Written evidence submitted by Oracle Corporation (TFP0006)

Introduction

Oracle in the UK

Oracle is a global cloud computing, software, and hardware company with many industry verticals, such as Oracle Communications, and employs thousands of people in the UK. A strategic supplier to the UK Government, it has more than 800 public sector customers of which hundreds have moved to Oracle Cloud. Current customers include the Home Office, Foreign, Commonwealth and Development Office, Department for Work and Pensions, Ministry of Defence, Ministry of Justice and the NHS. In addition to the close relationship Oracle enjoys with central government and devolved administrations, it also powers much of the economy with an estimated 80 percent of FTSE100 companies through to start-ups making use of Oracle Cloud. Notable UK customers include Ocado Group, Barclays and Hermes. Oracle continues to invest in the UK, recently launching the only dual-region cloud that has been specifically built for use by public sector organisations.

Executive Summary

Oracle is pleased to respond to the Foreign Affairs Committee inquiry into *Tech and the future of UK foreign policy.* Oracle has a critical role underpinning the success and security of allied countries around the world, working in partnership with central governments, and particularly closely with defence, intelligence and security agencies, providing them with cloud-based and emerging technologies. This, added to our strategic partnership with the UK Government and our wider role supporting devolved administrations, local government, critical national infrastructure and much of the wider economy, means Oracle has a unique perspective to share.

The *Call for Evidence* set out the scope of this inquiry and this written submission will therefore focus on the key areas of cloud technology, cybersecurity and 5G. It aims to set out clear recommendations for how the UK and other allied countries can work together more effectively to safeguard critical national infrastructure and navigate the increasingly complex threat environment, where, as the recent *Integrated Review of Security, Defence, Development and Foreign Policy* made clear, cyber security considerations will be increasingly central.

Oracle's key observations and recommendations include:

- The UK should take a global leadership role in raising the profile of common standards setting for cybersecurity and 5G and make this a priority of its G7 presidency. This should also be prioritised on the agendas of other groupings such as the D10 and Five Eyes.

- The UK should harness the benefits of the cloud technologies underpinning 5G, particularly where these sit within the capabilities of allied countries and/or trusted providers.

- Greater focus should be given to the role cloud-native principles and cloud service providers can play in dealing with concerns over high-risk vendors and supply chain security and diversification.

<u>Tech and the future of UK foreign policy</u>

Cloud technology and cybersecurity considerations

Cloud-adoption trends

The market for cloud technology globally and in the UK continues to grow, as it has done consistently over the last decade. With Covid-19 prompting a rapid shift to remote working and access to business and public services, it will be no surprise to the Committee that the pandemic has led to a significant uptick in cloud-adoption, including by organisations with little or no previous experience with cloud. This will inevitably lead to these organisations focusing over the coming months on replacing tactical, short-term IT modernisation solutions with more strategic and long-term ones. These decisions are crucial as cloud technologies enable customers to connect their entire business ecosystems through a suite of applications and services. This leads to fundamental changes in the way businesses collect and analyse data, transforming overall business strategy.

While the pandemic has undoubtedly been a catalyst for further growth in cloud-adoption, many of the underlying trends in the market prior to the onset of the pandemic signalled a similar direction of travel, and we expect these to continue. The cloud migration and modernisation market globally is currently estimated to be worth around $88bn but is expected to grow to roughly $516bn by 2027. While these developments are to be welcomed for the benefits they will bring to organisations across the public and private sectors, they also come with cyber security challenges that should be an increasing focus of public policymakers in the domestic and international spheres, to ensure these technologies are safeguarded against potential threats.

Building-in security from the outset

Cloud architectures are differentiating, including in relation to security capabilities, and as a result, organisations across the public and private sectors can now take advantage of the innovation in this space. Organisations considering cloud-migration should look only to cloud providers that ensure security is foundational across all products and services. Those in charge of procurement decisions should look specifically for autonomous capabilities that eliminate human error - often the primary cause of some of the most recent and high-profile breaches - to be built-in from the outset. Additionally, they should also look for Artificial Intelligence (AI) and Machine Learning (ML) to be leveraged throughout all products and levels. These capabilities prevent, detect, respond to, and predict sophisticated security threats throughout the network.

As cloud migrations increase and the threat environment becomes more complex, it is vital that countries centre cybersecurity considerations in their strategic thinking about the global threat environment. Oracle was particularly pleased to note that the recently published *Integrated Review of Security, Defence, Development and Foreign Policy* committed to developing a UK Cyber Strategy later this year.

We encourage the Committee to help ensure that cybersecurity remains at the forefront of the UK Government's thinking in the implementation of the integrated review, and that the UK embraces the challenge of adopting a leadership position in the setting of global cybersecurity standards. For example, the UK could use its position across a range of groups and institutions, such as the G7, D10 and Five Eyes, to vocally support better coordination on enforcement action to more effectively deter states from supporting, tolerating or neglecting cyber-attacks. Additionally, the UK's exit from the EU and the new trade agreements it is now seeking to negotiate could provide a timely opportunity to review best practice and new methods of cooperation on cybersecurity via trade deals in particular, and more broadly through Mutual Assistance Treaties and R&D collaborations.

Cloud-native 5G

5G supply chain security

In recent years, it is 5G that has increasingly become the frontline of efforts to counter security threats and ensure critical networks and infrastructure remain secure and open to fair competition. While Oracle supports the recent strong measures taken by the UK Government and its allies to safeguard critical parts of the 5G network, we think it is important that there is better recognition of the role cloud-native principles and cloud service providers can play in allaying many of the security concerns that have been raised in relation to high-risk vendors.

As the Committee will be aware from other recent inquiries, 5G networks are increasingly built in data centres and accessed through cloud services, requiring telecommunications-specific technologies to be replaced with IT technologies. Cloud-native 5G benefits from the cloud's scale, reliability and security. Network functions are carried out in software, meaning there are additional tools such as network slicing, containerization, and zero-trust software defined perimeters to further enhance security.

This shift to an IT-based supply chain for 5G is important because it means moving from a fragile telecommunications equipment supply chain to an agile, secure, and diverse IT supply chain where there are a host of trusted vendors who can compete in the software space, particularly as 5G technology requirements fall in the sweet spot of the software and IT industry in both the UK and US as well as other allied countries. This presents a new opportunity to shift the security advantage in favour of countries who share the interests of the UK and US and away from those players who would potentially seek to cause harm, mitigating the risks associated with telecoms vendors vulnerable to third country influence.

The security and competition concerns in the market become all the more crucial from a government perspective when the true nature of 5G is considered. At its most fundamental, 5G supports devices to connect in a concentrated area – covering all kinds of activities such as industrial processes and logistics. Unlike 4G and previous generations, a significant number of these networks will be private and in the enterprise market. Consequently, the potential damage caused through cyber threats and security breaches may be even more significant.

We encourage the Committee to consider these unique security attributes that can now be brought to bear in 5G technology and its supply chain as an important line of defence in the cyber security capabilities of the UK and its allies.

Diversification in 5G

Recognition of this new landscape appears absent in many of the policy conversations around the 5G supply chain and vendor ecosystem in the UK, abroad and in international institutions. As we move towards a global telecommunications architecture that is IT and cloud-centric, software solutions become available to tackle the problem of a supposed lack of diversity in the 5G supply chain and reduce the need to depend on high-risk telecoms vendors – something which the Committee will note is currently being explored by the '5G Supply Chain Diversification Strategy' being led by the Department for Digital, Culture, Media and Sport and which we were also glad to see addressed in the resolutions which came out of the G7 'digital track' ministerial summit in April 2021.

With this shift to the virtualization of the 5G network, the market of providers is extended beyond the telecoms hardware providers typically considered - Nokia, Erikson and Huawei. A whole new set of competitors can enter the market, in particular cloud and software companies like Oracle. This choice drives further competition, which in turn means the market benefits from a virtuous circle of rapid evolution with providers competing to improve capabilities and drive innovation.

Creating a viable and sustainable market for these new entrants will be crucial. This could be done by the UK working with partners and allies to better promote 5G private or enterprise networks, which could result in a potential marketplace for new entrants rather than the current ~800 mobile providers. Central to this will be exploring how spectrum can be made more affordable and readily available to small and large enterprises alike.

In assessing the security challenges that the 5G market faces, the UK and its allies should factor in the role of software and not limit potential solutions to physical equipment, to take advantage of new business models and innovative 5G applications. Governments should look to foster an environment where firms with a trusted history of IT expertise can compete fairly as they deliver new 5G services to the market. The UK should therefore work with partners and allies to support the fair competition needed to realise the full ecosystem of 5G vendors while holding to account those who are not competing fairly or pose a threat.

International collaboration

5G supply chains are increasingly complex and dependent on a global network of suppliers which require governments and companies to make complex risk mitigation decisions. There is no shortage of supply chain risk management efforts, but the results to date have largely resulted in a collection of existing standards and best practices rather than a clear framework. This underlines the need for a more integrated and cohesive approach to global standard-setting and leadership to tackle cyber threats and to ensure that the current lack of consistency in approach does not provide an opening for those launching attacks or seeking to undermine the security interests of the UK and its allies.

To give a clear example, an improved approach to risk management is a framework-based model, such as the one developed at the Prague 5G Security Conference, where nations agreed to a set of recommendations for governments to consider as they design and deploy 5G systems. These Principles include recommendations on supply chain security for telecommunications infrastructure and networks, and on managing the risks associated with vendors vulnerable to third country influence. Such a framework can move supply chain discussions beyond cataloguing standards and best practices. Further, it provides a standard that removes the burden of "proving" a company is untrusted by finding evidence of implants or backdoors.

More broadly, Oracle supports efforts of like-minded countries to adopt consistent measures to promote alternatives to high-risk vendors, particularly where software solutions built in the cloud can help to diversify and secure 5G supply chains. In so doing, Oracle recommends that the UK and its allies should also consider how to best leverage industry expertise, such as through regular and active collaboration with industry players who are already defining global security standards via security organisations. Doing this globally and with allied partners is necessary to inform a broader perspective of the threat environment and to address emerging cybersecurity concerns.

Conclusion

In a rapidly shifting threat environment where companies and governments alike increasingly look to the cloud to modernise their services and functions, it is more important than ever that UK foreign policy takes full account of the role that tech companies can play in addressing cyber security threats and safeguarding critical digital infrastructure.

Oracle is a longstanding provider of mobile network technology and has provided UK businesses with the technology for their networks from 2G through to 5G. Based on insights from this unmatched cyber security pedigree, our aim with this submission is to underline the ways in which we believe the UK can steer the agenda with its allies in responding to threats, particularly in light of recent concerns about the safety and security of 5G networks.

In practical terms, we believe there is more scope for the UK to play a global leadership role in raising the profile of standards setting for cybersecurity generally and 5G specifically, particularly by spearheading collaboration of like-minded countries with trusted industry partners who are already defining global security standards. In a year when the UK holds the presidency of the G7, this is an opportunity that should not be missed, and every effort should be made to ensure it is also carried through as a priority to the German presidency in 2022. It is also an issue that should be prioritised on the agendas of other groupings and bodies such as the D10 and Five Eyes.

Oracle is also supportive of measures to ensure that critical 5G networks are protected from potential exposure to threats, and we believe that the UK should increasingly focus on supporting and championing the cloud-native principles and software solutions that underpin 5G networks. We would underline the cross-cutting benefits of this in terms of both protecting the UK's fundamental security interests and in dealing with the contemporary policy challenge of securing and diversifying the 5G supply chain.

We appreciate the opportunity to provide our insights and recommendations, and we would be happy to speak privately to the Committee members or clerks to further discuss our submission and to provide additional context or information where that might be required.

May 2021