number of legislative changes which might help to mitigate ethical risks that data presents, including the GDPR (General Data Protection Regulations) and the Data Protection Act 2018, which gave citizens more control over their data and enhanced transparency.[146] The Minister for Digital and the Creative Industries compared GDPR to the Estonian data-consent system, in which citizens can access all the data the Government holds about them and have to consent to sharing it with departments (full details are set out at paragraph 23):

> I believe that the incorporation of the GDPR—and, indeed, the Data Protection Act, which goes beyond the GDPR—puts citizens in control of their own data. It gives them a panoply of rights over their data.[147]

[140] Science and Technology Committee, Fifth Special Report of the Session 2015–16, *The big data dilemma: Government Response to the Committee's Fourth Report of Session 2015–16,* HC 992, para 56 - 59

[141] Science and Technology Committee, Fifth Special Report of the Session 2015–16, The big data dilemma: Government Response to the Committee's Fourth Report of Session 2015–16, HC 992, para 57

[142] Science and Technology Committee, Fifth Special Report of the Session 2015–16, The big data dilemma: Government Response to the Committee's Fourth Report of Session 2015–16, HC 992

[143] medConfidential (DIG0028) para 69

[144] The Legal Education Foundation (DIG0029) para 2

[145] Centre for Data Ethics and Innovation, "Centre for Data Ethics and Innovation 2-year strategy", March 2019

[146] General Data Protection Regulation, Regulation (EU) 2016/679 and Data Protection Act 2018 (c. 12) May 2018

[147] Q436

68. Conversely, we heard from some witnesses that there was a tendency for the Government to be overly pre-occupied and concerned by the prospect of data ethics, which might inadvertently affect the deployment of technologies. For example, Doctors in Unite noted:

> A Ministerial decision to give people the right to opt out of the use of their data for epidemiological and public health research is smothering important research and important health analysis, even when the only use that is being made of the data is to count people.[148]

In addition, Joel Bellman representing Deloitte, highlighted research conducted by his company, which showed that the public was not only happy to have their data shared, but also assumed that data was being shared between departments much more than it was in reality. He told us:

> Over three quarters of the people said they would be very happy for us to share their data within the NHS to improve outcomes and care. Anecdotally, they then said, "Surely you are doing that anyway." That made us think that expectations around what the Government are already doing are out of kilter with what people think we are doing.[149]

69. Many of our witnesses emphasised the role of public outreach and education in both ensuring that the public had faith in the Government's use of data and in measuring how the public felt about the Government's use of it. Professor Helen Kennedy and Professor Helen Margetts, for example, both emphasised the use of outreach and education, whilst Dr Fiona Lugg-Widger recommended that the Government consider adopting a model not dissimilar from the Understanding Patient Data Initiative—this was a programme that went out and talked to the general public about their understanding of data use.[150]

70. **We welcome the steps that the Government has taken to enhance public trust in data use, including the establishment of the Centre for Data Ethics and Innovation. However, we are concerned that the Government might be taking an overly-cautious approach and second-guessing citizens' views on how their data should be used.** ***DCMS should ensure that the Centre for Data Ethics and Innovation annually assesses public opinion on Government data use. This review should start in summer 2019 and should aim to report by Spring 2020.***

[148] Doctors in Unite (The Medical Practitioners' Union) (DIG0030) para 3

[149] Q183

[150] Q116; Q309; Q182

4 Cultural challenges

71. This Chapter assesses the leadership of the digital Government transformation agenda and of GDS, as well as the pace at which change is being implemented.

Loss of momentum?

72. We heard from several witnesses, including Tom Loosemore, a former Deputy Director of GDS, and GlobalData, a technology advisory company, that digital Government in the UK had lost momentum.[151] GlobalData said that digital Government in the UK has suffered from "a loss of momentum through changes of leadership and weak political backing".[152]

73. Tom Loosemore emphasised the importance of leadership, including in GDS, for realising the ambition of Government to digitise and suggested that the political standing of the figurehead at the top of digital Government was integral to its initial success.[153] Mr Loosemore argued that the current Government did not have the leadership that the then Government had had during the coalition Government:

> Francis Maude [Minister for the Cabinet Office 2010–2016] would get the chief executives of global technology businesses into his office and show them the door, saying, "'You are not taking our billions off us anymore. Enough—the game is over.' That alignment and political support from the centre, with Jeremy Heywood right behind it, is now absent.[154]

He went on to explain that momentum had slowed since Francis Maude had left and he argued that, since his departure, there had been a "wilful, deliberate misdirection of the centre".[155] SAS, a software analytics company, said that the Government had lacked political backing and leadership in its commitment to innovative technologies, whilst Deloitte explained that there was a need for further leadership in Government to "shape and support" the digital economy.[156]

74. GDS has seen three leaders since 2011 and is set to see a fourth leader in eight years later this year. In 2011 Mike Bracken was appointed Executive Director of GDS, he was replaced by Stephen Foreshew-Cain in 2015 and then Kevin Cunnington in 2016. In June 2019, Kevin Cunnington left GDS to take on the role of Head of the International Government Service. A recruitment process for a new Director General will shortly be launched.[157]

75. Tom Loosemore, a former Deputy Director of GDS, told us that the Civil Service had a role to play in providing the continuity of leadership and drive, even if Ministers change post: "at the end of the day, you need a Civil Service leadership that can provide the continuity and help Ministers to understand—even if they are there for only 18 months—

[151] Q14
[152] GlobalData Public Sector (DIG0024) para 13
[153] Q23
[154] Q21
[155] Q55
[156] Deloitte LLP (DIG0014), p 11; SAS (DIG0015) para 4.18– 4.19
[157] The Cabinet Office and GDS, "Head of Government Digital Service to take on new role", June 2019

that this is an important long-term mission and change".[158] As such, he emphasised the importance of a strong central leadership within the Civil Service, that could support Ministers and ensure momentum was not lost.

76. However, much of the evidence we have received regarding a lack of leadership in digital Government is anecdotal. The Minister for Implementation, Oliver Dowden MP and the Minister for Digital and the Creative Industries, Margot James MP, refuted claims of a lack of leadership, arguing that Civil Service leadership and political backing were still there, but the nature of the relationship between digital leaders and departments had changed.[159] Oliver Dowden MP told us that centralisation and leadership from the centre were no longer necessary to ensure digital success across Government.[160] He explained that GDS was successful in the initial first steps of breaking up department silos, but since then, the role of GDS had developed and matured over time. It was only if digital projects were getting off track that they were escalated to Ministers at department level.[161]

77. The Institute for Government (IfG) reaffirmed this perspective in its 2017 report *Improving the management of digital government*.[162] In that report it explained that although there must be a driving force at the centre of Government, in the form of a Minister for Digital Government, to ensure digital transformation had enough buy-in from departments, GDS and its leaders now had to take on a supportive role with departments instead of driving digital transformation.[163]

78. Further, when we put Mr Loosemore's accusation that the centre of the Civil Service had deliberately slowed the progress of digitisation (see paragraph 72 and 73 for a detailed explanation of his remarks), to John Manzoni, the Chief Executive of the Civil Service, he refuted such a claim, explaining that there was "little to no evidence" to support the assertion that the UK had lost momentum.[164] He explained that "the UK consistently ranks internationally in the top five countries globally for digital government and open data", and had hosted 69 delegations so other countries could learn from the UK's success.[165] As set out at paragraph 4 of this Report, although the UK was placed fourth in the 2018 UN e-Government survey, it was ranked number one in 2016 before falling behind Denmark, Australia and South Korea.

79. Despite this, the majority of the evidence we received on this issue argued that a lack of central leadership could impact on the success of Government digitisation. Peter Fleming representing the Local Government Association, for example, explained that for local Government there had been a "backwards step" in the drive for digitisation over the last few years, resulting in an un-coordinated approach throughout Government.[166] This was also expressed in evidence submitted by his organisation, the Local Government Association, which set out the negative effect this could have on the relationship between the citizen and the State element of digitisation:

[158] Q60

[159] Q390

[160] Q390

[161] Qq389–390

[162] Institute for Government, "Improving the management of digital government", (June 2017)

[163] Institute for Government, "Improving the management of digital government", (June 2017), p 3–4

[164] Correspondence between the Chair of the Committee and John Manzoni, Chief Executive of the Civil Service and Cabinet Office Permanent Secretary, regarding Digital Government, 10 January 2019

[165] Correspondence between the Chair of the Committee and John Manzoni, Chief Executive of the Civil Service and Cabinet Office Permanent Secretary, regarding Digital Government, 19 December 2018

[166] Q139

> Despite the creation of the GDS, the various elements of the Government's digital work are spread widely […] This means the citizen's experience of government can be confused, contradictory and complicated.[167]

UKCloud also advocated that "strong leadership and direction from the top down" was needed if the Government was to build on GDS's earlier success.[168] Daniel Korski, CEO of PUBLIC, a GovTech consultancy company, explained that for digital transformative progress to happen there needed to be an alignment of political will and Civil Service leadership. He recommended: "I would like to see a situation where in every Department there is a Minister and a senior official who think it is their job to drive innovation and rethink how the Department works".[169]

80. When we enquired about how ministerial responsibility for digital Government was split, the Minister for Implementation and the Minister for Digital and the Creative Industries told us that cyber security resided with the Duchy of Lancaster, GDS and digital transformation resided with the Minister for Implementation and data policy resided with DCMS.[170] However, we heard from witnesses that specific elements of digital Government might need a specific Minister. For example, Professor Chris Johnson from the UK Computing Research Committee told us he would like to see a specific Minister for Cyber Security.[171] Furthermore, in the 2017 Institute for Government Report, *Improving the Management of Digital Government*, the Institute recommended a Minister for Digital Government who drives digitisation and transformation from the centre.[172]

81. **Political leadership in digitisation has been lacking in recent years since Francis Maude ceased being Minister for the Cabinet Office. This, coupled with the departure of senior Civil Service figures in GDS, has resulted in a slowing in the Government's digital momentum, as evidenced by other countries overtaking the UK in international rankings. It is now necessary to put in place processes which embed digitisation at a department-level and across the Civil Service.**

82. ***The Government should introduce a ministerial digital champion in every department by the end of 2019 who has responsibility for using innovation and digitisation to transform the way their department operates. These champions will need to co-ordinate at a department level and across departments. In response to this Report the Government should set out how this co-ordination will take place.***

The role of GDS

83. Kevin Cunnington, then Director General of GDS, told us that GDS was far more advanced compared to where it was when it first started: "When GDS started in 2012 we really had no capability: no people and no profession. Developing digital service was not normal but abnormal".[173] However, there is evidence to suggest that the Government was cultivating and valuing the digital technology profession long before the creation of GDS. The National Audit Office's 2011 *Information and Communications Technology in*

[167] Local Government Association (DIG0018), para 4.2

[168] UKCloud Ltd (DIG0008), para 3.3

[169] Q296

[170] Qq387–388

[171] Q250

[172] Institute for Government, "Improving the management of digital government", (June 2017), p 4

[173] Q331

Government Landscape Review report noted that a clear strategy for the professionalisation of the government ICT workforce was first set out in 2005.[174] Further, that report referenced the development of a competency framework to support career development of technology professionals and establishing a Government IT academy to "support both the professional development of IT Professionals in government and the building of a culture and identity for the Profession."[175]

84. Further, Mr Cunnington's claim that the Government had "no people" contradicted the 2011 NAO report, which had explained that "Government is one of the most significant employers of ICT professionals in the United Kingdom. Estimates of the number employed range from 35,000 to, if staff contracted to the public sector were included, well over 135,000."[176, 177] Though there might not have been a coherent team in the form of a digital service, there were several previous central Government teams who were responsible for driving cross-Government change prior to GDS, such as the Central Computer and Telecommunications Agency (1957), the Office of the e-Envoy (1999), the E-Government unit (2004), and the central Chief Information Officer Council (2010), made up of the Chief Information Officers in all Government departments.

85. Mr Cunnington set out the role of GDS in detail to us:

- Setting the cross-Government strategy;
- Setting standards and assurance;
- Providing capability across Government;
- Designing services and platforms;
- Providing expert services; and
- Providing continuous improvement across the Departments.[178]

The Minister for Implementation, Oliver Dowden MP, affirmed that the role of GDS, alongside the Cabinet Office and DCMS, was to provide departments with the "drive and direction" for digitisation.[179]

86. Evidence from GlobalData, techUK and others was positive about the initial role of GDS and the achievements it had made, but still said that as its role had changed it had struggled to consolidate its purpose.[180] GlobalData said that one of the good things that GDS had achieved was "the approach to digital service development that is now pervasive across Government and championed by GDS", but that now "GDS appears to have lost its way somewhat".[181] Further, techUK explained that "GDS has played a key role

[174] National Audit Office, Information and Communications Technology in government Landscape Review, HC 757, (February 2011)

[175] Cabinet Office, *Transformational Government,* Cm 6683, November 2005, para 46

[176] National Audit Office, Information and Communications Technology in government Landscape Review, HC 757, (February 2011), para 2.17

[177] Mr Cunnington told the Committee that "When GDS started in 2012 we really had no capability: no people and no profession." Mr Cunnington was referring to the lack of a Digital, Data and Technology profession including roles such as data scientists, and not just the creation of the IT workforce in Government

[178] Q311

[179] Q418

[180] GlobalData Public Sector (DIG0024) p1; techUK (DIG0022) para 3

[181] GlobalData Public Sector (DIG0024) p 1

in stimulating change both in how public authorities adopt and how suppliers provide new digital technologies and services", but agreed with the NAO's 2017 report, *Digital Transformation in Government*, that GDS had struggled to redefine its role as it has grown.[182] This view was shared by UKCloud, a cloud platform provider.[183]

87. Tom Loosemore and Dafydd Vaughan, former senior leaders at GDS, as well as Joel Bellman representing Deloitte, for example, recommended that GDS needed to be part of a more powerful centre of digital Government.[184] This was supported by evidence from PUBLIC, which explained that there was still an important role for GDS to act as the "rule-setter" and "to control underlying data so citizens can own it, and to be the manager of equitable, cheaper and better provision of services, whoever delivers them".[185] In this sense, they advocated that GDS had a role to play in setting the digital standards and policies that departments should adhere to.[186] This perspective was also affirmed by Kevin Cunnington, the Director General of GDS.[187]

88. Further, Joel Bellman, recommended that GDS, and the Cabinet Office in general, should have a greater role in compelling departments to take action with regards to their digital capacity, and should utilise powers to enforce departments to collaborate. He suggested that more hard power should be given to GDS, such as control over funding and accountability structures:

> They could be strong, carrot-and-stick levers, as in, "We can force you to and use spending controls and hold you to standards"; they can also use funding levers through the way they allocate money to projects and programmes that are cross-departmental; and they can use softer levers. But the power of the centre in making things happen is very important in a settlement such as we have in the UK where there are department boundaries.[188]

89. Conversely, the Chief Digital Officer at HMRC, Jacky Wright, advocated that the role of GDS could be, as set out by Mr Cunnington and the Minister for Implementation, more facilitatory (see Annex 3). In a meeting, Ms Wright explained that GDS should be a central co-ordinator around standards and knowledge-sharing, bringing together best practice, while operational departments designed platforms for current Government use as required. In particular, she highlighted how HMRC's identification verification tool was a model that could have been used by different departments, and GDS could have taken the lead on sharing the model (see Annex 3). By doing so, it would have ensured that those with the capability led on design and implementation, and GDS's role would be to support and set standards. Others agreed. For example, GlobalData pointed to GDS leading digital service development across the Government.[189] The Cabinet Office highlighted successes of GDS in developing standards for data and shared components across Government, stating that GDS "have inspired similar initiatives in other governments internationally".[190]

[182] National Audit Office, Digital transformation in government, (March 2017)
[183] UKCloud Ltd (DIG0008) para 3
[184] Q151
[185] PUBLIC (DIG0027) p 5
[186] PUBLIC (DIG0027) p 5
[187] Q311
[188] Q150
[189] GlobalData Public Sector (DIG0024) para 13
[190] Cabinet Office (DIG0023) para 31

Shared components were demonstrated by the success of Government as a Platform, as referred to in Chapter 2, and in the creation of common components and platforms, such as GOV.UK Notify, Verify and Pay.[191]

90. The 2017 Report *Improving the Management of digital Government*, from the Institute for Government, recommended that GDS clarify its standards, so it was clear what were expected standards for departments, and what was guidance so as to ensure they were "applied more deeply in departments and more widely in the public sector".[192]

91. **GDS made good progress in its early years on standards and platforms that applied across Government. However, we heard how GDS has "lost its way somewhat" and its purpose is now less clear.** ***GDS's purpose should be twofold: to provide advice to departments when needed, but also to devise and enforce minimum standards to be applied consistently across Government digital services. Departments, with the relevant capacity, should retain the ability to develop platforms and software. The Government needs to clarify GDS's role and its relationships with other departments, as well as determining with GDS whether there are any powers it needs to compel departments to take particular action.***

Responsibility for data policy

92. From 1 April 2018, control of data policy and governance was moved to DCMS from GDS/the Cabinet Office. The Prime Minister announced this machinery of Government change in a written statement to Parliament in March 2018.[193] The following functions were moved from the Cabinet Office to DCMS:

- Responsibility for data-sharing (including coordination of Part 5 of the Digital Economy Act 2017);
- data ethics;
- open data; and
- data governance.

In addition to this, policy responsibility for digital signatures moved from the Department for Business, Energy and Industrial Strategy to DCMS. DCMS told us that GDS would still lead on delivering technical components that supported data-sharing e.g. the Application Programming Interface strategy, open registers, and attribute exchange.[194]

93. Evidence from the Cabinet Office argued that the entirety of Government was "committed to using data more effectively in order to design and deliver high-quality and efficient public services",[195] and as such, emphasised that data policy must remain at the heart of digital policy for the successful implementation of digital Government (we explored in detail the issues surrounding the use of data to achieve digitisation in Chapter 2). However, witnesses raised concern that the move of data policy from GDS to DCMS might signal the opposite. Councillor Peter Fleming representing the Local Government

[191] Cabinet Office (DIG0023) para 29

[192] Institute for Government, Improving the management of digital government, (June 2017), p 3

[193] HC Deb, 29 March 2018, HCWS609

[194] Department for Digital, Culture, Media and Sport (DIG0031) para 3

[195] Cabinet Office (DIG0023) para 64

Association, for example, explained that the move of data policy to DCMS could potentially be damaging to digitisation, as DCMS might lack the same clout as the Cabinet Office in instructing departments to take action on its data policy.[196] This point was also made by Tom Loosemore, a former Deputy Director of GDS, who highlighted to us that DCMS did not have any enforcement powers to reprimand or compel departments for failing to comply with central data policy and guidance.[197] While the Cabinet Office did not have such powers either, Tom Loosemore and Councillor Peter Fleming argued that the Cabinet Office had soft power that it could exercise in such circumstances.[198] When asked whether there had been occasion when DCMS had been able to compel a department to do something against resistance, Matthew Gould, the then Director General for Digital and Media Policy, pointed to a number of policy reviews, but was unable to give a specific clear example.[199]

94. Matthew Gould, the then Director General for Digital and Media Policy advocated that it made good sense for the Government to create a department that dedicated its resource and attention to data, and refuted claims that DCMS lacked standing with other departments:

> Increasingly, across the range of what we do we are seen as delivering competence and having expertise. It is a sensible investment by Government to create a Department that is capable of taking all those digital policy issues in the round, including the wider data issues, so that we can lead on the data economy and some of the policy questions around data as a counterpart and partner to GDS.[200]

95. Tom Smith representing the Office for National Statistics was also positive about the move, explaining that it ensured better links with other parts of data policy, which sat within DCMS, such as the Centre for Data Ethics and Innovation and the Information Commissioner.[201] Private sector companies and non-government organisations such as SAS and 360Giving also viewed the move to DCMS as presenting fresh opportunities to improve the use of data, such as in the work on identification verification and in using AI and innovative technology.[202]

96. **It is too early to tell if the move of data policy to DCMS presents a challenge or an enhancement for Government digitisation.** ***We urge the Government to keep under review whether DCMS should be the lead department for open data and data ethics, governance and sharing. Further, in response to this Report, the Government should set out whether DCMS requires any additional powers to drive data reform across Government. If it does not deem this necessary it should set out why.***

[196] Q159
[197] Q74
[198] Qq314–316
[199] Q317
[200] Q313
[201] Q158
[202] SAS (DIG0015) para 4.8.3; 360Giving (DIG0019) p 1

5 Technical challenges

97. This Chapter sets out technical challenges of legacy systems and cyber security, that the Government will need to overcome if it is to maximise the potential of digital for the Government.

The challenge of legacy

98. The Government Digital Service has defined legacy systems, which can include:

- infrastructure;
- systems;
- on-premise hardware;
- business and IT processes;
- old digital services.

as technology that is:

- old or at the end of its life;
- no longer receiving support from the supplier;
- impossible to update;
- presenting unsolved and unsolvable problems;
- inherited, with inadequate documentation for current users;
- unable to meet current standards; and/or
- no longer the most efficient option, in terms of cost or technically.[203]

99. In *Managing the risks of legacy ICT to public service delivery,* the NAO explained that legacy systems created issues for the Government as they increasingly presented barriers to the introduction of new digital advances, as developments in policy required faster, newer and more efficient systems. They said:

> The risks of legacy ICT will increase over time as the gap between the system functionality and business need widens and the complexity of the systems and software increases. The management and technical resources needed to maintain and make further changes also increases.[204]

100. UKCloud Ltd, a cloud platform provider, characterised Government legacy technology as complex, as they had a "lack of interoperability between systems and services, and by monolithic long-term contracts that are expensive and difficult to break".[205] Further, the British Computing Society explained that "legacy systems create vulnerabilities that need

[203] Lucy Carey and Claire Ashworth, "Understanding legacy technology in Government", GOV.UK, May 2018
[204] National Audit Office, "Managing the risks of legacy ICT to public service delivery", HC 539, (September 2013)
[205] UKCloud Ltd (DIG0008) para 4.2

to be understood and managed".[206] Reports from both the Institute for Government and the NAO noted that legacy systems are the major obstacle to "digital by default". The 2011 *Government ICT strategy* also cited legacy ICT as a major barrier to the rapid introduction of new policies and GDS strategies.[207]

101. The British Computing Society told us that at the heart of most of the digitisation issues that the Government faced (within the field of digitisation) was technical infrastructure, based in legacy systems.[208] In a 2013 NAO Report, it was estimated that £480 billion of Government revenue was reliant on legacy technology, and that key systems such as the Department for Work and Pensions' pension service and HMRC's VAT collection service were both reliant on embedded legacy systems.[209] Further, Simon Hansford from UKCloud told us that the Government's continued spending on legacy systems without an appropriate plan to replace them would result in "wasting public money".[210] As the Institute for Government pointed out in its October 2018 Report, despite the recommendations made in the 2013 Report, the 2017 *Government Transformation Strategy* recognised that many of these systems were still in place.[211]

102. The British Computing Society argued that departments could not afford to ignore legacy technology, due to the increasing security risk it presented, as well as how it impinged upon the Government ability to harness innovative technology and effectively utilise data to improve its relationship with citizens, a key aim of digitisation (as we outlined in Chapter 2 of this Report). UKCloud also expressed concern that if the Government did not appropriately address its legacy issues, this would impinge upon transformation.[212]

Data

103. Legacy systems have created many different barriers to digitisation. The first, and perhaps most pressing issue was that Government data was held in these legacy systems, meaning that the full transformative potential of collaborative data use could not be reached. We have explored in further detail the challenges relating to data-sharing and collaboration between departments in the previous Chapter. The British Computing Society explained that because the data was held in separate, department legacy systems, interoperability was an issue for departments who otherwise could have benefited from the sharing of data about citizens.[213] Daniel Korski, representing PUBLIC, shared these concerns.[214]

104. The evidence we received, such as from Mr David Durant and others, generally expressed encouragement for the use of application programming interfaces (APIs) (a way of enabling different systems to interact with one another), open standards (ensuring different systems and data can interoperate) and open source software policies (enabling users to copy, distribute and use software freely or at low cost), but often asserted that more needed to be done, structurally, aside from the publishing of standards, to ensure cross-

[206] BCS, The Chartered Institute for IT (DIG0016) para 3.2
[207] Cabinet Office and Efficiency and Reform Group, "Government ICT strategy", March 2011, para 35
[208] BCS, The Chartered Institute for IT (DIG0016) para 2.2
[209] National Audit Office, "Managing the risks of legacy ICT to public service delivery", HC 539, (September 2013), para 2
[210] Q216
[211] Institute for Government, "The hidden obstacles to government digital transformation", (October 2018), p 6
[212] UKCloud Ltd (DIG0008) para 4.2
[213] BCS, The Chartered Institute for IT (DIG0016) para 4.3
[214] Q285

department collaboration and data-sharing.[215] The British Computing Society pointed to the need for GDS to overcome the significant technical challenges, such as interoperability issues that stemmed from legacy systems. They suggested that in order for data silos to be addressed "citizen and government environments need to integrate in the back office and unlock data to make the citizen experience as rich as possible; and this has not yet been achieved."[216]

105. We also heard that silos within departments were an issue for the Government. Jacky Wright, the Chief Digital Officer for HMRC noted that her department specifically experienced this issue, as there were large amounts of disparate data throughout HMRC within embedded legacy systems, meaning that effective collaboration with other departments, such as the Department for Work and Pensions, proved to be a challenge. Further, though APIs were utilised to extract and re-format data so that it was shareable, the British Computing Society pointed out that this was only possible with the "right standards and a solid data model".[217] This view was supported by Tom Smith representing the Office for National Statistics, who explained that "you need to understand and develop the data engineering and infrastructure that underpin the management, storage and safe use of data."[218] Mr Smith, however, urged us not to ignore the progress made by GDS to address these issues in previous years, stating that "some of the Departments have developed on the back of GDS's work very strong technical expertise, and that level across Government is now much stronger than it was."[219]

106. Evidence from the Cabinet Office, outlined a number of actions that the Government had taken to ensure that data could be appropriately shared across Government, despite its legacy foundations.[220] For example, using GOV.UK Registers to ensure data was accessible to those who needed it, as well as GDS's lead on the promotion of common standards across departments to ensure consistency and interoperability.[221] Tom Smith, representing the Office for National Statistics perceived that GDS had been successful in its promotion of standards: "one great success of GDS was enabling, facilitating and supporting a step change in the technical expertise and capability within Government."[222]

Procurement

107. We also heard that legacy systems had created a barrier in technology procurement, as departments had been "locked in" to large IT contracts as there were only a small number of suppliers who could support significant legacy issues.[223] UKCloud explained that the initial creation of GDS had "given Government a lever in its bid to break the stranglehold of its legacy technology suppliers (the so-called oligopoly)", but the momentum and commitment to change this had been compromised, and the Government needed to cultivate an environment that encouraged SMEs.[224] The British Computing Society told us that "80% of the work to be done is about addressing the issues of legacy systems, 20%

[215] Mr David Durant (DIG0020) para 4.2
[216] BCS, The Chartered Institute for IT (DIG0016) para 4.2
[217] BCS, The Chartered Institute for IT (DIG0016) para 4.3
[218] Q145
[219] Q146
[220] Cabinet Office (DIG0023) para 27–35
[221] Cabinet Office (DIG0023) para 29
[222] Q146
[223] UKCloud Ltd (DIG0008) para 4.3
[224] UKCloud Ltd (DIG0008) para 1.1 –1.2

is opportunity for innovation and the potential for SME involvement".[225] The Minister for Implementation, Oliver Dowden MP, also expressed concern to us about the accessibility of the current procurement framework for SMEs.[226] Further issues with procurement will be discussed in the next Chapter.

Skills

108. The final difficulty relating to legacy systems that was highlighted to us was that of digital skills. For example, the British Computing Society and techUK explained that the difficulties encountered by legacy technology had been exacerbated by the finite lack of digital skills in Government and it was difficult to ensure employees had the right digital capabilities to deal with legacy issues.[227] Simon McKinnon, the Chief Digital Officer for the Department for Work and Pensions, explained that though the Government currently had the right level of skills to deal with complex legacy systems, they would get increasingly hard to maintain as skills became shorter in supply.[228] However, he also told us that the Government was working to train employees and build capability in legacy systems going forward.[229] This is partially demonstrated by guidance published on the GOV.UK website, which outlined key strategies such as the *Digital Data and Technology Profession Capability Framework*.[230] This outlined the necessary digital skills for technical roles in Government, and the *Civil Service Workforce Plan 2016—2020*, which set out plans to build the capability of the Civil Service.[231] Skills will be explored in greater detail in the next Chapter.

What is the scale of the challenge for the Government?

109. Some of the evidence that we heard emphasised the importance of understanding the difficulty the Government faced in being able to move away from legacy, for example, techUK spoke of the need for GDS to be mindful of the constraints and challenges that public authorities had in moving away from or upgrading legacy processes and systems.[232] Simon McKinnon, the Chief Digital Officer for DWP, told us that although his department was taking action to tackle its legacy problem, it had to prioritise certain workstreams due to business critical need. This was confirmed by the then Director General of GDS, Kevin Cunnington, who explained:

> We tend not to fix it if it ain't broke; we tend to prioritise new policy requirements. Secondly, as Simon says, it is much harder to fix Government legacy because it comes with all sorts of legislative constraints than it is in the private sector.[233]

[225] BCS, The Chartered Institute for IT (DIG0016) para 5.2

[226] Q393

[227] BCS, The Chartered Institute for IT (DIG0016) para 5; techUK (DIG0022) para 16

[228] Q353

[229] Q353

[230] Digital, Data and Technology, "Digital, Data and Technology Profession Capability Framework", March 2017, last updated December 2018

[231] Civil Service, Civil Service Workforce Plan 2016–2020, July 2016

[232] techUK (DIG0022) para 7

[233] Q344

110. Jacky Wright, the Chief Digital Officer at HMRC, also explained that it was difficult to make a convincing case to the Treasury to replace legacy systems, due to the cost (see Annex 3). She told us that her department had begun an audit of its legacy systems to assess cyber vulnerabilities, in order to develop such a business case. We are not aware if HMRC has yet concluded this audit. Kevin Cunnington, the then Director General of GDS, was asked if there was a satisfactory level of ambition across Government to deal with legacy issues. He explained that it was their goal for the next spending round.[234] Further, when we asked the Minister for Implementation, Oliver Dowden MP, and Kevin Cunnington if there had been an appropriate audit of the scale of the legacy issue across Government, neither could provide us with an answer.[235] GDS have, however, set out public guidance that presented various options for departments when attempting to deal with legacy challenges.[236] Their guidance set out the five options for departments dealing with legacy systems. These were:

- "retain (do nothing);
- retire (drop);
- re-host (lift and shift);
- repurchase (shop and drop); and
- re-platform (life and shape)."[237]

111. Legacy systems have been flagged as an issue in previous Parliamentary inquiries and independent Reports from both the NAO and the Institute for Government yet there appears to be a limited mapping of legacy systems within departments and across the Government.[238] In the then Public Administration Select Committee's 2011 Report, it categorised legacy systems as a "a serious risk to government".[239] Despite this, similar conclusions were reached in the *Government Transformation Strategy* in 2017, and then again in the *Managing Legacy Technology* guidance published in February 2019.

112. Further, evidence we received emphasised the urgency for the Government to tackle the legacy problem now. The British Computing Society explained that "the longer the legacies remain in place the higher the risks become."[240] UKCloud also warned against allowing the legacy problem to go into stasis, as legacy technology becomes "locked-in to a small number of suppliers" and "will become tomorrow's problem for somebody else to solve".[241] The skills gap increases as legacy systems become more out-dated and hard to manage (see further exploration of this point at paragraph 109).

113. **Legacy systems are a significant barrier to effective Government transformation and digitisation. We acknowledge the attempts of the Government, its predecessors and individual departments to produce guidance and to deal with legacy issues.**

[234] Q346
[235] Q354 and Qq415–419
[236] Government Digital Service, "Managing legacy technology", February 2019
[237] Government Digital Service, "Managing legacy technology", February 2019
[238] National Audit Office, "Digital transformation in government", (March 2017); Institute for Government, "The hidden obstacles to government digital transformation" (October 2018)
[239] Public Administration Select Committee, Twelfth Report of Session 2010–12 , "Government and IT—"a recipe for rip-offs": time for a new approach", HC 715-I , July 2011
[240] BCS, The Chartered Institute for IT (DIG0016) para 3.2
[241] UKCloud Ltd (DIG0008) para 4.3

However, the same issues frequently recur, suggesting that the Government and GDS's advice has not been fully implemented. We acknowledge that there is a significant cost attached to the replacement of legacy systems, which the Treasury must resource adequately.

114. ***GDS should conduct an audit of all legacy systems across Government, including where they are based, what actions to take, the expected cost of such action and the resulting timescales. GDS's framework of retain (do nothing), retire (drop), re-host (lift and shift), repurchase (shop and drop), re-platform (life and shape) should be used to determine what actions to take with each legacy system. The audit should assess which approach is most realistic but 'retain' should not be used widely as the proposed action in the long-term as there is clear evidence that the legacy system issue is going to increase over time and there are challenges with regard to the skills for supporting such systems. GDS should seek to publish the findings of this audit. This audit should be completed no later than December 2020.***

Cyber security

115. Cyber security was presented to us as another technical challenge that the Government would face in its digital transformation process. This was a particular concern for cyber security company, Kaspersky Lab and UKCloud, the cloud platform provider, amongst others, as they argued that if the Government did not strengthen its cyber security policy, it could leave itself, and citizen data, vulnerable to attack.[242]

Cyber governance

116. The structures of governance and accountability around Government cyber security were set out to us in a joint letter from DCMS and the Cabinet Office:

- The Chancellor for the Duchy of Lancaster and Minister for the Cabinet Office is the leading Minister for cyber resilience in Government, who has accountability for the National Cyber Security Strategy, and responsibility for the security of Critical National Infrastructure.
- Each individual government department is responsible for the implementation of the cross-Government security policies and management of security risks.
- GDS creates and sets the technical standards and guidance on developing digital services and tools across government, while utilising advice from the National Cyber Security Centre and the Government Security Group.
- The Secretary of State for Digital, Culture, Media and Sport is responsible for cyber security, as it relates to skills and innovation, amongst others.[243]

117. The evidence received relating to the effectiveness of cyber security governance was mixed. Deloitte argued that the establishment of the National Cyber Security Centre (NCSC), as being the lead body for skill and strategy, was positive. They said:

[242] Kaspersky Lab (DIG0010); UKCloud Ltd (DIG0008) para 2

[243] Department for Digital, Culture, Media and Sport and the Cabinet Office (DIG0032) p 1–2

> The advent of the NCSC makes a significant step forward in ensuring that Government digitisation can be achieved with an increasing focus on cyber security. The quality of UK technical cyber security advice ranks among the best in the world.[244]

Further, the Office for National Statistics commended the guidance and standards that the NCSC had set out, as they ensured "significant digital services undergo the appropriate security assessment, including the protection of citizen and business data".[245] Professor Chris Johnson, representing the UK Computing Research Committee said that the National Cyber Security Centre was important as it aided individual departments and ensured that the Government was taking cyber security policy seriously both at the top of Government and through cyber essentials training of employees.[246]

118. Conversely, Ministers suggested that there was a split in cyber security accountability, as demonstrated when the Committee asked about the WannaCry attack on the NHS.[247] An investigation conducted by Redscan, a computer security service, in December 2018 revealed that despite the high profile nature of the WannaCry attack that affected the NHS in 2017, there were still significant cyber security issues facing the NHS that they were not equipped to deal with. Redscan's report was based upon the findings of a three-month freedom of information campaign, which surveyed more than 150 NHS trusts in the UK. The report concluded that:

- NHS trusts lacked sufficient in-house cyber security expertise;
- There was a wide imbalance in employee cyber security training and spending between trusts; and
- Many trusts were likely to be failing to meet training targets on information governance.[248]

When the Minister for Digital and the Creative Industries was asked about this, she explained that although it was the Government's responsibility to set cyber security standards, ultimately it was the role of individual departments to ensure that they were adhered to.[249]

119. techUK raised concerned that the "division of labour" of different parties in cyber security, such as GDS's oversight on setting standards and monitoring vulnerabilities, and NCSC's authority to respond strategically to incidents, could, at times "lead to confusion as to who is responsible for cyber security across government."[250] This view was supported by Deloitte, who observed that cyber security policy in the UK could be improved by a more joined-up Government approach.[251]

[244] Deloitte LLP (DIG0014) p 5

[245] Office for National Statistics (DIG0012) p 2

[246] Q244

[247] Qq454–459

[248] Redscan, "REDSCAN REVEALS A LARGE DISPARITY IN CYBERSECURITY SKILLS AND SPENDING ACROSS NHS", December 2018

[249] Q459

[250] techUK (DIG0022) para 22

[251] Deloitte LLP (DIG0014) p 6

120. Despite this, the Chief Digital Officer for HMRC, Jacky Wright, explained that the division of responsibilities for cyber security was a positive thing—as it had built in checks and balances—being an issue of major concern for national security. Further, the Cabinet Office suggested that the combination of skilled bodies, throughout Government, including GDS, NCSC and GCHQ, resulted in the UK being considered a "world leader" in global cyber security standards.[252] A 2017 report from the IfG explained that, although the establishment of the NCSC had been useful in reducing the overall number of various bodies responsible for cyber security, in the UK, no major attack had yet tested the robustness of the NCSC; the WannaCry attack had demonstrated the danger of leaving responsibility for cyber security squarely in the hands of departments or employees.[253]

121. Both Professor Chris Johnson, representing the UK Computing Research Committee and Antony Walker, Deputy CEO of techUK, recommended the creation of a new Ministerial role which had ultimate responsibility for cyber security.[254] When we asked the Minister for Digital and the Creative Industries, Margot James MP and the Minister for Implementation, Oliver Dowden MP, if there should be a Minister for Cyber Security, they explained that this role technically resided with David Lidington, the Chancellor of the Duchy of Lancaster.[255] However, the Minister of State for Security and Economic Crime also has responsibility for "cyber security" as part of portfolio, and the potential problems with this split of responsibilities was emphasised by the 2018 Report *Cyber Security of the UK's Critical National Infrastructure* by the Joint Committee on the National Security Strategy (JCNSS). In that Report the JCNSS explained:

> There is no single Minister with responsibility for the cyber resilience of CNI, or for cyber security in general. Instead, there is a patchwork of cross-cutting ministerial oversight that is structured by department […] focused political leadership is also essential, given the potential extensive impact of a major cyber-attack on the UK's CNI and the fast-changing nature of the threat, as well as the need to drive a consistent response across a number of departments and agencies. We have heard little to convince us that there is such a 'controlling mind' at the centre of Government that is proactively leading efforts to improve the cyber resilience of CNI.[256]

122. The Report went on to recommend the creation of a Cabinet Minister "designated as a cyber security lead" who could:

- "be empowered to hold departmental Ministers to account;
- sit on the National Security Council (NSC) and relevant NSC sub-committees; and
- oversee the work of the National Cyber Security Centre and the relevant section of the National Security Secretariat."[257]

[252] Cabinet Office (DIG0023) para 98

[253] Institute for Government, "Improving the management of digital government", (June 2017), p 13

[254] Q250

[255] Q450

[256] Joint Committee on National Security Strategy, Second Report of Session 2017–19, "Cyber Security of the UK's Critical National Infrastructure", HL 172 HC 706, July 2018, para 75

[257] Joint Committee on National Security Strategy, Second Report of Session 2017–19, "Cyber Security of the UK's Critical National Infrastructure", HL 172 HC 706, July 2018, para 80

In response to the JCNSS's Report, the Government explained that existing cyber security governance arrangements fulfilled the requirements set out and that the cross-cutting responsibilities of various ministers for different aspects of cyber security would remain in place.[258]

123. **More needs to be done to centralise leadership of cyber security policy and ensure that all departments are prioritising it in the same way. Responsibility in Government for cyber security policy is spread between departments to ensure checks and balances are in place, but we are concerned that this may result in a lack of accountability for specific incidents. We support the 2018 recommendation of our colleagues on the Joint Committee on the National Security Strategy that there should be a Minister for Cyber Security.** ***The Government should reconsider creating a Minister for Cyber Security who will be able to hold Ministers across Government to account for their internal cyber security. This Minister would also be responsible for working with other public sector bodies, including the NHS and local Government, to ensure that best practice and guidance was being shared across the public sector.***

Cyber standards

124. Concerns were raised by Kaspersky Lab, a private security company provider for Government services, that the WannaCry attack showed that basic cyber security was not up to scratch in the public sector.[259] The NAO published a report on WannaCry which emphasised its severity: "the attack led to disruption in at least 34% of trusts in England although the department and NHS England do not know the full extent of the disruption".[260] Kaspersky Lab explained that this attack had happened due to basic cyber security failures, including failures in updated software, patches, and vulnerabilities in programmes and applications that could be exploited so hackers could gain malicious entry.[261] The UK Computing Research Committee (UKCRC) argued that the Government had made good progress in the urgent action in cyber policy since the attack.[262] However, a recent report from the Public Accounts Committee concluded that the *National Cyber Security Strategy 2016–2021,* which set out how the Government planned to manage cyber security in the UK, was not on track to meet 11 out of 12 of its strategic outcomes by 2021, and that sufficient action had not been taken to ensure the Government and citizens were secure.[263] The Minister for Digital and the Creative Industries argued that the NHS had taken appropriate action for protection but conceded that "substantial financial pressures" sometimes compromised investments made to upgrade security systems.[264]

[258] Joint Committee on National Security Strategy Third Special Report of the Session 2017–2019, "Cyber Security of the UK's Critical National Infrastructure: Government Response to the Committee's Third Report of Session 2017–2019" HL Paper 304 HC 2003, March 2019, para 20

[259] Kaspersky Lab (DIG0010) p 2

[260] National Audit Office, "Investigation: WannaCry cyber attack and the NHS", (April 2018), para 5

[261] Kaspersky Lab (DIG0010) p 2

[262] UK Computing Research Committee (DIG0002), para 1-3

[263] Public Accounts Committee, Ninety-Ninth Report of the Session 2017–2019, "Cyber security in the UK" HC 1745, June 2019, para 4

[264] Q454

Department cyber standards

125. More generally, the oral evidence was mixed on the standards of cyber security expected across departments. For example, Simon Hansford representing UKCloud, a service provider for cloud computing services, explained that the standards of cyber security across departments were very low.[265] Conversely, Tom Loosemore, an ex-Deputy Director of GDS, observed that standards had been too high and had prevented GDS from implementing effective digitisation: "some of the cyber-security standards were terrifying in their inappropriateness, even in 2010. They actively stopped us doing the right thing from a cyber perspective".[266]

126. There was also a concern that cyber security standards varied across departments. An Institute for Government Report,*Improving the Management of Digital Government,* concluded that departments had variations of cyber security standards and dependency on vulnerable legacy systems.[267] This view was supported by the work undertaken by Jacky Wright in HMRC, as part of her audit of the vulnerability of HMRC legacy systems (see Annex 3). Professor Chris Johnson from the UK Computing Research Committee also shared this point of view, stating that the differing cyber security standards further disincentivised SME and small technology providers as the procurement landscape made it difficult for providers to understand how they should be bidding.[268] In contrast, techUK explained that the introduction of these standards had been a success for procurement as it set out "the minimum-security measures that government departments are required to implement to protect their information, technology and digital services".[269] We return in more detail to the issue of procurement in Chapter 5.

127. The Minister for Digital and the Creative Industries explained that all departments were subject to minimum cyber security standards.[270] The Cabinet Office told us that these standards should help both departments and suppliers to better understand cyber security risks in Government supply chains, as "Government will assess whether suppliers meet them, and they will be written into new contracts to enforce full compliance".[271]

128. **The Government has taken positive steps to develop cyber security standards. Despite this we remain concerned that cyber security policy varies between departments even if there are minimum cyber security standards. This creates unnecessary procurement barriers particularly for SMEs and small tech providers.** ***The Cabinet Office should review their universal, departmental cyber security standards and ensure they are sufficient, and clearly set out the requirements that bidders must meet to be eligible for Government procurements by the end of 2019. If any department wishes to diverge from these standards, they should have to make a case to the Minister for Implementation.***

[265] Q246
[266] Q9
[267] Institute for Government, "Improving the management of digital government", (June 2017), p 10.
[268] Q253
[269] techUK (DIG0022) para 23
[270] Q459
[271] Cabinet Office (DIG0023)

6 Institutional challenges

129. This Chapter assesses the level of institutional challenge that the Government faces in its digital strategy, in terms of procurement frameworks and internal digital skill capabilities.

Skills

130. The 2017 *Government Transformation Strategy* set out an ambition to create "one of the most digitally skilled populations of civil servants in the world".[272] The strategy suggested that digital skills were a necessary part of transformation, as digital transformation could not happen without a "skilled body of civil servants who have deep expertise in digital, data and technology (DDaT)".[273] The link between digital skills and internal Government transformation was set out:

> We will agree principles around which we can best organise digital, data and technology in departments. Digital, data and technology is a critical function within government but is less well-established than other Civil Service functions, such as human resources or finance. There are significant differences in capability across the public sector, often driven by the type of organisation (departments running transactions are generally more mature than policy making departments, for instance), which we need to recognise on departments' common journeys to becoming fundamentally digital.[274]

131. The Cabinet Office outlined the key ways in which GDS was leading the Government strategy to retain the right people and skills, including:

- The introduction of the Digital, Data and Technology Profession which covered over 17,000 specialists within Government;
- the GDS academy which taught civil servants' digital skills and technology awareness; and
- the upskilling of civil servants in areas with programmes such as the Data Science Accelerator and the Emerging Technology Development programme.[275]

Both Professor Helen Margetts, representing the Alan Turing Institute, and Professor Chris Johnson, representing the UK Computing Research Committee (UKCRC), emphasised the success of the Digital Skills Academy and were encouraged by the progress made.[276] Professor Chris Johnson commended its progress: "up to last year, the GDS Academy had seen 7,500 people through its courses. By any assessment, that is a really creditable performance in a very short space of time."[277]

[272] The Cabinet Office, Government Transformation Strategy, (February 2017) p 9

[273] The Cabinet Office, Government Transformation Strategy, (February 2017) p 39

[274] The Cabinet Office, Government Transformation Strategy, (February 2017) p 39

[275] Cabinet Office (DIG0023) para 49–50

[276] Q281

[277] Q222

The then Director General of GDS, Kevin Cunnington, also told us that GDS and the Government had made considerable, measurable progress. He explained that the creation of 38 job roles for the digital skills profession within Government had resulted in the Government being able to better measure competency and utilise appropriate pay scales and progression as incentives for employment.[278]

132. Despite this, evidence we received from PUBLIC and techUK suggested that although the Government had made progress in emphasising the importance of digital skills and implementing initiatives in Government to skill the workforce, it still struggled to find the right number and quality of digitally skilled employees.[279] We were told by the Ministers and UKCloud that this was not a problem that was just specific to the UK Government, but a global issue. This view was shared by Cloud Kickers, an engineering consultancy, who told us that they were concerned that the global skills gap constrained development across the world.[280] Professor Chris Johnson, UKCRC, agreed that this was not just specific to the UK Government.[281] Oliver Dowden MP, Cabinet Office and Margot James MP, DCMS, explained that the Government recognised there was a wider digital skills shortage, and was taking action to make the gap smaller through training and digital skills education.[282]

133. Tom Loosemore, a former Deputy Director of GDS, argued that the Government remained an attractive place to work as:

> those people are not always motivated by the high salary. They are motivated by hard problems, and Government has the hardest problems […] If you can continue to create bubbles of good culture, where people can do great work, entrusting empowered, humble teams, you will keep attracting brilliant talents.[283]

However, Mr Loosemore's view ran counter to the findings of a 2015 Report by the NAO, *The digital skills gap in Government*, which explained that "funding and pay are seen as biggest challenges to developing capability and capacity […] fewer than half of respondents were positive about their organisation's workforce plans".[284] The Minister for Implementation also recognised the challenges of competitive salary in the public sector: "clearly, across the whole Civil Service there are challenges in relation to pay". He explained that the Government was taking action to re-examine pay scales in order to address this issue.[285]

134. PUBLIC was concerned that the shortage in digital skills might have a significant knock-on effect on the capacity of the UK Government in relation to innovation and transformation. They told us:

[278] Q338
[279] PUBLIC (DIG0027) p 4; techUK (DIG0022) para 16
[280] Cloud Kickers (DIG0033)
[281] Q223
[282] Q440
[283] Q52
[284] National Audit Office, "The digital skills gap in government", (December 2015), p 30
[285] Q442

> Skills–both digital skills but also skills required to work in a more dynamic, agile fashion–across the public sector remain far below what they should be, and various initiatives remain uncoordinated and under-powered to make a real difference.[286]

135. The view that the lack of digital skills in Government might have a considerable impact on the ability of the Government to digitally transform was shared by the NAO in 2015, after it conducted a Government wide survey on digital skills.[287] This survey identified that the skills gap meant a "a risk of unsustainable cost reduction or service deterioration if government is unable to deliver transformation to any significant degree over the next 5 years."[288] In a 2017 Report, *Digital transformation in government*, the NAO pointed out the progress the Government had made to upskill employees, such as through its aim of training 3000 civil servants a year in the Digital Academies, the creation of 40 job roles across Government, and a review of pay grades. However it was too soon to see if this had had any impact.[289] The 2016 *Making a success of digital Government* report from the IfG also concluded that the Government's actions in skilling the workforce were proactive, but that it was too soon to see results and that "demand for staff continues to outstrip supply".[290]

136. Tom Loosemore told us that his major concern was the retention of digitally skilled staff, as opposed to the ability of the Government to recruit.[291] The IfG also alluded to this in its 2016 Report, explaining that pay and market conditions were still the biggest problem for the Government, as external, private companies tended to pay higher rates and therefore the best talent left the public sector. Kevin Cunnington told us that the current attrition rate, in March 2019, was 39%, but that most of the people who left GDS moved to work in other departments, and as such, the skills stayed within Government. In comparison, according to a recent Institute for Government Report, several London based Government departments lost about 20–25% of their staff every year.[292] In the private sector, tech companies in general experience a fairly high attrition rate, of around 23% between 2013–2018, according to a recent survey by Hay Group.[293]

137. Matthew Gould, the previous Director General for Digital for DCMS, agreed that the Government faced a specific problem retaining digitally skilled employees, but suggested that the flow of staff between roles and departments should be viewed as a positive opportunity for Government. He compared the UK model to what he had seen in Israel. He explained:

> They have a flow of people through Government agencies, academia and the economy. They cycle round and through them easily; there is relatively low friction in moving between different bits. I think that flow is helpful, so I would be wary of getting to a point where you regard people who move on as a tragedy. If you can get it right, it is a good thing.[294]

[286] PUBLIC (DIG0027) p 4
[287] National Audit Office, Digital skills gap in government , (December 2015)
[288] National Audit Office, Digital skills gap in government, (December 2015), p 4.
[289] National Audit Office, Digital transformation in government, (March 2017), para 3.16–3.18
[290] Institute for Government, Making a success of digital government, (October 2016), p 24
[291] Q52
[292] Institute for Government, "Moving On: The costs of high staff turnover in the civil service", (2019), p 4
[293] viGlobal, "Tech industry battles highest attrition rate in the world – and it's costly", accessed 3rd July 2019
[294] Q356

138. **The Government, including GDS, has made good attempts to tackle the digital skills shortage, through academies, creating job roles and considering progression pay. Nonetheless, more action is needed to ensure that digital skills capabilities are sustainable and not significantly affected by turnover of staff that is an issue for the digital workforce in both the public and private sector.**

139. ***The Government should publish a strategy by mid-2020 covering how it intends to make digital skills sustainable. It should also set out the ways in which it plans to continue to raise the skill levels of the Government workforce, ensuring that it is attracting and retaining the best and most digitally skilled employees as well as spreading best practice to staff working in roles which are predominantly non-digital.***

Procurement

140. Another factor which impacts the Government's ability to transform is procurement. According to the 2015 *Government Procurement Framework*, the overriding procurement policy requirement is that all public procurement must be based on value for money.[295] This is defined as "the best mix of quality and effectiveness for the least outlay over the period of use of the goods or services bought".[296] The 2017 *Government Transformation Strategy* focused on creating the right tools for the Government to consolidate its procurement policy. It suggested that procurement and contracting would be:

- data-driven;
- centred on the user;
- iterative;
- use the marketplace to ensure a common user experience.[297]

141. We heard from GlobalData that IT procurement in Government had historically been an "oligopoly" of large IT contracts, which was causing a "stranglehold" of Government by these legacy technology providers.[298] Furthermore, UKCloud told us that the Government had been locked into large IT contracts with firms that were "expensive and difficult to break". Many, including the Cabinet Office and PUBLIC, felt that opening up contracts to SMEs would drive innovation and competition, and thus not only provide the Government with better value for money, but also allow innovative technology companies to help solve public sector problems.[299]

142. However, we were told by Simon Hansford, representing UKCloud, that Government procurements were very onerous and complex due to Government restrictions and technical complications such as legacy systems.[300] To address challenges with procurement the Cabinet Office, prior to and after the 2017 *Government Transformation Strategy*, launched a number of ICT procurement initiatives. We cover some of these in the paragraphs that follow.

[295] Crown Commercial Service, "Public procurement policy", October 2015, last updated March 2018

[296] Crown Commercial Service, "Public procurement policy", October 2015, last updated March 2018

[297] The Cabinet Office, Government Transformation Strategy, (February 2017) pp 44–46

[298] GlobalData Public Sector (DIG0024) para 13

[299] Cabinet Office (DIG0023) para 43; PUBLIC (DIG0027)

[300] Q212

G-Cloud and the Digital Marketplace

143. The UK Government G-Cloud was created by GDS in 2012 as an initiative targeted at making the procurement process easier for departments and its Agencies.[301] The G-Cloud consisted of:

- A series of framework agreements[302] with suppliers, from which public sector organisations could buy services without needing to run a full tender or competition procurement process; and
- An online store—the "Digital Marketplace (previously known as "CloudStore")—that allowed public sector bodies to search for services that were covered by the G-Cloud frameworks.[303]

144. The Cabinet Office explained that, amongst other changes in its approach to IT procurement, the G-Cloud had led to significant savings. It estimated that GDS and the Crown Commercial Service (CCS) had saved £3.56billion between 2012 and 2015, and that the Digital Marketplace contributed toward a £725 million saving in 2016/17 alone.[304] However, a Freedom of Information request by Computer Weekly showed that four out of five G-cloud buyers were failing to share their savings data with the Government, and as such, figures that were produced about G-Cloud savings may not be entirely accurate, as users are likely to "over-report good deals and under-report uncompetitive deals".[305]

145. UKCloud Ltd praised G-Cloud, explaining that it had opened up digital procurement in Government to "new market entrants and SMEs", resulting in "improved citizen interaction with Government", a key aim of digitisation as outlined in paragraph 22 of this Report.[306] They went on to explain that G-Cloud had "saved the taxpayer money, bolstered the UK's burgeoning GovTech sector and had given Government a lever in its bid to break the stranglehold of its legacy technology suppliers".[307] techUK reiterated this view in its submission and told us that in a recent survey of GovTech SMEs the majority of respondents saw the G-Cloud as a useful means by which SMEs could access the public sector and it should therefore be seen as a success.[308] It is worth noting that UKCloud and techUK have both benefitted commercially from the G-Cloud and Digital Marketplace. However, GlobalData, a technology advisory company which has not benefitted directly from the Government's procurement initiatives was also positive about its impact.[309]

[301] Q212 and techUK (DIG0022) para 24

[302] An initial agreement between two parties on the future of their relationship, whilst acknowledging that the final agreement of their relationship has not yet been finalised.

[303] Government Digital Service, "The G-Cloud framework on the Digital Marketplace", September 2013, last updated July 2019

[304] Cabinet Office (DIG0023) para 18

[305] Caroline Donnelly, "Four in five G-Cloud buyers fail to share savings data with government, FOI response reveals", Computer Weekly, September 2015.

[306] UKCloud Ltd (DIG0008) para 1.1

[307] UKCloud Ltd (DIG0008) para 1.1

[308] techUK (DIG0022) para 10

[309] GlobalData Public Sector (DIG0024) para 3

146. In the book *Delivering on Digital*, commissioned by Deloitte, William D. Eggers further praised G-Cloud as an exceptional example of good IT governance:

> The store includes hundreds of suppliers who have been pre-evaluated and categorized, making it easy to find the right one for specific mission needs. Moreover, it has simplified the procurement process on both sides, giving suppliers one place to offer services and buyers one place to procure.[310]

147. We did not hear any evidence that suggested the Digital Marketplace or G-Cloud had been negative for digital transformation, although Simon Hansford, representing UKCloud and Professor Chris Johnson from UK Computing Research Committee, told us that the procurement process was still quite complicated, despite the introduction of the marketplace, and advocated that it should be simplified.[311] Professor Johnson explained that there were still many platforms on which to access available procurements in the UK—for example, these included the Digital Marketplace, Public Contracts Scotland and eSourcing Northern Ireland—which made procurement complex and access to it inconsistent.[312] In addition, Mr Hansford highlighted that the process was not transparent enough, as suppliers were not informed when a particular service was requested with the onus being on the Civil Service to draw the open bid to potential bidders' attention.[313] As such, he recommended that there should be more transparency and simplification of processes, and suppliers should be able to see what services were needed or be informed proactively which contracts were up for renewal, to encourage innovative SMEs and diverse companies to apply.[314]

148. PUBLIC, a digital transformation technology consultancy company, also took the view that current procurement policies limited the potential for Government technology-led reform:

> Procurement systems remain inflexible and complex, with a culture of risk averseness and a "computer says no" mentality. The disconnect between what the Government says it wants from technology and its systems to buy new technology is profound.[315]

149. The NAO also criticised the Government's procurement policy in 2017, concluding that although the Cabinet Office had made a "good start on reducing spending on ICT by departments", it needed to do far more to develop an accurate assessment of the impact and effectiveness of its ICT and procurement reform initiatives.[316] A 2015 NAO report, *The digital skills gap in government*, also pointed out that "procurement processes have the largest negative impact on obtaining external resources".[317] It identified that procurement lead times were the biggest barrier to the ability of the Government to access the necessary skills, followed by usability frameworks and payment thresholds. Thus it is clear that there is a link between the two institutional challenges that we are exploring in this Chapter—skills and procurement. This particular finding by the NAO was also made by Professor

[310] William D. Eggers, Delivering on Digital: The Innovators and Technologies that are Transforming Government, Deloitte University Press, 2016, p 116

[311] Qq241–242 and Q228

[312] Q240

[313] Q241

[314] Q242

[315] PUBLIC (DIG0027) p 4

[316] National Audit Office, The impact of government's ICT savings initiatives, (January 2013), para 17

[317] National Audit Office, The digital skills gap in government, (December 2015) p 30

Chris Johnson, representing the UK Computing Research Committee, who argued that it would be advisable for highly skilled employees to be more embedded in the procurement process, as much of what the Government was trying to procure was complicated.[318]

150. SME procurement was seen as a particularly important key to unlocking digital transformation and therefore maximising the potential of digitisation. UKCloud and PUBLIC, among others, argued that it offered an opportunity for the Government to support small business and engage with smaller, more flexible organisations that could offer agility and innovation.[319] In a roundtable that we hosted with SMEs and small GovTech companies (see Annex 1) we heard about the innovative ways that these organisations wanted to contribute to Government transformation, but they thought they were held back by procurement processes. Though it is possible for companies to find available contracts over £10,000 on the Government Contracts Finder website, there was a concern by tech companies that the information was scattered and hard to collate.[320] Despite recognition of the value that SMEs could play in digital transformation, the British Computing Society told us that, generally, contracts for SMEs were very complex because of unclear procurement frameworks, specifically with a lack of existing documentation about how Government IT systems operated, which made "it incredibly difficult for SMEs to get involved or realistically even take the financial risk and illustrates one of the key differences between public and private sector."[321] UKCloud also shared this perspective, explaining that, for SMEs, procurement frameworks were time consuming and costly, scattered on different procurement platforms, and had no consistency on durations, terms or products and services.[322]

GovTech Catalyst Programme

151. After the 2017 *Government Transformation Strategy* the GovTech Catalyst programme was launched in 2018 to support public sector organisations to find solutions to challenges through external tech companies that might not usually supply the Government.[323] Public sector organisations submitted their problems and applied for their share of the £20million GovTech Fund awarded via competitions, which, if successful, then provided support to define, develop, test and access creative solutions to these complex problems. The Cabinet Office told us that the GovTech Catalyst programme provided an "easy way" for private sector companies and social enterprises to develop their technologies, working directly with the Government, and assisting them to make their technology available across the whole of the public sector once it has been developed.[324]

152. We heard mixed views on whether the GovTech Catalyst Programme had been a success. techUK explained that the GovTech Catalyst was "an important opportunity to spread the use of digital services across Government and promote the use of new technologies",[325] whilst Daniel Korski, the CEO of PUBLIC, explained that the GovTech Catalyst had spread the use of innovative technology in some great areas, including, for example, using artificial intelligence to detect Daesh imagery that promoted a jihadi

[318] Qq226–227
[319] UKCloud Ltd (DIG0008) para 1.1; PUBLIC (DIG0027) p 2
[320] GOV.UK, "Contracts Finder", accessed 3 July 2019
[321] BCS, The Chartered Institute for IT (DIG0016) para 5.2
[322] UKCloud Ltd (DIG0008) para 1
[323] Government Digital Service, "The GovTech Catalyst challenge process", May 2018, last updated June 2019
[324] Cabinet Office (DIG0023) para 57
[325] techUK (DIG0022) para 11

message.[326] Conversely, at the GovTech roundtable, we heard from several GovTech SMEs and start-ups who thought the GovTech Catalyst was a good idea but had found it too bureaucratic and process heavy, particularly given that the fund was quite small (the GovTech Catalyst expects to fund 15 challenges in total) (see Annex 1).

153. In terms of the funding allocated to the scheme, there were suggestions of diverging views on whether it was enough. The then Director General of GDS, Kevin Cunnington, for example perceived that the fund was the right size.[327] While the Minister for Implementation did not question whether the size of the fund had been set at the right level initially, he suggested that more money for the GovTech Catalyst Fund would hopefully be agreed at the next spending round, as the "relatively small pot of money" had "now been used up".[328]

154. **The Government has introduced initiatives, such as G-Cloud, the Digital Marketplace and the GovTech Catalyst Fund, to try and open up digital/IT procurements to a broader pool of bidders. These have helped to partially overcome some barriers involved in procurement, including engagement with SMEs. However, further innovation in procurement is needed to encourage involvement from start-ups and SMEs so that their strengths can be drawn on to enable transformation.**

155. ***The Crown Commercial Service should produce a consultation immediately on the accessibility of the current Government technology procurement framework, asking for input from start-ups and SMEs on how accessible the current framework is. The consultation process (including a public response from the Government) should be concluded by Spring 2020, alongside the publication of a Government technology procurement strategy. The Minister should then provide this Committee with an update on how these are working within 12 months of publication.***

156. ***The Government should increase the funding pot for the GovTech Catalyst fund.***

[326] Q290
[327] Q335
[328] Q420

Conclusions and recommendations

Government digitisation

1. The open-ended definition of "digital" has meant that it is hard to assess the full scale of any progress that the UK Government has made with its digitisation agenda. We believe that Government digitisation should be defined as transforming how services are delivered so that the relationship between the citizen and the State is enhanced. *The Government should adopt this definition and set out metrics of success. Departments and associated Agencies should be required to publicly report against these metrics on an annual basis, starting from the financial year 2020/21, highlighting areas of success and areas for improvement. The Cabinet Office should be responsible for overseeing departments' action plans in response to this annual publication.* (Paragraph 15)

2. Single unique identifiers for citizens can transform the efficiency and transparency of Government services. We welcome the Government's announcement in June 2019 that it will consult shortly on digital identity. While we recognise that in the UK there are concerns about some of the features of a single unique identifier, as demonstrated by the public reaction to the 2006 Identity Card Act, we believe that the Government should recognise the value of consistent identity verification. *The Government should facilitate a national debate on single unique identifiers for citizens to use for accessing public services along with the right of the citizen to know exactly what the Government is doing with their data.* (Paragraph 34)

3. While we believe it is important for the Government to make its services end-to-end digital, it must do this in such a way that it includes access to public services for those who are not digitally connected. The Government must ensure that public spaces with digital access, such as libraries, are maintained. *The Government must ensure that public spaces with digital access, such as libraries, are maintained. The Government should also ensure that those who are not digitally connected have alternative ways of accessing services, for example, by using the phone or having assistance to use digital services, and those alternatives are properly promoted.* (Paragraph 36)

Levers for transformation

4. Data-sharing is key to ensuring that digital Government can be transformative. It enables departments to work together to produce efficient public services that work for the citizen, thus improving the citizen-Government relationship. We welcome that the Government has commenced phase one of developing its National Data Strategy. *As part of this process to inform the content of the National Data Strategy, DCMS should conduct an audit of data-sharing amongst Government departments to see where best practice is taking place, and identify which departments are particularly siloed. Further, the audit should also determine to what extent the initial recommendations by Martha Lane Fox were adopted. This audit should be completed and published in advance of the National Data Strategy being published in Winter 2020 so that its findings can inform the National Data Strategy.* (Paragraph 46)

5. We welcome the Government's establishment of a Data Advisory Board. However, at present its membership, agenda and decisions are not a matter of public record. *In response to this Report, the Government should set out how it will make the work of the Data Advisory Board more transparent. It should make public its membership, agenda and a summary of its decisions. If the Government decide that it is not possible to make the Board more transparent then it should set out its reasons why.* (Paragraph 50)

6. It is disappointing that the Government has not appointed a Chief Data Officer, some time after it committed to do so in the 2017 Government Transformation Strategy. *The Government should appoint a Chief Data Officer by the end of 2019.* (Paragraph 51)

7. The Government has made positive commitments to artificial intelligence and harnessing its value for transformation. It is too early to assess to what extent the National Data Strategy and Industrial Strategy will impact the Government's use of innovative technologies. We are concerned, however, that a lack of central leadership for the use of AI and other innovative technologies in Government services may result in inconsistent deployment across departments. (Paragraph 61)

8. *The Government should make the Government Office for AI responsible, as a central body, for leading on ensuring that all departments take advantage of the transformative benefits that Artificial Intelligence and other innovative technologies offer.* (Paragraph 62)

9. We welcome the steps that the Government has taken to enhance public trust in data use, including the establishment of the Centre for Data Ethics and Innovation. However, we are concerned that the Government might be taking an overly-cautious approach and second-guessing citizens' views on how their data should be used. *DCMS should ensure that the Centre for Data Ethics and Innovation annually assesses public opinion on Government data use. This review should start in summer 2019 and should aim to report by Spring 2020.* (Paragraph 70)

Cultural challenges

10. Political leadership in digitisation has been lacking in recent years since Francis Maude ceased being Minister for the Cabinet Office. This, coupled with the departure of senior Civil Service figures in GDS, has resulted in a slowing in the Government's digital momentum, as evidenced by other countries overtaking the UK in international rankings. It is now necessary to put in place processes which embed digitisation at a department-level and across the Civil Service. (Paragraph 81)

11. *The Government should introduce a ministerial digital champion in every department by the end of 2019 who has responsibility for using innovation and digitisation to transform the way their department operates. These champions will need to co-ordinate at a department level and across departments. In response to this Report the Government should set out how this co-ordination will take place.* (Paragraph 82)

12. GDS made good progress in its early years on standards and platforms that applied across Government. However, we heard how GDS has "lost its way somewhat" and

its purpose is now less clear. *GDS's purpose should be twofold: to provide advice to departments when needed, but also to devise and enforce minimum standards to be applied consistently across Government digital services. Departments, with the relevant capacity, should retain the ability to develop platforms and software. The Government needs to clarify GDS's role and its relationships with other departments, as well as determining with GDS whether there are any powers it needs to compel departments to take particular action.* (Paragraph 91)

13. It is too early to tell if the move of data policy to DCMS presents a challenge or an enhancement for Government digitisation. *We urge the Government to keep under review whether DCMS should be the lead department for open data and data ethics, governance and sharing. Further, in response to this Report, the Government should set out whether DCMS requires any additional powers to drive data reform across Government. If it does not deem this necessary it should set out why.* (Paragraph 96)

Technical challenges

14. Legacy systems are a significant barrier to effective Government transformation and digitisation. We acknowledge the attempts of the Government, its predecessors and individual departments to produce guidance and to deal with legacy issues. However, the same issues frequently recur, suggesting that the Government and GDS's advice has not been fully implemented. We acknowledge that there is a significant cost attached to the replacement of legacy systems, which the Treasury must resource adequately. (Paragraph 113)

15. *GDS should conduct an audit of all legacy systems across Government, including where they are based, what actions to take, the expected cost of such action and the resulting timescales. GDS's framework of retain (do nothing), retire (drop), re-host (lift and shift), repurchase (shop and drop), re-platform (life and shape) should be used to determine what actions to take with each legacy system. The audit should assess which approach is most realistic but 'retain' should not be used widely as the proposed action in the long-term as there is clear evidence that the legacy system issue is going to increase over time and there are challenges with regard to the skills for supporting such systems. GDS should seek to publish the findings of this audit. This audit should be completed no later than December 2020.* (Paragraph 114)

16. More needs to be done to centralise leadership of cyber security policy and ensure that all departments are prioritising it in the same way. Responsibility in Government for cyber security policy is spread between departments to ensure checks and balances are in place, but we are concerned that this may result in a lack of accountability for specific incidents. We support the 2018 recommendation of our colleagues on the Joint Committee on the National Security Strategy that there should be a Minister for Cyber Security. *The Government should reconsider creating a Minister for Cyber Security who will be able to hold Ministers across Government to account for their internal cyber security. This Minister would also be responsible for working with other public sector bodies, including the NHS and local Government, to ensure that best practice and guidance was being shared across the public sector.* (Paragraph 123)

17. The Government has taken positive steps to develop cyber security standards. Despite this we remain concerned that cyber security policy varies between departments

even if there are minimum cyber security standards. This creates unnecessary procurement barriers particularly for SMEs and small tech providers. *The Cabinet Office should review their universal, departmental cyber security standards and ensure they are sufficient, and clearly set out the requirements that bidders must meet to be eligible for Government procurements by the end of 2019. If any department wishes to diverge from these standards, they should have to make a case to the Minister for Implementation.* (Paragraph 128)

Institutional challenges

18. The Government, including GDS, has made good attempts to tackle the digital skills shortage, through academies, creating job roles and considering progression pay. Nonetheless, more action is needed to ensure that digital skills capabilities are sustainable and not significantly affected by turnover of staff that is an issue for the digital workforce in both the public and private sector. (Paragraph 138)

19. *The Government should publish a strategy by mid-2020 covering how it intends to make digital skills sustainable. It should also set out the ways in which it plans to continue to raise the skill levels of the Government workforce, ensuring that it is attracting and retaining the best and most digitally skilled employees as well as spreading best practice to staff working in roles which are predominantly non-digital.* (Paragraph 139)

20. The Government has introduced initiatives, such as G-Cloud, the Digital Marketplace and the GovTech Catalyst Fund, to try and open up digital/IT procurements to a broader pool of bidders. These have helped to partially overcome some barriers involved in procurement, including engagement with SMEs. However, further innovation in procurement is needed to encourage involvement from start-ups and SMEs so that their strengths can be drawn on to enable transformation. (Paragraph 154)

21. *The Crown Commercial Service should produce a consultation immediately on the accessibility of the current Government technology procurement framework, asking for input from start-ups and SMEs on how accessible the current framework is. The consultation process (including a public response from the Government) should be concluded by Spring 2020, alongside the publication of a Government technology procurement strategy. The Minister should then provide this Committee with an update on how these are working within 12 months of publication.* (Paragraph 155)

22. *The Government should increase the funding pot for the GovTech Catalyst fund.* (Paragraph 156)

Annex One: Roundtable with GovTech SMEs

1) On Thursday 24 January 2019, a roundtable event was held in Westminster. 15 SMEs and start-up private tech companies who provided public services met with the Chair of the Science and Technology Committee, Rt Hon Norman Lamb MP, and Committee members Mr Sam Gyimah MP and Darren Jones MP. This was an opportunity to discuss with the representatives their views on Government use of innovative technology.

The GovTech Catalyst

2) The GovTech Catalyst was launched in 2018 to support public sector organisations to find solutions for challenges, such as traffic management and rural isolation, through external tech companies. Public sector organisations submitted their problems and applied for a share of the £20 million GovTech Fund to run a procurement within the private sector support to define, develop, test and access creative solutions to complex public-sector problems. The objective of this fund was to incentivise the UK's own tech firms to devise solutions for public sector problems.

Points of discussion

3) Government departments and local Government bodies had built their own bespoke platforms and services when there were SMEs providing exact or similar services which were not being procured. Many of the companies thought that this approach was due to cultural "risk aversion" or a consequence of the complicated bureaucratic process which made local Government and the UK Government reluctant to use platforms created by SMEs.

4) Some parts of the procurement process created a barrier to start-ups being awarded contracts as smaller companies might not have made a profit at first, which could mean that larger more "risk-averse" companies were favoured. Having a Government contract would give the SME the stability that the Government was seeking.

5) The implementation of an insurance framework would mitigate some of the risk that concerned the Government.

6) The GovTech Catalyst was too bureaucratic and process heavy, particularly given that the fund was quite small.

7) The Small Business Research Initiative could be utilised to encourage start-ups to work with the Government and to create a central fund.

8) The G-Cloud was seen as a step in the right direction for procurement in general, but the requirement to contract through a third party meant that cost was being added.

9) Some companies would appreciate if they could apply to the preferred frameworks more frequently, as applications were capped at every four to five years.

10) International exemplars of engaging SMEs highlighted, included: Boston, Chile and South Korea who were all engaging "positively" with SMEs.

Annex Two: Meeting with the Estonian Ambassador

1) On Thursday 7 March 2019, the Chair of the Committee, Rt Hon Norman Lamb MP, met with the Estonian Ambassador, Tiina Intelmann and a representative from the e-Estonia Briefing Centre, Tobias Koch.

Points of discussion

2) Accessibility was a key feature of e-Estonia. Access to the internet had been legislated for in 2000 as a "social right", meaning that the public had a right to communicate with the government over the internet.

3) The 2007 cyber attack against the Estonian Government infrastructure was intended to destabilise the Government and e-Estonia had learned many lessons from this attack.

4) In 2008, Estonia became the first Nation State in the world to deploy blockchain technology in production systems. Estonia used blockchain technology for integrity verification of government registries and data. Blockchain was utilised to ensure that data was appropriately protected, ensuring all access to data was appropriately authorised and traced.

5) The Estonia data model was described as a consent-transparency hybrid. Though consent was not "explicit" in every step, citizens had a right to 'opt-out' of data being held and the Government was obliged to tell citizens why and how it had accessed their data.

6) The introduction of electronic ID cards in 2002 was considered a success, with many countries following Estonia's lead and implementing similar systems. With regard to civil liberty issues relating to ID cards the Estonian view was that sharing of data among government departments, with little transparency over who had accessed it and why, such as in the UK system, presented more of a civil liberties issue due to the lack of transparency and accountability.

Annex Three: Meeting with the Chief Digital and Information Officer, HMRC

1) On Tuesday 26 March 2019, Jacky Wright, Chief Digital and Information Officer, HMRC, met with the Chair of the Committee, Rt Hon Norman Lamb MP, to discuss digital Government and the Committee's inquiry.

Points of discussion

2) Current work: Jacky joined HMRC as its IT contract with Aspire ended. Since then, her priorities had included:

- ensuring the right capability and resourcing strategy was in place—achieving the correct blend between in-sourcing and out- sourcing;
- building a secure IT foundation, including the IT legacy estate; and
- continuing HMRC's digital transformation journey, including developing a data culture that exploited appropriately the data HMRC held.

3) HMRC had a data governance board. HMRC viewed trust as a critical part of making better use of data. Transparency was an important part of this process. Through transparency they also wanted to understand how to mitigate the ethical ramifications of data-sharing.

4) Successes: HMRC had undertaken an extensive discovery and assessment of its systems to identify legacy issues and appropriate remediation plans. It was identifying systems that needed to migrate, those that could be redesigned for the cloud and those that it could deprecate. "Securing Our Technical Future" was a programme to rationalise and modernise HMRC's existing IT infrastructure and migration to the cloud.

5) HMRC engaged in mutual sharing of digital and technology best practice with other departments and organisations outside the Government. In particular, HMRC worked closely with DWP due to the mutually collaborative relationship and interplay of taxation and welfare.

6) It also utilised GDS's offering as it related to the digital, data and technology professions, development and learning.

7) Areas for improvement: HMRC thought that the Government had a pivotal role to play in setting protocols and standards and rules of engagement for data use across organisations in both the public and private sector. When asked how the Government should be leading on data ethics policy, HMRC saw the value of the newly established Centre for Data Ethics and Innovation taking a role in consulting departments on their data policies. The Centre had an important potential role in connecting public thought and opinion on data with the creation of policy.

8) The current lack of central co-ordination and drive around data, given the federated data model across Government, meant that there was a need to ensure a framework of common standards to enable interoperability, and a need for a central enforcement of common standards and protocols to ensure they are implemented within Government.

9) When Jacky arrived at HMRC, digital capability had been in the hands of HMRC's suppliers. HMRC had been working to bring key core capabilities back in-house and to make better use of SMEs. Attracting early career talent to work in HMRC would be easier if people understood the ambitious work that was in progress. HMRC was currently working on brand and external presence.

10) HMRC explained that there remained some commercial constraints on the effective use of SMEs in terms of the ease of their participation in Government work. More work was required on getting Government procurement fit for purpose.

11) There was disparate data throughout Government but this was a particular problem for HMRC due to the age of its legacy systems and the need for effective collaboration with other departments, such as DWP. This would continue to be a challenge as HMRC balanced the need to perform while it transformed.

12) HMRC continued to drive the need to bring together data held across more than one system and department, as shown by PAYE, Self-Assessment, National Insurance, Tax Credits, Child Benefit, Marriage Allowance and the State Pension.

13) The checks and balances of multiple bodies having control over cyber security policy was thought necessary and overlap was viewed as positive in ensuring that policy was as thoroughly constructed as possible. It was acknowledged that GDS, could increase its role with regard to cyber security to include working to agree appropriate standards and protocols, and helping the public sector to work towards implementation. It could be playing a vital role around knowledge sharing and helping tackle common problems, such as data and legacy systems.

14) Role of GDS: GDS should evaluate a governing role versus an operational role. In this way, GDS would not be responsible for the building of systems, but should work with departments in identifying existing systems that could be scaled-up for wider cross-Government use. Departments could then work with GDS to ensure that what they designed and built was suitable for multiple departments rather than GDS building systems which did not reflect operational requirements.

Formal minutes

Wednesday 3 July 2019

Members present:

Norman Lamb, in the Chair

Bill Grant	Graham Stringer
Damien Moore	Martin Whitfield

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

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

Paragraphs 1 to 156 read and agreed to.

Annexes and Summary agreed to.

Resolved, That the Report be the Eighteenth 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).

[Adjourned till Tuesday 9 July at 9.00 am

Witnesses

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

Tuesday 27 November 2018

Tom Loosemore, Partner at Public Digital, former Deputy Director of the Government Digital Service (2011–2015), and **Dafydd Vaughan**, Director, Cedyrn Ltd Q1–80

Tuesday 4 December 2018

Sam Smith, Coordinator, medConfidential, **Professor Vishanth Weerakkody**, Professor of Information Systems Management and Governance, University of Bradford, **Robert McLaren**, Head of Industry, Technology and Innovation, Policy Connect, and **Professor Helen Kennedy**, Professor of Digital Society, University of Sheffield Q81–137

Dr Fiona Lugg-Widger, Research Associate for Routine Data, Centre for Trials Research, **Tom Smith**, Managing Director of the Data Science Campus, Office for National Statistics, **Joel Bellman**, Partner, Deloitte, and **Cllr Peter Fleming**, Chairman of the LGA Improvement and Innovation Board, Local Government Association Q138–196

Tuesday 8 January 2019

Simon Hansford, Co-founder and Chief Executive, UKCloud, **Professor Chris Johnson**, Member of the Executive Committee, UK Computing Research Committee, and **Antony Walker**, Deputy Chief Executive Officer, techUK Q197–264

Professor Helen Margetts, Programme Director for Public Policy, The Alan Turing Institute, **Peter Wells**, Head of Policy, Open Data Institute, and **Daniel Korski**, Co-founder and Chief Executive Officer, PUBLIC Q265–309

Monday 4 March 2019

Matthew Gould, Director General for Digital and Media Policy, Department for Digital, Culture, Media and Sport, **Kevin Cunnington**, Director General, Government Digital Service, and **Simon McKinnon**, Interim Chief Digital and Information Officer, Department for Work and Pensions Q310–385

Margot James MP, Minister for Digital and Creative Industries, Department for Digital, Culture, Media and Sport, and **Oliver Dowden MP**, Minister for Implementation, Cabinet Office Q386–467

Published written evidence

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

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

1 360Giving (DIG0019)

2 The Alan Turing Institute (DIG0005)

3 BCS, The Chartered Institute for IT (DIG0016)

4 Cabinet Office (DIG0023), (DIG0034)

5 Centre for Trials Research, Cardiff University (DIG0006)

6 Cloud Kickers (DIG0033)

7 defenddigitalme (DIG0021)

8 Deloitte LLP (DIG0014)

9 Department for Digital, Culture, Media and Sport (DIG0031)

10 Department for Digital, Culture, Media and Sport and the Cabinet Office (DIG0032)

11 Doctors in Unite (The Medical Practitioners' Union) (DIG0030)

12 Dr Louise Bennett, Information Assurance Advisory Council (IAAC) and Dr Edgar A Whitley, London School of Economics and Political Science (DIG0017)

13 Durant, Mr David (DIG0020)

14 GlobalData Public Sector (DIG0024)

15 Kaspersky Lab (DIG0010)

16 The Legal Education Foundation (DIG0029)

17 Local Government Association (DIG0018)

18 medConfidential (DIG0025), (DIG0028)

19 Moss, Mr David (DIG0013)

20 Office for National Statistics (DIG0012)

21 Open Rights Group (DIG0026)

22 Policy Connect (DIG0011)

23 PUBLIC (DIG0027)

24 The Royal Statistical Society (DIG0009)

25 SAS (DIG0015)

26 Stamper, Professor Ronald (DIG0001)

27 techUK (DIG0022)

28 UK Computing Research Committee (DIG0002)

29 UKCloud Ltd (DIG0008)

30 University of Bradford (DIG0003)

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	Pre-appointment hearing: chair of UK Research & Innovation and executive chair of the Medical Research Council	HC 747
Second Report	Brexit, science and innovation	HC 705
Third Report	Genomics and genome editing in the NHS	HC 349
Fourth Report	Algorithms in decision-making	HC 351
Fifth Report	Biometrics strategy and forensic services	HC 800
Sixth Report	Research integrity	HC 350
Seventh Report	E-cigarettes	HC 505
Eighth Report	An immigration system that works for science and innovation	HC 1061
Ninth Report	Flu vaccination programme in England	HC 853
Tenth Report	Research integrity: clinical trials transparency	HC 1480
Eleventh Report	Evidence-based early years intervention	HC 506
Twelfth Report	Quantum technologies	HC 820
Thirteenth Report	Energy drinks and children	HC 821
Fourteenth Report	Impact of social media and screen-use on young people's health	HC 822
Fifteenth Report	Evidence-based early years intervention: Government's Response to the Committee's Eleventh Report of Session 2017–19	HC 1898
Sixteenth Report	'My Science Inquiry'	HC 1716
Seventeenth Report	Japanese knotweed and the built environment	HC 1702
First Special Report	Science communication and engagement: Government Response to the Committee's Eleventh Report of Session 2016–17	HC 319
Second Special Report	Managing intellectual property and technology transfer: Government Response to the Committee's Tenth Report of Session 2016–17	HC 318
Third Special Report	Industrial Strategy: science and STEM skills: Government Response to the Committee's Thirteenth Report of Session 2016–17	HC 335

Fourth Special Report	Science in emergencies: chemical, biological, radiological or nuclear incidents: Government Response to the Committee’s Twelfth Report of Session 2016–17	HC 561
Fifth Special Report	Brexit, science and innovation: Government Response to the Committee’s Second Report	HC 1008
Sixth Special Report	Algorithms in decision-making: Government Response to the Committee’s Fourth Report	HC 1544
Seventh Special Report	Research integrity: Government and UK Research and Innovation Responses to the Committee’s Sixth Report	HC 1562
Eighth Special Report	Biometrics strategy and forensic services: Government’s Response to the Committee’s Fifth Report	HC 1613
Ninth Special Report	An immigration system that works for science and innovation: Government’s Response to the Committee’s Eighth Report	HC 1661
Tenth Special Report	Research integrity: clinical trials transparency: Health Research Authority Response to the Committee’s Tenth Report	HC 1961
Eleventh Special Report	Quantum technologies: Government Response to the Committee’s Twelfth Report	HC 2030
Twelfth Special Report	Impact of social media and screen-use on young people’s health: Government Response to the Committee’s Fourteenth Report	HC 2120