PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

TELECOMMUNICATIONS (SECURITY) BILL

First Sitting

Thursday 14 January 2021

(Morning)

CONTENTS

No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor's Room, House of Commons,

not later than

Monday 18 January 2021

The Committee consisted of the following Members:

Chairs: † Mr Philip Hollobone, Steve McCabe

† Britcliffe, Sara *(Hyndburn)* (Con)
† Cates, Miriam *(Penistone and Stocksbridge)* (Con)
† Caulfield, Maria *(Lewes)* (Con)
Clark, Feryal *(Enfield North)* (Lab)
Crawley, Angela *(Lanark and Hamilton East)* (SNP)
† Johnston, David *(Wantage)* (Con)
† Jones, Mr Kevan *(North Durham)* (Lab)
† Lamont, John *(Berwickshire, Roxburgh and Selkirk)* (Con)
† Matheson, Christian *(City of Chester)* (Lab)
† Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Richardson, Angela *(Guildford)* (Con)
† Russell, Dean *(Watford)* (Con)
† Sunderland, James *(Bracknell)* (Con)
Thomson, Richard *(Gordon)* (SNP)
† Warman, Matt *(Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport)*
West, Catherine *(Hornsey and Wood Green)* (Lab)
† Wild, James *(North West Norfolk)* (Con)

Sarah Thatcher, Huw Yardley, *Committee Clerks*

† attended the Committee

Witnesses

Patrick Binchy, Technical Services Director, Three

Derek McManus, Chief Operating Officer, O2

Andrea Donà, UK Head of Networks, Vodafone

Howard Watson, Chief Technology Officer, BT Group

Alex Towers, Group Policy and Public Affairs Director, BT Group

Public Bill Committee

Thursday 14 January 2021

(Morning)

[Mr Philip Hollobone *in the Chair*]

Telecommunications (Security) Bill

11.30 am

The Chair: Before we begin, I have a few preliminary announcements. Please switch electronic devices to silent. Tea and coffee are not allowed during sittings of this Committee. I would also like to remind Members of the need to observe the rules on physical distancing, both in this room and when entering and leaving via the marked entrance and exit doors. It is important that Members find their seats and leave the room promptly in order to avoid delays for other Members and staff.

Today we will first consider the programme motion on the amendment paper. We will then consider a motion to enable the reporting of written evidence for publication, and then a motion to allow us to deliberate in private about our questions, before the oral evidence session. In view of the time available, I hope, but cannot insist, that we take those matters without debate. I call the Minister to move the programme motion standing in his name, which was discussed on Tuesday by the Programming Sub-Committee for this Bill.

Motion made, and Question proposed,

That—

(1) the Committee shall (in addition to its first meeting at 11.30am on Thursday 14 January) meet—

(a) at 2.00 pm on Thursday 14 January;

(b) at 9.25 am and 2.00 pm on Tuesday 19 January;

(c) at 11.30 am and 2.00 pm on Thursday 21 January;

(d) at 9.25 am and 2.00 pm on Tuesday 26 January;

(e) at 11.30 am and 2.00 pm on Thursday 28 January;

(2) the Committee shall hear oral evidence in accordance with the following table:

Table

Date	Time	Witness
Thursday 14 January	Until no later than 12.30 pm	Three; O2; Vodafone
Thursday 14 January	Until no later than 1.00 pm	British Telecommunications
Thursday 14 January	Until no later than 2.45 pm	Mobile UK; TechUK
Thursday 14 January	Until no later than 3.30 pm	Mavenir; NEC Europe Ltd
Thursday 14 January	Until no later than 4.15 pm	Small Cell Forum; Digital Policy Alliance
Thursday 14 January	Until no later than 4.45 pm	British Standards Institution; Royal United Services Institute
Tuesday 19 January	Until no later than 10.10 am	Webb Search; Oxford Information Labs
Tuesday 19 January	Until no later than 10.45 am	Dr Alexi Drew, the Centre for Science and Security Studies, King's College London
Tuesday 19 January	Until no later than 11.25 am	The Office of Communications
Tuesday 19 January	Until no later than 2.45 pm	Catapult Compound Semiconductor Applications; Dr Nick Johnson; UtterBerry
Tuesday 19 January	Until no later than 3.30 pm	MWE Media Ltd; Lumenisity; Dr David Cleevely CBE
Tuesday 19 January	Until no later than 4.00 pm	Information Technology and Innovation Foundation

(3) the proceedings shall (so far as not previously concluded) be brought to a conclusion at 5.00 pm on Thursday 28 January.—*(Matt Warman.)*

Mr Kevan Jones (North Durham) (Lab): I have no problem with the programme motion, because it is sensible, but I want to put it on record that it is frankly nonsense for us to come in today and sit in a room to take evidence from virtual witnesses, as we will do next week as well. There is no reason why evidence sittings, particularly, could not happen remotely. I have attended two meetings this week, including a meeting on Tuesday of the Defence Committee, which took evidence from witnesses virtually.

I understand that things are being done in this way at the insistence of the Leader of the House. I think he is hiding behind the usual channels having sorted it out. I want to put it on the record that that is not true and that objections have been raised by the official Opposition, certainly about evidence sittings being done in this way. If we are to travel long distances, as many of those present have, to get here today and next week, that flies in the face of the advice of not only the Government but Public Health England about moving between areas.

I do not know whether, at this late stage, we could at least consider whether next week's evidence could be taken virtually, because it is a bit ironic that we are sitting in a room here—I accept your rulings about social distancing and so on, Mr Hollobone—and that the evidence that we shall listen to from the witnesses today and next week will be given virtually.

The Chair: Mr Jones, I note your remarks and know that many others will share your view. As the Chair of the Committee I can operate only under the rules that I have been given by the House.

Question put and agreed to.

Resolved,

That, subject to the discretion of the Chair, any written evidence received by the Committee shall be reported to the House for publication.—*(Matt Warman.)*

The Chair: Copies of written evidence that the Committee receives will be circulated to Members by email and made available here in the Committee Room.

Resolved,

That, at this and any subsequent meeting at which oral evidence is to be heard, the Committee shall sit in private until the witnesses are admitted.—*(Matt Warman.)*

The Chair: We will now go into private sitting.

11.34 am

The Committee deliberated in private.

Examination of Witnesses

Patrick Binchy, Derek McManus and Andrea Donà gave evidence.

11.35 am

The Chair: All our witnesses today will be giving evidence by video link. Before calling the first panel of witnesses, I should first like to remind all hon. Members that questions should be limited to matters within the scope of the Bill and that we must stick to the timings in the programme order that the Committee has just agreed. For this first panel, we have until 12.30 pm. Secondly, may I ask whether any hon. Members on the Committee wish to declare now any relevant interests in connection with this Bill?

I now call the first panel of witnesses: Patrick Binchy, technical services director at Three, Derek McManus, chief operating officer at O2 and Andrea Donà, UK head of networks at Vodafone. Would the witnesses please be kind enough to introduce themselves for the record?

Patrick Binchy: Good morning. I am Patrick Binchy, and I work for Three, as you said, as the technical services director. I do not know what happened previously, but we lost some degree of ability to hear what you were saying. I think it was Chi Onwurah who was talking, but we could not hear what she was saying, and then it went completely silent for about two minutes.

The Chair: Patrick, I think that was because we were in private session, deciding how we were going to conduct our affairs. You were not cut off out of any rudeness; it was simply that we were going through some procedural matters. May I ask Derek McManus to introduce himself, please?

Derek McManus: Good morning. My name is Derek McManus; I am the chief operating officer of O2 in the UK, and part of my responsibility is therefore network.

The Chair: Thank you. Andrea Donà?

Andrea Donà: Good morning, everyone. I am Andrea Donà; I head up networks for Vodafone UK. I would like to thank you all for inviting us today; I appreciate the opportunity to give evidence to the Committee.

Q1 The Chair: May I ask our witnesses whether they would like to make a short opening statement? It is not compulsory. Then we will go on to questions.

Patrick Binchy: Other than thanking you for the ability to represent the industry here, I do not have anything to add, thank you.

Derek McManus: I will add my thanks too. As I have said, my name is Derek McManus, chief operating officer. My teams run the network and the roll-out of 5G and maintain the security and integrity of the network. I am here to answer questions on the Bill and the impact from a business and operational perspective. The security Bill and associated diversification strategy need to be viewed as part of wider powers and requirements being introduced via the Telecommunications (Security) Bill.

The telecoms sector faces considerable costs—resources and time, among other things—in introducing new security measures in the Bill while removing HRVs from networks and looking into diversifying. A balanced approach that gives the sector time to implement the new measures in a cost-effective manner is essential if the Government want the same individuals and companies to develop and roll out ORAN while maintaining and building a secure network.

Andrea Donà: Vodafone accepts the UK Government's policy on high-risk vendors and continues to work actively with the NCSC and the Government on maintaining the highest security standards in our network. We want to ensure that the objectives of the Bill are fulfilled. We also welcomed the Government's recently published 5G diversification strategy and the policy framework that comes with it. The strategy sets out ways in which the Government plan to work with industry, and we very much welcome that. We also support the Government's drive for higher minimum security standards in the telecoms network, and we are continuing to work with DCMS, the NCSC and Ofcom to ensure that all those relevant measures to protect our customers are implemented.

The Chair: Thank you. We have three superb witnesses from Three, O2 and Vodafone. I am now in the hands of Members.

Q2 Chi Onwurah (Newcastle upon Tyne Central) (Lab): It is a pleasure to serve under your chairship, Mr Hollobone. I want to start by thanking, as well as the witnesses, the members of the Committee, the officials and the staff of the House, who in coming into Parliament during a pandemic are also taking risks, which we very much regret.

I should have mentioned, as an interest, that I spent 20 years working in the telecoms industry within four network operators and vendors, as well as Ofcom, the regulator. I also may know personally some of the witnesses.

The Chair: It sounds like you might be dangerously over-qualified to take part in this Committee.

Chi Onwurah: You make a very good point, Mr Hollobone. I am going to try to keep my engineering and technical interest as much to the back as possible.

I am the shadow Minister for digital, and I am leading for Labour on this Bill. I will focus on the costs of removing Huawei and the diversification strategy, and Opposition colleagues will be focusing on different areas. I thank you for your presence and expertise. I want to ask two somewhat related questions.

First, some have given estimates of the costs of removing Huawei from your networks, and I want to verify whether those are the most up-to-date estimates. I also want to know whether they include opportunity costs, and the time and resources from your boards and others in your organisations. Are they the full costs, if you like, of the removal of Huawei? How can we minimise the economic impact, in your view? Are there other significant costs associated with the Bill and the implementation of a new security framework?

Secondly, your mobile network procurement is currently made through what I will call full-service providers, such as Huawei, Ericsson and Nokia. They basically

[Chi Onwurah]

design and make a network, and provide it to you—I know it is not quite as simple as that. Do you think the removal of Huawei or the develop of open RAN will change that? Critically, is the Government's diversification strategy likely to lead to the emergence of significant full-service suppliers that will compete head on with the remaining suppliers, Ericsson and Nokia? If not, what other measures should the Government consider taking? How best can the Government work with partners around the world to achieve their goals? That is quite a lot in two questions.

Patrick Binchy: There was quite a lot in those questions. I guess the first thing is that the costs are obviously commercially sensitive, and we cannot disclose them in a public environment, but we would be very happy to respond to any of the Members or the Committee in private to give the detail behind that. At a more generic level, there will, of course, be cost to the industry and to Three. We had selected Huawei to build our 5G network, and we have now selected a second vendor, Ericsson. We have to go through the process of mobilising Ericsson and removing the Huawei equipment, which has a cost to it and will have an impact.

In terms of the diversification of the market, there are really only two players in the UK market now. As you rightly point out, there are service as well as equipment capabilities within those suppliers. As we look for diversification, we need to diversify across all those aspects of the market. We are working with the Government, NCSC and DCMS in terms of how to approach that and how to build that. We will continue to support that as we go forward.

Derek McManus: We have similar commercial sensitivities on cost. You may or may not be aware that we are not indebted to Huawei. For our network, the cost of removing from the radio network is relatively small compared to some of our competitors. So, I will focus more on your second question, if that is okay.

You are absolutely right that we tend to buy end-to-end service in the current mobile environment. ORAN today is set up with a quite separate and different supply chain, with different companies specialising in software, different companies specialising in hardware and specialists doing the integration. It is likely to change the nature and relationship that we will have with supplies. ORAN is relatively immature in its development. As it is technically and commercially ready for scale deployment, that may well change. But we see today that the leaders in ORAN tend to be smaller companies specialising in the hardware or, more specifically, the software.

Andrea Donà: Very much like my colleagues, I am more than happy to write to the Committee in the future, once we have completed our procurement process, with the details on the cost for replacing our high-risk vendor. More specifically, when it comes to the diversification strategy and the role that open RAN has, we at Vodafone believe that the UK should seek to be a leader in open RAN. We are, indeed, leading the way, and have committed to swapping out 2,600 of our base stations to an open RAN technology.

In order to fulfil that ambition, the current timescales for removing the high-risk vendor equipment must remain unchanged. We need the stability and the time, as Derek rightly points out, to allow industry and Government to develop a diverse supply chain and allow the technology to mature, both in its functionality and its capability, as well as the possibility of scaling industrially. The legacy vendors have had a lot of time in the market to develop their competence. We need to support any new entrants in the open RAN space with appropriate investment incentives and a policy framework that attracts and supports new entrants in the open RAN space.

The Chair: Three Members have indicated that they would like to ask questions. We will take them in the following order: James Sunderland, Miriam Cates and Kevan Jones.

Q3 James Sunderland (Bracknell) (Con): Gentlemen, good morning. Thank you for coming in. As a military man, you will forgive me for asking a very simple question. Are you satisfied that the framework of this Bill, as it currently stands, satisfies the full requirement for national security, and if not, why not?

Patrick Binchy: I think, initially, it is not for the industry to comment on and define national security and risk. That is for the Government. However, we absolutely support whatever is put in place beyond that. I think that this Bill, in the way that it is structured, very much helps with that, because not giving a definition, and the way that it will be able to include additional vendors and additional technologies, gives it the flexibility to move forward and to adapt to threats, whether they are technical or through suppliers in the future. In that way, it is well constructed.

Irrespective of the Bill itself, we work with the security bodies on a regular basis—on a day-to-day basis—and we continue to do that, to protect the British public from any and all security threats. And I would add that the UK is actually very well advanced in terms of protecting itself and its security posture.

Derek McManus: Similarly, I am the COO of a commercial organisation; I am really not best placed to answer that point specifically. But what I will say is that we run our business by security by design—it is a key part of the evolution of our network and all of our services. I believe that as an industry we are actively engaged with the security forces to deliver a good track record in terms of national security from telecoms. It is important that we continue to do that. Everyone who is connected closely to security knows that it constantly evolves as technology evolves, and the continued collaboration between the industry, the Government and the security forces is essential beyond the completion of the Bill.

Andrea Donà: Similarly to my colleagues, I am not in a position to comment on national security. What I would say is that Vodafone worked very closely with Government on how the Bill best enables us to secure our networks in practice. I think it is very important that we maintain a very close collaboration as we work in implementing the Bill.

We believe the Bill is sufficiently flexible for the Secretary of State and Ofcom to interpret the security threats and issue notices to providers to deal with them. Reviewing the legislation at regular intervals to assess its efficacy in the face of new technological challenges, and also in the light of new strategic aims by Government and that constant review involving the industry, will be

very welcome for us. Our continual engagement will enable us to ensure that the new regulations can be enforced in practice effectively to achieve the scope of the Bill.

The Chair: Thank you. We will come to Miriam Cates next. Then, after Miriam, the order will be Kevan Jones, David Johnston, Christian Matheson, Dean Russell and James Wild.

Q4 Miriam Cates (Penistone and Stocksbridge) (Con): May I, too, pass on my thanks to the witnesses for appearing before us today? You have all referred to the significant financial costs to your organisations of removing the equipment from the high-risk vendors, but obviously, given the potential security implications, some are calling for the 2027 deadline to be brought forward. What would be the financial and logistical impacts of bringing forward the deadline on your organisations and your ability to operate? Would that be just too impossible—too difficult?

Patrick Binchy: In line with the previous answer, I cannot go through the specific commercials—they are commercially and competitively sensitive. But I would be happy to take such questions offline if you want to follow up on that.

Regarding the 2027 deadline, I think there is a balance here between UK connectivity and UK security. First and foremost, I would say that we have a security regime in place today. We use the Huawei cyber-security evaluation centre to check all of the technology that comes through Huawei and goes into UK networks, and we work closely with the security authorities to make sure that we are protecting the UK public today. We also have full visibility of any traffic that is transiting our network, either incoming or outgoing, so we are confident that we have the security in place today that is necessary.

In terms of achieving the 2027 timeline, that is a challenge. It is not going to be easy, because we need to balance that national connectivity against security and do it in a way that ensures that we continue to provide good-quality connectivity to the public.

There are a number of timelines within the legislation. We do not think the timeline for 2021 in terms of using equipment is a major issue. The 2023 35% cap and the 2027 are challenging, but we have plans in place. We have put our second vendor in place. They are already rolling our 5G network out in Manchester, Glasgow and Reading, and we are confident that we can meet those timelines and supply good-quality connectivity to the UK public.

Derek McManus: I think everybody, particularly in this environment, understands the immediate value of connectivity in the situation that we as UK society face. In terms of the opportunity for that connectivity to be part of economic growth as we evolve 5G and help build the economy, those are two of the competing challenges that we have to balance, while also removing HRVs and delivering diversification.

Yes, it is a matter of balancing costs in terms of investment, but we also have to recognise the customer disruption caused by removal of equipment. It is important that we maintain those other two key criteria—that important connectivity and that support to economic growth. By working together and taking the right balance, the Bill's timescales are appropriate. I cannot, obviously, talk about the plans of individual businesses to meet the deadlines, but as an industry, I think it is appropriate.

Andrea Donà: At Vodafone, we believe that the Government's decision to set a timeframe of 2027 truly reflects the complexity of what we have been asked to do. It is important that the deadline of 2027 does not change further. We need certainty and a fixed time plan so that we can plan for the future. Any further changes will disrupt our investment plans and will also cause undesired further disruption, as we attempt to accelerate a swap out that is, in itself, very complex, and will deliver inevitable disruption to our customers—the businesses and the public services. We are actively working with all the involved parties—the Government, Ofcom, NCSC and DCMS—to ensure that we minimise disruption. It is a complicated and difficult effort from a technology perspective, but also from the perspective of the practical implementation on the ground.

If the Government truly share our ambition to be a leader in digital infrastructure, we need to ensure that we give the high-risk vendor enough time to carry out the plans, under a very well-defined timescale and, as I said earlier, in parallel, allow the diversification agenda to grow, as well as the stability, to allow new entrants to come in and be a viable alternative to the incumbent high-risk vendor that we are swapping out.

The Chair: We will come on to Kevan Jones. Now I am getting the hang of this now, I do not think it is fair to always ask Patrick to be the first out of the blocks to answer the questions, so I will try to rotate so that everyone has a chance of going first.

Q5 Mr Jones: What is very clear from the first report from the National Cyber Security Centre is that existing Huawei equipment is a manageable risk. The only things that changed the Government's stance were US sanctions on semiconductors for future equipment and, added to that, a layer of—I think—lobbying on behalf of certain anti-China parts of the Conservative party to remove the equipment from day one. Personally, I think there is no justification to do that. However, as you said, that leaves you with just two vendors for hardware, and any new entrant would have to meet the conditions in the Bill. What do you think the Government mean by a diversification strategy, and what are the timescales for that?

Having met many of you at a previous Committee and taken evidence from you, it is clear that there is little profit to be made on the hardware side because we all want cheaper phone calls, and you obviously react to customer demand to try to get costs down. What are the realistic prospects of any UK-based company or other vendor coming into the hardware side? On open RAN, I accept that it is for the future, but what timescales are we talking about for that having an impact on how our telecoms networks are organised?

Derek McManus: On timescales for ORAN, I think we are very early in the evolution of that technology. There are trials in the UK, as there are in various markets across the world. In our view, it will be at least a couple of years before you have a viable technical and commercial product, focused initially on rural. To have diversification in a meaningful way, you have to have

scale, and scale will take a number of years beyond that—I would say five to eight years to get a real, viable-scale vendor to challenge the two incumbents.

On your previous question about the likelihood of there being UK players in that market, the UK used to have a very healthy telecoms supply industry, which sadly over time has faded away. I think it is more likely that the UK could play in the software part of the future of radio, and particularly ORAN, than in the hardware part. I cannot see today a viable UK hardware provider. Actually, there are not that many UK telecoms suppliers around. But software is a bigger opportunity. Part of the diversification work that is going on with the industry and Government is looking at ways to encourage the inclusion of UK business in that emerging opportunity.

Q6 Mr Jones: So, for the conceivable future, we will be reliant on those two vendors: Nokia and Ericsson.

Derek McManus: Yes, and if you look at the scale of mobile growth, the fact that there are only two remaining viable competitors is an indication of how difficult it is to have competition in today's marketplace. That is technical and, to meet the economic challenges, that requires scale, too. There are other providers in the marketplace, but only two provide the 2G, 3G, 4G and 5G capability that the current UK markets require.

Andrea Donà: To answer the specific question on timescales, Vodafone UK is pioneering the development of open RAN. We were the first operator to achieve a commercial open RAN solution, in August last year, having delivered the first commercial open RAN unit on the ground radiating and carrying traffic at the Royal Welsh showground. We recently developed and announced plans to deploy open RAN across 2,600 sites. It is a promising innovation, but it is not yet mature enough to match the traditional vendors in terms of functionality and efficiency on an industrial scale.

However, if the UK wants to lead in this field and take advantage of the existing advantage that it has when it comes to design, it should continue putting its weight behind this promising technology and allow partnerships to be formed, where the incumbent vendors are asked to play a role in the architecture of this new technology. That will allow other parts of the technology chain—as Derek said, software, the baseband or the antennas—to attract and welcome new entrants through appropriate policy frameworks and the diversification strategy.

With new entrants, as we open this technology, we fuel innovation. If the UK keeps ahead of that, it will be able to be at the forefront of exciting new innovation. We welcome the steps that were outlined by Government to try to press this technology ahead. You could do that through trials or through incentives for the MNOs to use their technology. We can work together to create local research and development centres to fuel this new technology.

Q7 Mr Jones: In the near term, it is not going to replace the hardware that we need at the moment, which the two vendors are providing. Are you talking specifically about open RAN, or are you talking about diversification or any strategy to develop a UK hardware supplier?

Andrea Donà: There is an opportunity for British companies to play an active role in the open RAN ecosystem. As we open up the interfaces of the technology, it creates a golden opportunity for British companies, with British support and know-how, to come and contribute to the development of this new technology.

Patrick Binchy: My views are broadly aligned with the previous answers. The reality of the situation that we find ourselves in is that there are only two practical vendors for the next couple of years. As both my colleagues have said, beyond that there is opportunity for ORAN.

I am not sure if it came across in the previous answers, but I would stress strongly that the first thing we need is the R&D. We need to understand how we can move this technology forward. As Derek said, trials are primarily operating in rural capacity, but to be a true competitor to the incumbents we have to be able to use it in deep urban areas, under significant loads, which needs a lot of development.

The Government can support trials and help build the ecosystem around them, but the first thing that we need is to get the research and development that will feed the trials. In terms of the Government's development of opportunities in ORAN, it is key that they look at working with international partners. This has to be scaleable; otherwise, it is never going to be commercially viable. The UK market will not be big enough to drive that scale and commerciality.

Q8 David Johnston (Wantage) (Con): It was widely reported that between 2009 and 2011, Vodafone found back-door vulnerabilities in equipment in Italy, and that you were assured by Huawei that they were being removed. You subsequently found that, in fact, they had not been removed. Do you have any concerns about back-door vulnerabilities in the equipment between now and 2027, and can you give us a sense of your management of that risk and what you do to try to make sure that there are not any?

Andrea Donà: Specifically on the incident you are referring to, which was in April 2019, it was a Telnet protocol, which is used by many vendors in the industry to perform diagnostic functions. It is important to note that it would have not been accessible from the internet. Detailed analysis showed that it was simply a failure to remove a function that is used, as I said, for performing diagnostics after it had been developed.

On the broader question of security and our concerns, we have always maintained the very highest level of security policies, security processes and security procurement mechanisms and frameworks. We use a layered approach to our security needs, whereby we secure by design. All our systems and process put in place guarantee the highest security standards, end to end. The UK networks and standards are the highest in the world. We constantly work hand in glove with the NCSC, and abide by all the latest NCSC guidance and policies to keep those minimum standards high every time. We have worked very closely with the NCSC to set up HCSEC, an ad hoc centre where any new Huawei equipment or software goes through rigorous checks, audits and assurances, in line and in close collaboration with NCSC.

Patrick Binchy: I do not have much to add to that. We are similarly aligned in terms of our processes, from procurement to deployment. We have security checks throughout, and separate functions to make sure that

we are adhering to those. We work very closely with the NSCS and HCSEC in terms of the technologies that are in the network. Going forward, we will continue to do so. We will be reviewing the software and hardware versions that we have in place and ensuring that those are fully checked and validated. As I said earlier, we also have a full, independent view of the traffic traversing our network, so if something untoward were to start happening, we would immediately have a view of it, and would be able to shut it down independently.

Derek McManus: As I said earlier, we do not have sufficient numbers in the UK. We have fewer than 10 Huawei base stations, so although we perform all the necessary checks, we are not exposed on the scale of others in the market.

The Chair: I propose drawing this part of our deliberations to a close at 12.30 pm. We have five Members seeking to ask questions. If our panellists keep each of their answers to one minute, we will get everybody in—and we will get all the answers as well. I call Christian Matheson.

Q9 Christian Matheson (City of Chester) (Lab): Thank you, Mr Hollobone. In that case, I might take liberties and squeeze two questions into one.

Gentlemen, can I assume that you have done an audit—an asset register, if you like—and that you know where all the at-risk equipment is in your networks, so that once the Government push through an order, you know exactly where to go to address the requirements of that order? How interconnected are your networks? Are you as confident as Mr McManus, who says that the integrity is fairly good? Do you all rely on each other to maintain an overall integrity? What if one is insecure ?

Patrick Binchy: Of course, the networks are interconnected. As I said, we have full visibility and control of what transverses between the networks, so we can maintain full control over that. I do not think there are any significant risks in this space, because of all the security checks that we do on the equipment that comes into the network. We maintain a regular relationship with NCSC in terms of any future threats or concerns that it has. We all have our asset registers, and an understanding of what we have in our networks. We maintain and update those on an ongoing basis as the technology changes and evolves.

Q10 Christian Matheson: So you know where all the dodgy stuff would be, if you were asked to find it.

Patrick Binchy: We know where all the equipment is for our main supplier, yes.

Derek McManus: On the question on the asset register, absolutely. As for whether networks are interconnected, Patrick gave a good answer. The O2 and Vodafone networks are somewhat different, in that we work together on a network share; the O2 team manages and maintains a network in a certain geography, and the Vodafone team manages and maintains a physical network in another geography. In that sense, the O2 and Vodafone networks are very interconnected.

Andrea Donà: It is vital that the secondary legislation that accompanies the Bill clarifies assets in the telecoms network architecture that will be in scope of the security requirement, so that we can work knowing what we have audited, and knowing that the auditors always shared with NCSC. We need a clear understanding between Ofcom and us as providers before the legislation is enforced, so that we understand exactly the boundaries and the scope, and we all work together, having done the audits, to close any vulnerabilities that we might have. That is a clear aspect of our working together: ensuring that the assets in the telecoms network infrastructure that are in scope are very well defined.

Q11 Dean Russell (Watford) (Con): Can you describe in layman's terms the types of security threats that your organisations face, and how the security framework would address those?

Derek McManus: There are a number of different security threats. I will talk about network from a physical point of view, though there are obviously also scams and threats through direct human contact. It is mostly penetration of the physical network either from attack or from virus software. Attack is where foreign agencies or bodies look for vulnerabilities or holes in your defences. The role of the telecoms operator is to ensure that all its physical equipment and software are of the highest support and variation that defends from attack. We see quite a high volume of attack, either DDoS or penetration, on a regular basis. As I said, we do cyber-security by design. It is built into the fundamental processes of expanding and adding to our network, to protect us from those very things.

Andrea Donà: To add to what Derek says, it is also important that Government play a role in securing the additional security needs across the whole ecosystem of the supply chain, including the vendors. With the ever-changing nature of the threats we are exposed to, as Derek explained in layman's terms, we have to change the protocols and the rules by which we and our vendors implement our defence mechanisms.

It is important that the Government do not leave providers such as us alone to reinforce these additional minimum security standards; they should play an active role in ensuring that vendors adapt their technology road map, so that things are done in a much more future-ready, cyber-security-compliant manner, because we face an ever-changing picture and ever-changing scenarios.

Patrick Binchy: In terms of the threats and penetration, as Derek said, the key things are that they get into the networks, either to bring the networks down and create chaos for the UK economy, or to extract information from the networks. All our security, as both my colleagues have said, is built into design, right from the very start of the procurement process. How do we protect against, and build networks that are able to detect, avoid and block, any of those risks and threats? We do that through our knowledge, the knowledge of NCSC and the authorities, and the knowledge of the wider industry on what is going on beyond the UK and in the international regime. We are constantly reviewing and updating our capability to protect against any of those threats.

The Chair: Gentlemen, we are right up against the clock. We have seven minutes left. Your answers are superb, but they need to be pithy, because we have three sets of questions coming and we need to get the answers in, and I am afraid that 12.30 pm is a hard cut-off; I am not allowed to extend beyond that.

Q12 James Wild (North West Norfolk) (Con): Hopefully my question has a simple yes-or-no answer. The Bill enables the Secretary of State to issue directions to telcos not to use a designated vendor's equipment. Does that provide the legal certainty that you need—a direction based on national security—to deal with any contractual issues you might have with those suppliers?

Patrick Binchy: I do not think it is quite as simple as yes or no; there are some challenges in how those rules and laws are articulated, and whether that allows us to move away from our commercial obligations. Of course we work with NCSC, and so far, what is in place is fully aligned with the direction taken by the Government and the Bill, so in this case, we believe it is sufficient.

Derek McManus: I refer you to Patrick's answer. I have nothing specific to add. It depends on the circumstances. We continue to collaborate, and to speak with the authorities to ensure that we align with current and future needs, from a security point of view.

Andrea Donà: We will abide by the requirements.

The Chair: Superb—textbook answers.

Q13 Chi Onwurah: I ask these questions on behalf of Catherine West. Vodafone runs networks across Europe, and so does Three, whose owner is headquartered in Hong Kong, and O2, which is owned by Telefónica. Does the Bill duplicate or reflect legislation that you have seen elsewhere in your operations? What international comparisons are you aware of? Also, we have talked about standards being a key part of international collaboration. How many people, or what presence, do you have on international standards bodies?

Derek McManus: Basically, we have not seen anything directly like the UK legislation, although various forms of it can be seen internationally. The second question was on standards. We operate in 23 countries, and as you can imagine, their standards are key to us. We hold a lot of expertise, from a Telefónica group point of view, that the UK team is able to rely on and work with to ensure that we are at the very edge of developing the right standard.

Andrea Donà: As the Government plan to take a lead in enhancing the minimum security requirements, and in diversifying their telecoms strategy, we as a global company are happy to support the standard setting, and to advise on the practical implementation of the additional security requirements.

Patrick Binchy: I refer to Derek's answer. We have a very similar position with regard to the UK legislation: we have not seen quite the same in the other countries. On standards, we play an active role, and we have a number of UK staff who act actively in standards setting.

Q14 The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport (Matt Warman): Thank you to all of you for your engagement today and with the Government up to this point. Given the time, I have one, simple question. The Bill is setting up a new telecoms security framework to enhance network security. How confident are you that you will be able to comply with that in full, and what else would you like to see from the Government to enable you to do that?

Andrea Donà: We need the clarification that I mentioned of what is, and what is not, in scope, so that we have absolute clarity from the word go. We all work together to understand the profile of that implementation. It cannot be a big bang—everything complying from day one. We obviously need to do a detailed risk assessment of the areas that we need to work on immediately on the Bill's coming into force, and of what can afford to be done at a secondary stage, based on the risk assessment and the risk management analysis of the various assets in our network.

Derek McManus: As I said in my opening remarks, collaboration to date on getting the Bill to this stage has been positive. We should continue that. My request is for flexibility to help us execute effectively, while balancing the other demands on the industry.

The Chair: You have 30 seconds, I am afraid, Patrick Binchy.

Patrick Binchy: Again, very similarly, we have to balance good connectivity with security. We are confident that our plans will meet the needs, but we will continue to work with Government and security on how we achieve and deliver that. It will be challenging, but we are confident that we can do it.

The Chair: Order. I am afraid that brings us to the end of the time allotted for the Committee to ask questions. On behalf of the Committee, I thank all our witnesses very much indeed for their evidence this morning.

Examination of Witnesses

Howard Watson and Alex Towers gave evidence.

12.30 pm

Q15 The Chair: We now move on to our second panel, which consists of Howard Watson, chief technology officer, and Alex Towers, group policy and public affairs director, both from BT Group. We have until 1 o'clock for this session. Would our two witnesses please kindly introduce themselves for the record and make a brief opening statement?

Howard Watson: Good afternoon, Mr Chairman. My name is Howard Watson, and I am BT Group's chief technology officer.

We at BT support the principles of the Bill. We echo what the other operators have said—I have just listened in to the previous session—about the importance of having realistic timeframes, and we are pleased that the Government have listened on that. We have some outstanding questions, but they are pretty much about the detail of the implementation of the Bill. There is also need for some further reassurance about the proportionality across the rich landscape of operators that we have in the UK in how that regulation will be applied.

Alex Towers: Hello, my name is Alex Towers and I am director of policy and public affairs at BT Group. I have not really got anything to add to Howard's opening statement. I think that covers it.

The Chair: Lovely. I am now in the hands of Members. I am very happy to give preference to Members who did not ask a question in the previous session. First out of the blocks is Sara Britcliffe.

Q16 Sara Britcliffe (Hyndburn) (Con): Thank you, Chair. It is just a quick one. What are the most pressing threats facing public telecoms networks, and how does this Bill address them?

Howard Watson: I note that some of this was answered by my colleagues earlier. Threats to the network include physical access. We all saw earlier this year a lot of attacks on our physical infrastructure, which were highly regrettable. I mean by that the setting alight of some of our infrastructure. We also faced logical threats, such as malware implants, DDoS attacks and what are called advanced persistent threats, which is an actor embedding themself into parts of the environment, staying hidden for a while and potentially collecting credentials—think of the SolarWinds hack that is in the news at the moment.

We take all those threats extremely seriously at BT. For as long as we have operated, we have worked very closely with all aspects of Government, and in particular with the National Cyber Security Centre. We take a sort of defence in depth approach. We have a red team who are ethically hacking us, and we are part of the TBEST scheme.

We think that the UK has a good track record here, but we also welcome the strengthening of that in the Bill. We think that some of the specific items about protecting even more against potential insider threat, looking hard at the vendors we use in the supply chain and having specific rigour about that, and the reporting mechanisms and requirements in the Bill, specifically around telecoms security requirements, will enhance that for all operators in the UK.

Alex Towers: I do not have much to add to that, except to say that, as Howard says, lots of the attention in the debate in the run-up to this Bill has been focused on a small number of very specific, clearly high-risk vendors. It is right that we take steps to protect ourselves around them, but just as important in the Bill will be the telecoms security requirements that stretch well beyond those specific vendors into all manner of aspects in which operators run their networks. Putting those two things together will be important.

The Chair: Thank you. The running order is Dean Russell, Miriam Cates, Kevan Jones, Christian Matheson and Chi Onwurah.

Q17 Dean Russell: Thank you, Chair. I would like to understand more how the diversification strategy that accompanies this Bill will benefit you as an organisation and the public.

Alex Towers: I think we see long term that diversification of vendors would be good for the operators in the marketplace if we can get to that point. It is important to say, I suppose, as the other operators were doing earlier on, that we are not at that point right now, so we are having to manage a situation where with the market as it stands we have a small number of very large-scale, important vendors and suppliers and we are having to remove one of them, clearly, from the 5G marketplace. That creates a degree of complexity and engineering difficulty that we need to just work our way through; so there is a lot of work to do just to manage within the current market framework to replace Huawei and to bring Nokia and Ericsson to the point we want. While we are doing that, if we can at the same time create the prospects of, in the longer term, a more open marketplace with a wider range of vendors—with other-scale vendors that do not quite work at the minute in the UK market, and Howard could probably explain exactly why that is, as well as with the potential for open RAN and other types of technology and software-based models to be developed—that is good for the whole industry and could be good for UK jobs and potential UK companies and therefore also for the citizen.

Howard Watson: I certainly welcome the Government's supply chain diversification initiative here. It is concerning that we are moving from, essentially, three suppliers in the mobile supply chain down to only two. Our network going forward will use both of those. So widening that choice over time, for all the operators in the UK, is I think a critical opportunity. Please bear in mind that most operators quite like to have a primary source and a second source. It is unlikely that we will all start deploying equipment from four or five different vendors, because the operational challenge of the person in the van maintaining that tends to limit you to a choice of two; but being able to choose two from six is a lot better than choosing two from two, of course.

We welcome the three initiatives, which I will summarise. The first is whether we can we encourage Samsung, NEC and other large vendors who build mobile networks elsewhere to enter the UK market. The second is open RAN and it really just creates through more open standards the ability to have more players in that end-to-end solution. The third area really is to have a thriving research agenda for the UK. We really welcome the £250 million allocated in the recent spending review. We already have a thriving research capability in the UK and I think continuing to focus that on antenna design, optoelectronics and semiconductors will have a role to play in diversification going forward.

Q18 Miriam Cates: You have said in your written evidence that you fully support the objectives of the Bill, to improve security in the networks, but 20 years ago we could not possibly have anticipated the kind of threats that we face today, so it is safe to assume that we cannot perceive the kind of threats that we will face in the future. Do you think that the Bill is wide-ranging and flexible enough for the Government to be able to respond to future threats and, if not, what could be done to make it more future-proof?

Howard Watson: I actually think the structure of the Bill accommodates that quite well. It allows secondary legislation and guidelines to be upgraded. We note the critical role of the National Cyber Security Centre working with Government in doing that. I think, actually, you have taken care of that well with the way the Bill is structured.

Alex Towers: Yes, I would completely agree with that. I suppose our concern, slightly, at the minute, is to see some of the detail that is going to sit underneath the Bill in terms of a code of practice, in particular, and secondary legislation, because that is where it will become clear exactly what the implications are for operators. The sooner we can see some of that detail and get into the teeth of that, that would be great; but the way the Bill is structured, to allow that sort of detail to be updated on a regular basis as the world changes around us, seems totally sensible.

Q19 Mr Jones: The debate to date has mainly been around hardware, but you raised the issue—the bigger threat, certainly that I see, is from hacking and the vulnerability there. In terms of diversification, to be honest, we will have two vendors for the next considerable time, so when we talk about the diversification strategy and getting new vendors into the market, what timescales are we looking at? Are we actually putting all our eggs

[Mr Kevan Jones]

into the open RAN basket? I agree that there is the possibility of advancing that sector in the UK. Realistically, we will have those two, one of which, we know, is financially vulnerable. What difference would having just one vendor make to you?

Howard Watson: Let me work through that. First, from our perspective, given that we do have quite a large amount of BT in our mobile network, which is with the high-risk vendor, we have a large swap-out programme already under way. Effectively, we already use Nokia to extend their reach, but also to introduce Ericsson. That essentially means that I will be replacing a significant amount of my network over the next seven years.

It is quite difficult for me to start introducing new opportunities and new options into that, certainly in the early part of that. For my network, I see the opportunities in the latter part of this decade, not the early part. That does not mean that there will not be opportunities to try open RAN in some of the rural areas or to conduct some trials with the other vendors that we have talked about. It is very much an industry approach that we are taking here. Some of my colleagues may be able to move a bit earlier. It is important that we collaborate and work as a UK set of operators with the Government to make sure that we have the right rich set of solutions.

We would not want to come down to just one vendor. That would certainly be a worry for many reasons, so we need to continue to ensure that, in the short term, we absolutely have the choice of two.

Alex Towers: Given the timeframes that Howard has described, it is a five to seven-year cycle of replacement for the vendor. That is why it makes sense, we think, to go big now on large-scale trials of things like open RAN. The important investment in R&D and the £250 million is a good step towards that, but we will probably need some more, because we need to be ready for the next cycle if it is going to be a workable solution in future.

Q20 Chi Onwurah: Thanks very much for joining us. We have heard that open RAN will not be mature for another eight years. Do you agree with that assessment? In that case, as you have outlined, we have two vendors and potential financial concerns about one. Can you say categorically whether it is possible to have network security with only one full-scale vendor to choose from and whether it is possible to have that with two?

Secondly, we heard from Sir Richard Dearlove, the previous head of MI5, that when Huawei was first used as a vendor or equipment supplier by BT, it was not considered worth informing Ministers of that fact, despite what he considered to be evident security concerns. Can you say what in the Bill changes that so that the Government of the day will be better aware of ongoing and future security concerns?

Thirdly, on behalf of Catherine West, on international collaboration, what presence do you have on standards bodies? Can you say what your budget is for research and development so that we can see how that compares with the £250 million on offer?

Alex Towers: I will defer to Howard on the questions about standards and technical details. On your point about the relationship with Government, I do not think that any of us were around in 2005, but I know that there is some sort of contested story about exactly who was told what about the introduction of Huawei. You would—*[Inaudible.]* We have moved a long way on that. We have a very close working relationship with the NCSC and with other parts of Government, and we would be very confident that we are constantly in contact with them about exactly the mix of suppliers that we are using. The introduction through the Bill of TSRs will take that even further, so we would be very confident that we have got a good enough structure there to ensure that any concerns that any part of Government had would be captured and dealt with, and Ofcom is also now in a position to regulate.

The question about relying on just the one supplier is less a concern about security and more one about the commercial resilience of that position. Howard can probably say a little bit more about the standards and the technical questions around that.

Q21 Chi Onwurah: Do you not think resilience is part of security? Is a network secure if it is not resilient?

Alex Towers: I think they overlap and that is one of our questions about the drafting of the Bill. There is clearly a relationship between those two things, and the concern about the timeframes for the removal of Huawei, for example, has been partly about ensuring that we have operational resilience during what is going to be a very complicated engineering programme to take out all its kit without losing resilience, in the sense of outages and blackouts for customers. Some of the Bill's provisions talk about outages, but there is a difference between outages for operational maintenance and updating of kit and outages because of a security issue or attack. It is going to be quite important to pull those threads apart a little bit.

Howard Watson: On the vendor point, to summarise the approach that we are taking, we stopped purchase at the end of December, we will stop deployment in September of this year, we get down to 35% by two years hence from the end of next week, and then we have it removed from the mobile network by December 2027. I think that timeframe works well for us with introducing effectively a third supplier into our mobile network in terms of that 2027 point. It certainly helps mitigate any future steps in terms of a two-to-one.

I would not bank on it taking a full eight years to have an open RAN opportunity. As we heard from Andrea, colleagues at Vodafone have already started deployment . The real challenge there is about being able to use open RAN in dense urban areas where the technology works at its hardest, shall we say.

On your final question about research, we are in the top five investors in R&D in the UK—we invest in excess of £500 million a year across both research and development. In fact, the only companies that research more than us in the UK are the pharmaceuticals. I have 280 researchers based in the BT labs at Adastral Park near Ipswich and they, plus a standards organisation —we also draw in from engineers across my organisation— remain really actively involved in the standards bodies. I welcome what colleagues from the other operators say and think it is really important that we maintain that as a UK presence and as a European presence to ensure that we are not lost in the middle of any risk of

divergence between the US and eastern and Asian countries and China. I would implore us all to work hard to ensure that that does not happen.

Q22 Matt Warman: Thank you to BT for your engagement thus far. I have two questions. The first is the same question I asked the other operators and is about the telecoms security framework. How confident are you that you will be able to comply with all the strictures in that? Secondly, to develop one of the questions that you have just answered, 2027 is very much a deadline and not a target. It is important that we hear more about your ability to meet that target. How taxing is that? How do you plan to make sure that everything you do can encourage the presence of a third—or more—vendor over the time we have between now and then?

Howard Watson: Let me take the final part of that question first, Minister. We are very much aware that that is a deadline, not a target, but we welcome the fact that the deadline is 2027. I have given evidence previously and have talked with Government significantly about the real risks to the availability of service if we pull that date forward.

We have a lot of infrastructure. That deadline allows us to plan carefully how we can switch off a site, if we have to, to replace it and swap it out, so that the spike has overlapping coverage from adjacent sites. Were we to be required to bring those timescales forward, we would be talking about mobile blackouts in the UK, which clearly we all want to avoid, given the increasing dependence of UK citizens on networks. We have a plan that gets us to that. The 35% by 28 January 2023, just two years away, is a little bit more challenging, but we have a plan to get us there. The pandemic is making that challenging, but right now we are on track for that too. I think that answers the second question.

In answer to your first question, the ambition that we have, and what will become requirements across the TSRs, will put the UK ahead of the pack, in being a safe place for people to work and run businesses, secure in the knowledge that we have a high level of protection against cyber-threats. We welcome that, particularly in the environment in which we are now operating.

We have remaining questions—we raised some of those in our written evidence—about the sequence by which the requirements will be applied. We think it is critically important that there is a strong baseline level of compliance that applies to everybody who operates a network in the UK. We do not want to have entry points through weak links across our environment.

Alex Towers: A large majority of what is in the TSRs reflects current best practice and we are already complying with it. There are some places where there is a stretch for us to do more, which is good. The key point, I suppose, concerns Howard's point about making sure that the baseline for all operators is higher and strong enough, given that these are inter-connected network, as you have already heard this morning. The whole edifice is only as strong as its weakest point. We are concerned about the idea that the code of practice might not apply to some operators, for example. That is the sort of detail that we will begin to see debated further as the Bill goes through.

The Chair: Are there any further questions from Members?

Q23 Chi Onwurah: I was interested in what you said about the weakest link for networks. I agree wholeheartedly with that. What are your thoughts on fixed networks? While the Government are consulting on fixed networks, apparently they are not minded to require the removal of high-risk vendors from existing fixed networks. You have Huawei in your fibre-to-the-cabinet network. Do you agree with that? Do you think that there is a reduced risk in the existing fixed network? Do you intend to remove high-risk vendors—that is, Huawei—from existing full-fibre build? Do you think that presents a security risk?

Howard Watson: We do believe that fixed networks, whether full-fibre or fibre-to-the-cabinet, have a different risk profile—a lower risk profile—from mobile networks. Please remember that it is only in the access part of the network, so the fibre—the device in the exchange that connects to that. In the core of the fixed network, we have no presence of high-risk vendors. So we do believe that is manageable. We worked really closely with DCMS and NCSC to arrive at the 35% threshold that was published a year ago, and we think maintaining that in the fixed network is proportionate and sufficient to ensure security there, combined with the oversight that, again, we continue to support from the HCSEC and NCSC to ensure that we are inspecting everything that goes into the network.

I will also say that it is essential that we do take that approach because, as you know, we have large ambitions to increase full-fibre coverage in the UK. Ofcom reported in December that that was now at 18%. We at BT have now built for 3.5 million homes. We have a plan, which we have talked about—this is with the right conditions—to get to 20 million. We do need that 35% to be part of that plan because, again, introducing alternative vendors is challenging.

Q24 Chi Onwurah: Can you say why the risk profile is different for fixed as opposed to mobile?

Howard Watson: Fundamentally, you are dealing with a customer that is a fixed end point, so you are not having to provide handover between different sites as you do in mobile. Essentially, we are taking an electrical signal, modulating it into optical and converting it back to electrical at the other end, in very standard ethernet-based protocols. It is therefore really easy to see if there is a problem, so if something was infiltrating the network, we would spot it very quickly. Also, it is a very segmented network. The FTTC network has a granularity of over 85,000 cabinets in the UK, and the FTTP network has splitters for every 32 homes. Any issues are very easy to spot and so it is much easier to keep secure.

Q25 Chi Onwurah: Finally, with regard to having only two vendors for the mobile network for a number of years, can I ask two questions? I think that there has been a little discussion about resilience versus security, but if you are dependent on two vendors, one goes down and you are dependent on the other, would you say that that network was still secure? And is an increase in prices for equipment likely to accompany the reduction in the number of vendors available?

The Chair: I am afraid you have only about a minute to respond. Which of you gentlemen would like to answer?

Howard Watson: I will take that. You are right. We want two vendors to be consistently in the market, so that we can continue to deploy. If one of them were to

fail—well, we insist on commercial and physical measures being in place such that we could step in and run the equipment that was already in the network, so it would not be switched off in the short term or anything like that; there would be no immediate threat to the existing network. It is the ability to build forward that is important.

As I think Alex mentioned earlier, the primary reason, which relates to the second part of your question, is that we want competition on pricing. As we have looked to have the two remaining vendors compete with each other for replacement of our Huawei estate, that has actually worked quite well as we have put in place contracts for that replacement.

The Chair: Gentlemen, I am afraid we have reached the limit of our own bandwidth this morning. That brings us to the end of the time allotted for the Committee to ask questions. I thank both gentlemen for their evidence. The Committee will next meet in this room at 2 o'clock this afternoon to take further evidence. Members will be delighted to know that they will have a far more accomplished and competent Chairman present.

Ordered, That further consideration be now adjourned. *—(Maria Caulfield.)*

1 pm

Adjourned till this day at Two o'clock.