Witness Name: Susannah Storey
Statement No.: WITNXXXX
Exhibits: [SS/1 - SS/34 & INQ numbers]
Dated: [21/04/2023]

UK COVID-19 INQUIRY

WITNESS STATEMENT OF SUSANNAH STOREY

I, Susannah Storey, will say as follows: -

Contents

Preface

0.1. This statement has been authored by Susannah Storey. I am the Director General for Digital, Technology and Telecoms at the Department for Science, Innovation and Technology (DSIT). Until 7 February 2023, I was the Director General for Digital and Media at the Department for Digital, Culture, Media and Sport (DCMS). The 'digital' part of DCMS was moved across to the newly created Department for Science, Innovation and Technology (DSIT) as a result of the machinery of government changes announced on 7 February 2023. Throughout this statement, when I refer to DCMS I am referring to the department's previous functions as the DCMS prior to the machinery of government changes. I make this statement pursuant to a Rule 9 request from the Inquiry dated 24 November 2022 and follow-up questions dated 15 February 2023.

0.2. This statement is provided in response to the Inquiry Chair's request for a witness statement covering the issues raised in the 'Provisional Outline of Scope for Module 1' ("M1") of the Covid-19 public inquiry. M1 is concerned with the UK's preparedness for whole-system civil emergencies, including resourcing, the system of risk management and pandemic readiness.

0.3. The focus of this statement is specifically on the government's Counter Disinformation Unit. This statement should be read alongside the broader M1 statement submitted by the Department of Culture, Media and Sport, and signed by Sam Lister, Director General for Strategy and Operations, which includes more general information on DCMS's structure and planning.

Section 1: The Counter Disinformation Unit

Overview of the Counter Disinformation Unit

1.1. His Majesty's Government (HMG) defines disinformation as the deliberate creation and dissemination of false and/or manipulated information that is intended to deceive and mislead audiences, either for the purposes of causing harm, or for political, personal or financial gain. Misinformation refers to inadvertently spreading false information.

Historical development of the CDC and CDU

1.2. DCMS (now DSIT) currently leads the government's overall counter disinformation policy and operational response to disinformation incidents which impact UK audiences. The operational response is led by the Counter Disinformation Unit (CDU) which sits within DCMS. A policy team leading on disinformation was first established

in March 2018, following the Salisbury poisonings[1]. This team drove the creation of a Counter Disinformation Cell (CDC) in 2019. This was a virtual, cross-Whitehall team which was led by DCMS, and was designed to come together for specific events. The CDC was the first formal structure designed to operationally manage disinformation impacting the UK.

1.3. Over the course of the pandemic response in 2020, the government moved away from this approach. The CDC evolved into the Counter Disinformation Unit (CDU), a permanent DCMS (now DSIT) team that works with other departments and serves as the government's lead for countering disinformation targeting domestic audiences. For ease, throughout this statement, we shall use 'Counter Disinformation Unit', or 'CDU', to refer to the DCMS disinformation team throughout its existence even though it has only become known as the CDU more recently. It is important to note that the CDU is different in make up and intent from the CDC, the latter being a now defunct virtual cross-Whitehall structure of which DCMS was a part.

1.4. The development of DCMS's thinking on disinformation began with the 2017 Internet Safety Strategy Green Paper. The government's response to that paper, published in May 2018, set out the intention to manage new and emerging issues, including disinformation [**SS/1 INQ000102740**]. The focus was to prevent misleading information from being disseminated for political, personal, and/or financial gain. In August 2018, cross-government discussions, led by the Cabinet Office (CO), were held on developing a counter disinformation strategy [**SS/2 INQ000102749**].

1.5. In January and February 2019, the CDU identified key cross-Whitehall stakeholders for the formation of a cross-Whitehall Counter Disinformation Cell (CDC). This structure was intended to provide the most comprehensive picture possible about the level, scope and impact of disinformation during times of heightened risk. An early official draft outlines the rationale for this and identifies the key stakeholders and teams [**SS/3**].

1.6. On 7 February 2019, DCMS chaired a disinformation roundtable with the relevant Whitehall stakeholders (identified in January 2019) to discuss the structure and make-up of a potential cross-Whitehall CDC [**SS/4 INQ000102753**]. In this meeting a general election scenario was used to test the CDC's proposed structure [**SS/5**] and establishing working relationships with social media platforms was also discussed. On 15 February 2019, DCMS chaired a second disinformation roundtable discussion, which focused on developing the cross-Whitehall response structure.

1.7. On 20 February 2019, DCMS's CDU sent a submission to the DCMS Minister for Digital and Creative Industries setting out DCMS's approach to the coordination of a cross-Whitehall response to disinformation, particularly in periods of heightened sensitivity [**SS/6 INQ000102799**]. The aim of this was:

"to strengthen Government capability in this area through three work streams:

[1] The use of the nerve agent Novichok in the attempted assassination of Sergei and Yulia Skripal in the UK city of Salisbury in March 2018.

a) cross-Whitehall coordination of operational capabilities
b) cross-Whitehall collaboration with major social media platforms
*c) strengthening public resilience" [**SS/6 INQ000102799**] (2).*

1.8. On 25 February 2019, there was a third disinformation roundtable in which Whitehall stakeholders continued to discuss the CDC's structure.

1.9. The CDC was formally established in March 2019 after No.10 wrote to departments setting out the Prime Minister's position on ministerial responsibilities for countering disinformation [**SS/7 INQ000102807**]. While this strategy was a pan-government effort, the DCMS Secretary of State was tasked with leading on overall counter disinformation policy:

> *"The Culture Secretary will formally lead on HMG's overall counter-disinformation policy in order to provide a single spokesperson to set out the Government's position and coordinate the delivery of the disinformation strategy. This role includes setting the direction, focus and principles of domestic policy; leading our engagement with social media companies and the media; working with partners to further the aims of the strategy and representing and promoting domestic activity amongst our international partners and the public. DCMS should consider the wider problem of online manipulation and will need to work closely with other departments in their respective policy areas, commissioning expert advice from them when necessary. In designating this responsibility, I hope this will facilitate a unified areas approach that aligns a range of cross-government activity." [**SS/7 INQ000102807**] (P2)*

1.10. Reflecting the direction from No 10, the key departments that made up the CDC alongside DCMS were the Foreign, Commonwealth and Development Office (FCDO), Cabinet Office (CO) and Home Office (HO). The UK Intelligence Community was also involved. DCMS subsequently worked with CO and other departments to ensure that disinformation risks were accurately reflected in the National Security Risk Assessment[2] in 2019 and 2020. Further to this work, disinformation was included as a risk in the public National Risk Register[3] for the first time in 2020.

1.11. DCMS stood up the cross-Whitehall CDC on 5 March 2020 in response to the acute disinformation risks emerging from the Covid-19 pandemic. As set out in paragraph 1.10, the CDC drew on a range of cross-government teams, bringing together relevant expertise from CO, HO and FCDO, and working closely with the UK Intelligence Community where appropriate. At its peak, the CDC was formed of a team of up to 50, however, this figure is indicative. The CDC was virtual and flexible

[2] The National Security Risk Assessment (NSRA) is the main tool for assessing the most serious civil contingencies risks facing the UK. The NSRA assesses, compares and prioritises the top national level risks facing the UK, focusing on both likelihood of the risk occurring and the impact it would have, were it to happen. The NSRA is an internal government document, with the process run and owned by CO. A public version - the National Risk Register - is published after each refresh of the NSRA.
[3] The National Risk Register is available at https://www.gov.uk/government/publications/national-risk-register-2020

in nature, with DCMS and other departments pulling on their wider resources (which may not have been entirely focused on disinformation) as needed. DCMS can only be certain in its figures for its own departmental FTE. Core staffing levels within the DCMS disinformation policy team varied between 6-10 FTE. Additional staff (surge capacity) were brought in wherever needed, including for the pandemic response, when the DCMS core team reached c.25 FTE at its peak. The CDC structure was limited to government teams so engagement with platforms and wider civil society took place outside of this structure.

1.12. Over the course of the pandemic response in 2020, government moved away from this approach with the CDC evolving into the Counter Disinformation Unit (CDU), a permanent DSIT (formerly DCMS) team that works with other departments and serves as the government's lead for countering disinformation targeting domestic audiences. Staffing requirements are continually reviewed to ensure appropriate levels of resourcing, including surge capacity as needed.

Current CDU ways of working and oversight

1.13. The CDU, as part of the wider security and online harms directorate within DSIT (formerly DCMS) is overseen by and accountable to its departmental ministers, as well as facing scrutiny from relevant parliamentary committees.

1.14. In cases where the CDU seeks to establish a sustained provision of monitoring for disinformation narratives it seeks ministerial agreement to do so (as it did for the Russian invasion of Ukraine, and during the Covid-19 pandemic). All monitoring is conducted in accordance with relevant legislation and gives due consideration to protecting freedom of expression online, as set out below.

1.15. The CDU aims to reduce the potential impact of disinformation on UK democracy, society, and economic and national security interests in line with UK democratic values. The CDU does not seek out, nor aim to respond to, all incidents of mis- and disinformation, but rather seeks to understand mis- and disinformation narrative trends online which have the potential to cause harm to UK audiences, in order to build an assessment of the risks and threat. The circumstances in which the CDU 'stands up' are agreed by DSIT ministers, as are the areas of monitoring within a particular topic.

1.16. The CDU works with a range of partners including other government departments, social media platforms, academia, civil society and external monitoring partners to produce a comprehensive picture of disinformation and misinformation. DSIT holds a key role in understanding the threat landscape, developing the overarching counter disinformation policy for the government and working with social media platforms to flag content to relevant social media platforms (as set out in 1.19) or working with the platforms to ensure that they are aware of and, where possible, seek to promote the government's authoritative sources.

1.17. However, there are limitations to the effectiveness of these actions in isolation, and there may be times when it is appropriate to deploy a different or complementary

response, such as a direct rebuttal or government public engagement strategies and campaigns to develop and promote authoritative facts and sources. Such efforts are usually led by relevant strategic communications teams in other departments (such as DHSC in relation to Covid-19), with CDU insights used to inform their development. For example, when the CDU identified a spike in 5G disinformation in April 2020, DCMS and CO communications teams worked to promote authoritative information including via the creation of a dedicated gov.uk page linking to independent sources of verified information[4].

1.18. When considering specific content or narratives and determining whether these are false or harmfully misleading, in line with the HMG definition in paragraph 1.1 above, the CDU utilises fact-checking (including via authoritative government sources and the relevant lead departments, such as DHSC on health and Covid-19) and news reporting, considering these against terms of service for the purposes of escalation to social media companies. Any potential escalation is governed by internal processes and oversight (as set out in **SS/8 INQ000174766**) to ensure there is no interference with legitimate democratic debate with opportunities for challenge at each stage. Ministers would be made aware of any content or narratives which raised particular issues or sensitivities. The ultimate arbiters of whether any action was taken on specific pieces of content were the social media platforms concerned, in line with their terms of service and policies. The CDU did not mandate any action, flagging content for consideration only. These principles were core to the work of the CDU throughout the pandemic and remain in a similar form today.

CDU approach to protecting freedom of expression when escalating content to social media platforms

1.19. The primary purpose of the CDU is not to monitor for harmful content to flag to social media platforms, but to understand the disinformation landscape which has the potential to impact UK audiences, as outlined in paragraph 1.15. HMG does not seek to, nor does it have the legal power to compel social media platforms to remove mis- and disinformation content. However, when in the course of its work the CDU identifies content which potentially violates platforms' terms of service, including coordinated inauthentic or manipulated behaviour, CDU may decide to escalate the content to the platform. This escalation is done following robust assessment against the platform's own individual terms of service, and detailed consideration of both the risk of harm to public safety or health (in consultation with the relevant policy department if necessary) and any potential impact on freedom of expression. It is then up to the platforms to decide whether or not to take action against the content, based on their terms of service and their own assessment. CDU does not, and cannot, mandate any action by the platform. Therefore any appeal or challenge on the nature of the content and whether it did indeed breach a platform's terms of service would be with the platform in question, rather than the government.

1.20. As a matter of principle the CDU does not escalate content to platforms from elected

[4] https://www.gov.uk/guidance/5g-and-coronavirus-covid-19

politicians, journalists or established news outlets. The CDU double-checks the sources of content and has robust internal oversight systems in place ahead of any decision being made to flag content to platforms.

1.21. The CDU operates in full compliance with all applicable legislation including, but not limited to, human rights laws such as the European Convention on Human Rights (ECHR) and the Human Rights Act 1998 (HRA). The CDU does this by making sure that its staff are aware of the applicable legislation and the consequences of failure to comply with any applicable legislation i.e. enforcement or other action, such as legal proceedings, being taken against DSIT. Further, the CDU has a series of processes and checks in place to ensure that legislation is complied with. For example, staff have to be satisfied that all data monitoring and analysis which they conduct is lawful, necessary and proportionate, and that they have the appropriate internal legal advice and senior approvals.

1.22. The CDU is committed to protecting freedom of expression in line with the UK's democratic values and does not seek to limit or impact political debate or opinion. The CDU continually develops and implements solutions to the challenges of mis- and disinformation that are consistent with our principles and values, protecting freedom of expression and promoting a free, open and secure internet.

Inter-organisational processes and cooperation

1.23. In early 2019, the CDU developed and worked through a plan for a disinformation crisis response and timeline of planned crisis response work, as set out in paragraphs 1.5-1.10 **[SS/9]**; **[SS/10 INQ000102769]**. This work allowed the building of closer relationships with the identified cross-Whitehall disinformation teams.

1.24. In April 2019, a wash up meeting took place to discuss findings from a three day disinformation-focused exercise involving teams from DCMS, the HO, CO and FCDO. This reported that the participants found the exercise useful and were generally reassured by the collective response. It stressed the need for strong communication links throughout the cell as well as good relationships with social media companies so they can assist with monitoring mis- and disinformation **[SS/11]**.

1.25. During the first half of 2019, at the request of DHSC, working-level discussions were held with DCMS policy officials to discuss DCMS's approach to mis- and disinformation in response to DHSC concerns about the link between falsehoods online and a broad decline in vaccination uptake. Following this engagement, DHSC and DCMS began a dialogue around the inclusion of disinformation in the Online Harms White Paper[5], and how anti-vaccine content fitted within that regulatory framework. DHSC was subsequently invited to join the cross-Whitehall counter disinformation working group in 2019 - an informal group created to forge links between relevant departments and to build a wider counter disinformation community. Collaboration between DCMS and DHSC in tackling vaccine

[5] The Online Harms White Paper sets out the government's plans for a package of measures to keep UK users safe online

misinformation was noted in *'England's Vaccine Strategy to 2030: protecting everyone, everywhere against vaccine-preventable disease'* which stated: "*We will continue to work with social media companies to agree what joint action is needed for tackling misinformation on vaccination and hold a summit, in partnership with the Department for Digital, Culture, Media and Sport, to discuss these issues further*". We held a series of events with social media companies, explored in more detail at paragraph 1.54.

1.26. In March 2020 the CDU engaged with the existing vaccine policy team in DHSC, DHSC communications teams and, in due course, the newly established UK Covid-19 vaccine security team. DCMS worked closely with these teams to share insights on Covid-19 mis- and disinformation and help inform communications strategies and interventions led by those teams.

1.27. Throughout 2019, the CDU also worked directly with the CO National Security Communications Team (NSCT) which ran the "Don't Feed the Beast" campaign. This was a public campaign intended to build resilience to misinformation among UK domestic audiences. The campaign created the 'SHARE checklist'[6], which provided the public with five easy steps to identify false content, encouraging users to stop and think before they share content online. It targeted 18-34 year olds and encouraged them to think critically about information before sharing online, running in two waves in autumn 2019 and spring/summer 2020.

Work with the media, social media, and the wider information sectors

1.28. Since 2019 DCMS has worked with social media platforms (principally Meta (formerly Facebook), YouTube, Twitter and TikTok) on the subject of disinformation. In March 2019, as part of work on the cross-government approach to disinformation crisis response (set out in paragraphs 1.5-1.10), it was agreed that DCMS would take on a central role in platform engagement, to improve coordination across government and in line with the direction in the letter from No. 10 [**SS/7 INQ000102807**].

1.29. In early 2019, DCMS held various meetings, presentations and workshops with social media companies to discuss a range of online harm issues (including but not limited to disinformation) and to help improve cooperation between the government and industry. For example, in July 2019, a meeting was held along with the Royal Society for Public Health to discuss anti-vaccine messaging, the minutes of which are exhibited [**SS/12 INQ000102794**]; [**SS/13 INQ000102742**].

1.30. The last DCMS 'Industry Disinformation Workshop' with Google, YouTube, Twitter and Meta before the pandemic began was held in December 2019. The objective of this workshop was to foster a closer relationship between the organisations, with hopes to facilitate a process by which social media platforms and government could share information on disinformation. A briefing for this meeting outlined proposals from DCMS to cooperate with these companies on disinformation harms, particularly on the topic of anti-vaccination:

[6] Share Checklist

"Agenda Item 2: Initial discussion on Anti-Vaccination

...

Anti-vaccination messaging

1. Recognise the serious and lasting effects anti-vaccination messaging is having globally. As DHSC note, while it is clear there are still high levels of vaccine confidence in the UK, we cannot be complacent.

...

3. DCMS are keen to continue working with DHSC, Platforms, and Civil Society to better understand this potential threat and develop effective, proportionate, policies to overcome it.

*4. We would welcome your thoughts on how UK researchers and civil society can gain access to the data they need from your platforms to make a full assessment of the reach and scale of anti-vaccination messaging on your platform." [**SS/14 INQ000102743**] (P2).*

1.31. From March 2020 the CDU met social media platforms regularly via bilateral and industry-wide meetings. The CDU also undertook regular engagement on content it identified which violated platform terms of service, with a view to improving HMG's understanding of how platform policies were applied in practice.

1.32. The CDU also worked with civil society organisations, academics and think tanks (including the Royal United Services Institute, Full Fact, and Demos) with a view to sharing insights. For example, in August 2019 the CDU hosted a presentation by Digitalis on their research into anti-vaccination misinformation and the search engine landscape [**SS/15 INQ000102744**]. This was also presented at a separate meeting to senior civil servants in DHSC.

1.33. The CDU also inputted into FCDO-led engagements with international partners in multilateral fora, including attending disinformation sessions at the Internet Government Forum[7], Digital Nations (previously D9)[8] and G7[9] to share best practice.

Work with the devolved administrations in Scotland, Wales, and Northern Ireland

1.34. Disinformation is a devolved policy matter and, as such, the CDU was not in contact with devolved administrations in a formal way, meaning that there were no regular meetings or joint work programmes. There were occasional, ad hoc interactions where updates on work and approaches were shared during the relevant period, such as through the mis- and disinformation analyst working group, led by UK Covid

[7] A global forum convened by the United Nations Secretary-General for dialogue on Internet governance issues.
[8] A network of digital governments committed to harnessing the potential of digital technologies to improve their citizens' lives. The UK is a founding member.
[9] The Group of Seven (G7) is an international, intergovernmental political forum consisting of Canada, France, Germany, Italy, Japan, the United Kingdom and the United States.

Vaccine Security (UKCVS) with DCMS participation. DCMS does not own the minutes for these meetings and, if they are required, DHSC should be approached.

Decision-making bodies and individuals within DCMS with responsibility for the Counter Disinformation Unit

1.35. Senior level governance of counter-disinformation policy and operational action relating to UK audiences was provided by the government's Disinformation Board. This was regularly attended by directors and senior civil servants from the following departments and teams: HO, FCDO, CO (government security group, national security secretariat, national security comms team, constitution group, internet harms) and the UK Intelligence Community. The board was chaired by the DCMS Director of Security and Online Harms and was approximately 12 people. Additional DCMS staff who worked to support the board meetings were the Deputy Director of Security and International, the Head of Digital National Security and Online Manipulation, the Head of Counter Online Manipulation and a number of junior policy advisers.

1.36. A range of DCMS staff worked on the CDC and CDU during this period and their job titles are below. It should be noted that not all of the following staff would have spent the entirety of their effort and resource on the issue of countering disinformation, especially those at more senior grades:

- Director of Security and Online Harms (SCS2);
- Deputy Director Security and International (SCS1);
- The Head of Digital National Security and Online Manipulation (Grade 6) a post which later became Head of the Counter Disinformation Unit (Grade 6);
- CDU Operational Lead (Grade 7);
- CDU Lead Analyst (Grade 7);
- A number of policy advisers, analysts and senior staff surged in temporarily from other roles, including other Deputy Directors/SCS1 staff (up to 15 individuals at the peak of the surge).

Readiness and preparation in practice

1.37. This section outlines how, in practice, the CDU prepared for emergency situations, including in relation to arranged exercises and tests.

1.38. Prior to the pandemic, DCMS's crisis response preparation had been principally focused on mis- and disinformation threats in the context of democratic events or public order issues. Whilst work had been undertaken on the issue of vaccine mis- and disinformation (as set out in paragraphs 1.24-1.25 and 1.28-1.31 above), this was largely focused on providing insights to policy development designed to address the issue in general. DCMS had not developed specific plans for a disinformation response in the particular context of a public health emergency. However, the crisis response mechanism was not designed with a single specific scenario or mis- and disinformation threat in mind (such as being solely election-related). A deliberate choice was made to make this subject and actor agnostic, in order to enable swift adaptations to new threats. As noted in paragraph 1.10 above, DCMS also worked

with CO to ensure that potential disinformation risks were accurately reflected in the National Security Risk Assessment and National Risk Register.

1.39. The work on a disinformation crisis response plan started following the development of the cross-Whitehall Counter Disinformation Cell. This involved DCMS working closely with analytical teams in the HO, FCDO and CO to bring together and understand relevant information, to better enable DCMS to present a comprehensive picture of any harmful disinformation which posed a risk to UK audiences. DCMS would then disseminate those insights to the relevant teams in government, including to communications teams within CO and relevant departments who would lead on any reactive or proactive comms, where appropriate. DCMS led on any platform-related actions where appropriate. This process was designed to improve cross-government coordination and collaboration in terms of understanding and countering potentially harmful disinformation.

1.40. On 19 March 2019, a disinformation focused tabletop exercise was held, which brought together a range of departments in order to test the operation of the Counter Disinformation Cell [**SS/16 INQ000102750; SS/17**]. The exercise was a response to a possible YELLOWHAMMER crisis event (disinformation relating to perceived food shortages in relation to a no-deal Brexit) [**SS/18 INQ000102800**].

1.41. Following the roundtable discussions in 2019, DCMS worked with teams in HO, CO and FCDO to set out clearer definitions for Red-Amber-Green rating levels in relation to potential disinformation campaigns. DCMS arranged a further table-top exercise to stress test Red-Amber-Green rating assessment levels and capacity to respond to a major event in the early recess period, particularly in the context of elections. [**SS/19; SS/20**].

1.42. As noted in paragraph 1.23, in April 2019, DCMS ran a three day CDC disinformation-focused exercise with teams from the HO, CO and FCDO. The CDC responded to a fictional scenario of increased misinformation relating to the status of EU citizens. The test involved trialling monitoring, communications, and platform engagement structures in the event of a crisis to test the CDC structures and team remits. The post-exercise review notes that participants found the exercise useful and were generally reassured by the collective response [**SS/11**] (P2).

1.43. On 17 April 2019, DCMS stood up the cell for the first time as part of the activation of the 'Election Cell', an established governance structure around democratic events led by CO, in response to the UK's participation in European parliamentary elections [**SS/21; SS/22**]. DCMS was responsible for coordinating input from cell members and providing a weekly situation report (a collection of all reporting setting out the overall situation) on disinformation to the Election Cell [**SS/22**] [P1]. Following this, DCMS and the cross-Whitehall counter disinformation working group considered lessons learned from participation in the Election Cell which helped inform future work supporting democratic events, in particular the general election in 2019. It was noted that there would be benefits to understanding the environment to create a baseline of 'normal' levels of disinformation.

1.44. In the October 2019 disinformation directors board meeting, DCMS set out the CDC's operational response to a general crisis scenario related to YELLOWHAMMER and elections in a slide deck [**SS/23 INQ000102795**], which outlined the remits of each department. DCMS was named senior responsible owner of the cell, coordinator of the cell and social media platform engagement lead.

1.45. In November 2019, the CDC was activated following the calling of a general election on 12 December 2019. The cell's coordination and engagement with social media platforms and organisations relevant to disinformation (such as Full Fact) was led by DCMS. Monitoring was led by HO, FCDO and CO, the intelligence assessment was led by the UK Intelligence Community, and strategic communications were led by the CO national security communications team. In its coordinating role, DCMS produced daily and weekly situation reports (SITREPs) on behalf of the CDC to share with the CO Election Cell, providing information on disinformation narratives about the election targeted at domestic and international audiences. Election monitoring was not designed to capture the broad spectrum of democratic debate but was instead tightly focused on agreed categories relating to:

- Mis- and disinformation relating to electoral processes which could undermine the integrity or administration of the election.
- Mis- and disinformation which could impact national security or public safety.
- Disinformation, intimidation or abuse which is illegal, e.g. inciting violence or hate speech (any illegal content would be referred to relevant parts of HO).
- Suspected foreign interference.

1.46. A cross-government, working level lessons learned exercise was completed after the general election [**SS/24**]. Recommendations included: to continue to improve information flows between social media platforms and the government (including arranging sessions with the platforms to build understanding of working practices and share learnings); to increase the resources available across departments to the CDC (i.e. higher staff numbers) and to further clarify remits to help improve operational readiness for likely disinformation events by developing criteria for standing up the cell and a list of standard disinformation techniques [**SS/25**]. The aim was to improve the response to any disinformation campaign targeting the UK in the instance of a democratic event or national crisis [**SS/9**] [P3].

1.47. In January 2020, the government's disinformation board considered the CDC lessons learned, with four key emerging themes identified: cross-government coordination, operational ability, resourcing and remit and terminology, including Red-Amber-Green ratings. The board also considered a 'Counter Disinformation Strategic Review' which sought to establish a three year, cross-Whitehall work programme designed to facilitate cross-government collaboration, provide effective programme management and accountability and effectively prioritise use of existing resources. The review built upon the existing counter-disinformation strategy which consisted of four pillars: understanding the threat; disrupting the actor; enabling a resilient audience; and enhancing the quality of our information environment. Task and finish groups were created for each of the four themes, in addition to a group focused on

international work. The groups were tasked with identifying priorities and developing detailed proposals for the government's future structures and strategy [**SS/26 INQ000102751**]. To inform this work, DCMS also engaged with social media companies to better understand their policies in relation to mis- and disinformation and identify content which violated these policies [**SS/27 INQ000174767; SS/28 INQ000102796**].

1.48. Although the work of the task and finish groups was paused due to the pandemic, these priorities have since been taken forward through the ongoing work of the CDU, in collaboration with other teams across Whitehall. A disinformation response playbook was also created to provide a coordinated government response during periods of heightened sensitivity, including disinformation and misinformation with the potential to impact public order or safety [**SS/29**]. Although staffing levels had not increased between January and March 2020, operational ability was ensured through a very rapid response at the onset of the pandemic, including significant surge resourcing into the DCMS CDU. All lessons learned fed into how we approached the Covid-19 response and our approach has continued to evolve [**SS/30**].

Section 2: Planning for a pandemic

Expert advice in DCMS

2.1. The Counter Disinformation Unit relies on expert input to identify instances where disinformation or misinformation may cause a risk to health and safety, for example, vaccine misinformation. This helps inform both the monitoring categories agreed by ministers and the monitoring process itself. In the CDU, data concerning harmful disinformation narratives is obtained through open-source monitoring of social media by a mixture of both internal and external experts. For example, the CDU has contracted an external provider to monitor mis- and disinformation on social media platforms and also obtains reporting from teams within HO and FCDO. In addition, the CDU regularly engages with other government departments, civil society organisations and international partners who provide additional insights on potentially harmful disinformation, based on social media data and academic research.

2.2. In addition to working closely with internal experts across other government departments and the UK Intelligence Community as set out in Section 1, the CDU has engaged with a range of external experts including:

a) Safety tech companies, e.g. Logically and Faculty.
b) Civil society and think tanks, e.g., Full Fact, and Demos.
c) Academia and researchers, including on anti-vaccination misinformation (September 2019).
d) International partners e.g. other G7 nations.

2.3. In line with the government's view that countering disinformation requires a whole-of-society approach, DCMS (now DSIT) continually seeks to engage with leading experts in the field, from a range of different organisations, as set out above. The evidence provided from these sources is used by DCMS to develop an

understanding of harmful mis- and disinformation and its potential impact on UK audiences. Coupled with insights from the major social media companies on the steps they are taking to address these themes, DCMS is able to leverage this expertise to develop policies and approaches to address the harm of mis- and disinformation on UK audiences. By way of example, the "Don't Feed the Beast" campaign (as discussed at paragraph 1.44) and the 'SHARE checklist' were designed to increase audience resilience to disinformation and educate and empower those who are affected by false and misleading information [**SS/14 INQ000102743**].

2.4. This engagement with civil society and other external partners enabled the government to grow its understanding of the risk of harm posed by mis- and disinformation online and approaches to addressing this, including through improving transparency and information-sharing, improving media literacy, working more closely with social media platforms and regulatory approaches. This was supported by international engagement through which the UK has helped to develop consensus around the need for government action to tackle a wide spectrum of state and non-state backed mis- and disinformation. This engagement has focused on sharing best practice in a number of areas including monitoring and analysis, platform engagement, media literacy and regulation.

2.5. DCMS also took part in a cross-Whitehall disinformation research sub-group which involved relevant departments (FCDO, HO, CO, DHSC) from the wider cross-Whitehall counter disinformation working group. As set out in its terms of reference, the group was focused on coordinating research activities (using external experts) across Whitehall on mis- and disinformation, discussing research priorities and managing relationships with external stakeholders. This was intended to help avoid duplication, achieve value for money on procurements and facilitate knowledge dissemination across Whitehall [**SS/31 INQ000102806**].

Learning by DCMS from past simulation exercises and near pandemic events

2.6. DCMS considered the challenge of tackling disinformation from Russia in relation to The Salisbury Novichok poisonings in March 2018 ***[SS/32 INQ000102798]***. Again, this event was useful in allowing DCMS to understand how Russian disinformation could spread and prompted discussion on how we develop policies to address this issue.

Section 3: Planning for future pandemics

Reflections on our effectiveness and contribution

Operational readiness

3.1. In March 2020 the government's operational response to domestic disinformation incidents was based on mobilising a cross-government team, the Counter Disinformation Cell [**SS/33**]. Based on the same principles of cross-government

cooperation this evolved as a result of learnings during the pandemic into the permanent Counter Disinformation Unit team within DCMS (now DSIT). This team has led work which was identified both just before and during the pandemic as priority areas, including further developing relationships with platforms, civil society and academia. This, along with the standing nature of the CDU has enabled HMG to make significant improvements to its ways of working, such as the ability to prepare and pivot smoothly to work on completely new areas of risk. This was well demonstrated in February 2022 when the CDU pivoted rapidly to respond to the Russian invasion of Ukraine [**SS/34**].

External partnerships

3.2. The lessons we learnt responding to the pandemic (from March 2020 onwards) improved our ways of working and preparation for future emergencies, including through making the best use of external partnerships. The CDU signed contracts with three external monitoring suppliers as part of its pandemic response. Two of these, with Global Disinformation Index and Digitalis respectively, were selected through direct award due to reasons of extreme urgency[10]. These contracts were not renewed beyond the periods stated below :

- A contract with Global Disinformation Index ran from 23 April 2020 to 22 October 2020. This was intended to help the CDU identify disinformation narratives related to COVID-19 and understand how these were spreading on platforms the CDU did not have any engagement with. The total contract value for this period was £114,274.

- A contract with Digitalis ran from 4 May to 3 June 2020 to provide the CDU with insights on online search terms related to COVID-19. This was to allow the CDU to understand the extent to which UK audiences were being exposed to mis- and disinformation. The total contract value for this period was £18,900.

3.3. In addition, the CDU ran an accelerated open procurement exercise in December 2020 to identify an external supplier to enhance its understanding of mis- and disinformation which posed a risk to UK audiences, via monitoring and analysis of COVID-19 mis- and disinformation online. Logically Ltd were selected through the open procurement exercise and a contract was initially signed for the period 1 January - 31 March 2021. This was extended twice, in line with the agreed contractual terms, to cover the period 1 April - 30 June and 1 July - 31 August 2021 while a further tendering process was underway. The total value of this contract was £454,400. Logically have since been successful in two subsequent open procurement exercises. One for the period 1 September 2021 - 30 June 2022 at a total value of £691,200. The other is the current contract covering the period 1 July 2022 - 31 March 2023 at a total value of £503,392.50.

[10] The direct award process was conducted in line with Procurement Policy Note 01/20: Responding to COVID-19

3.4. DCMS worked with Logically to enhance its understanding around online Covid-19 mis- and disinformation narratives which could pose a risk to the UK public. Logically use proprietary open source tools and AI technology to provide monitoring of online mis- and disinformation narratives. This provides analysts with the insights they need to identify and assess harmful content online. Examples of this kind of content include:

- medical misinformation around vaccines which could undermine vaccine confidence.
- mis- and disinformation falsely connecting COVID-19 to 5G technology which could lead to physical violence or abuse.
- mis- and disinformation targeting minority or vulnerable groups such as claims that a particular ethnic group were responsible for spreading the virus.

3.5. Insights from the CDU's monitoring and analysis of mis- and disinformation narratives were shared with relevant teams across government, including with communications teams working in DHSC to help inform and shape any reactive or proactive public health comms interventions. In addition, where the CDU identified content or coordinated inauthentic behaviour on major social media platforms which was deemed to violate the platform's terms of service, this was escalated to the platform for them to decide on any appropriate action, in line with their own policies (as per paragraphs 1.19 -1.21).

3.6. Building on our pandemic experience, the CDU has continued to work with external suppliers to understand how mis- and disinformation narratives related to other themes (such as general health mis- and disinformation, Russia's invasion of Ukraine and elections) is developed and spread, enhancing our understanding of this threat. Our use of external suppliers has demonstrated that where they possess the technical capability and subject matter expertise they can provide a valuable addition to enhance government efforts to understand the range of harmful mis- and disinformation narratives that could impact UK audiences. In a fast evolving industry with many leading UK companies, safety tech providers face healthy competition to come up with innovative solutions to identifying harmful mis- and disinformation content.

3.7. In parallel, the government is seeking to reduce reliance on external providers and platforms for access to relevant data and insights relating to mis- and disinformation. DSIT is leading a Shared Outcomes Fund funded project to build a Counter Disinformation Data Platform (CDDP). The CDDP will be a tool that can be used by teams across government to improve our collective understanding of the mis- and disinformation threat, enabling better sharing of data and consistency of analysis across government.

Platform engagement

3.8. Prior to the pandemic DCMS engagement with social media platforms in relation to mis- and disinformation was largely focused on their overall approach and policies regarding potentially harmful content and their means of promoting authoritative information. Engagement on specific content was primarily related to disinformation

in the context of elections (specifically the European parliamentary election and UK general election in 2019). However, as set out in paragraphs 1.28 - 1.31, HMG had also proactively engaged with platforms on vaccine disinformation in 2019.

3.9. With the onset of the pandemic, this approach was rapidly adapted to the risk posed by Covid-19 mis- and disinformation with more regular bilateral meetings with the major platforms (Meta, YouTube, TikTok and Twitter) and improved information-sharing around narrative trends to ensure both platforms and HMG are better informed. DCMS gained 'trusted flagger' status (an individual or entity considered by a hosting service provider to have particular expertise and responsibilities for the purposes of tackling harmful content online) with these platforms, enabling HMG to urgently escalate harmful mis- and disinformation content assessed as potentially violating the platforms' terms of service.

3.10. DCMS developed a strong expertise in platforms' terms of service, which enabled the CDU to make informed assessments of violative content and identify where terms of service may be failing to address harmful content. In April 2020, DCMS worked closely with platforms on the prevalence of dangerous 5G mis- and disinformation which included direct incitement to physical violence and abuse. In response, major platforms acted to ensure their terms of service addressed this and subsequently took action to reduce the likelihood that harmful 5G disinformation could proliferate online.

3.11. The strong relationships developed with the major social media platforms during the pandemic have enabled the CDU to respond more quickly and effectively to acute disinformation risks. The pandemic provided an opportunity for the CDU to build trust with the platforms by demonstrating the value of two-way information sharing and these relationships have been key to the CDU's work on subsequent disinformation threats. For example, at the start of the Russian invasion of Ukraine the CDU was able to rapidly convene an industry group meeting with the major platforms to discuss mis- and disinformation risks, narrative trends and platform policy updates and maintain engagement through regular bilateral meetings. Building on experience from the pandemic, the CDU facilitated the sharing of authoritative sources of information with platforms for signposting, such as information published on gov.uk in relation to visas for refugees and donation pages. Wider awareness across government of the CDU's role in engaging with platforms on disinformation and cross government coordination was also improved thanks to prior experience of cross government collaboration during the pandemic.

3.12. DCMS is aware that the issue of mis- and disinformation goes beyond the major platforms. As such, we keep our stakeholder relationships under review and are currently developing a 'secondary platform' engagement strategy to ensure that smaller and alternative platforms (such as Telegram) are considered. This strategy is embryonic and has so far involved a cross government exercise seeking to understand the prevalence of disinformation on platforms other than those the team already engages with. DCMS also seeks to understand particular features of platforms (technical or policies) which may increase the prevalence or spread of disinformation and work planned with UK Intelligence Community on disinformation

from hostile states, including to understand specific communities that may be targets of such disinformation and technologies and techniques which are utilised and being invested in. This positioning will assist HMG in preparedness for future events where there is a heightened disinformation risk, such as pandemics and civil emergencies.

Addressing vaccine and wider health mis- and disinformation

3.13. Our pandemic experience highlighted specific challenges in addressing vaccine mis- and disinformation. The disproportionately lower vaccine uptake rates in minority ethnic communities created a challenge for HMG as there was a broad lack of research into the impact of anti-vaccine mis- and disinformation on vaccine hesitancy. To improve government's understanding of vaccine hesitancy among ethnic minority communities, the CDU joined MHCLG's (now DLUHC) community vaccine champions working group to share information on anti-vaccine mis- and disinformation narrative trends.

3.14. Following the pandemic, the CDU has continued to work with Whitehall partners to identify harmful mis- and disinformation content related to health. The CDU is a member of the UK Health Security Agency (UKHSA) led health mis- and disinformation working group, in which colleagues from DHSC, UKHSA and the devolved administrations of the NHS share updates of prevalent and emerging health mis- and disinformation narratives that audiences are being exposed to.

3.15. Additionally, to improve the government's future threat detection capabilities, DCMS (now DSIT) is developing the previously mentioned Counter Disinformation Data Platform (paragraph 3.7) to identify emerging mis- and disinformation narratives. DCMS has engaged with partners in UKHSA throughout the development of the tool to ensure that it will be effective in detecting mis- and disinformation narratives related to health and vaccines and to ensure that UKHSA analysts will be able to make use of the platform. This will enhance the government's capability to identify emerging mis- and disinformation threats and prepare sooner, including through pre-emptive engagement with the major social media platforms where appropriate.

3.16. We are also taking action to address mis- and disinformation where it constitutes illegal content or harmful content to children through the Online Safety Bill (OSB). Under the Online Safety Bill, all companies subject to the safety duties will be forced to take action against illegal content online, including illegal mis- and disinformation, and will be required to take steps to remove in-scope content if companies become aware of it on their services. This includes state sponsored disinformation and content captured by the False Communications Offence, which will be brought into law through the Online Safety Bill, where the individual knows information to be false but sends it intending to cause harm, such as hoax Covid-19 cures. All companies in scope of the legislation will be forced to assess whether their service is likely to be accessed by children and, if so, deliver additional protections for them. Those safety measures will need to protect children from a wide range of content that is harmful to children, including some types of mis- and disinformation.

3.17. In addition, under the Online Safety Bill, Category 1 services (those with the largest

audiences and a range of features which enable content and activity to reach large numbers of people) will need to have clear terms of service, and will need to enforce their terms and conditions consistently, including on health misinformation and disinformation. In circumstances where there is a significant threat to public health, the Secretary of State will have additional powers to require Ofcom to prioritise specified objectives when carrying out their media literacy activity, and to require companies to report on the action they are taking to address the threat. Ofcom will also be required to set up an expert advisory committee on mis- and disinformation, empowering Ofcom to conduct research into online safety issues, and giving it the tools to understand how effectively disinformation, including health mis- and disinformation where appropriate, is being addressed by platforms through transparency reports and information gathering powers.

Statement of Truth

I believe that the facts stated in this witness statement are true. I understand that proceedings may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief of its truth.

Signed: Personal Data

Dated: 21/04/2023