**Designated Vendor Direction under section 105Z1 of the Communications Act 2003, given to [a Public Communications Provider]**

Background

1. Section 105Z1 of the Communications Act 2003 ("the Act") provides that the Secretary of State may give a 'designated vendor direction' to a public communications provider if the Secretary of State considers that it is necessary in the interests of national security. Such a direction may impose requirements on a public communications provider with respect to the use of goods, services or facilities supplied, provided or made available by a 'designated vendor' specified in the direction.

2. On 13 October 2022, the Secretary of State issued a 'designation notice' under section 105Z8 of the Act, designating Huawei Technologies (UK) Co., Ltd. and its affiliated companies (together, "the Huawei corporate group" or "Huawei") for the purposes of a designated vendor direction.

3. Reference to a 'network' in this direction means a "public electronic communications network", as defined by section 151(1) of the Act (see paragraph 7(h) below).

The Designated Vendor Direction (the "Direction")

4. **The Secretary of State hereby imposes the following requirements, in accordance with Section 105Z1 of the Act, on [the Public Communications Provider] ("the Public Communications Provider"), with respect to the use of goods, services or facilities supplied, provided or made available by Huawei.**

5. **Accordingly, the Public Communications Provider:**[1]

   **(1) at any time after the date this Direction comes into force, must not make use of any Huawei equipment in its 5G networks if such equipment was procured after 31 December 2020.**

   **(2) at any time after the date this Direction comes into force, must not make use of any Huawei equipment in any network, except for fixed fibre access**

[1] A table summarising the requirements imposed on the Public Communications Provider is produced at Annex C to this Direction.

**networks, if the manufacturing process or supply chain for such equipment has been altered as a result of changes to the United States Foreign-Produced Direct Product Rule announced on 19 May 2020 and 17 August 2020.**

**(3) at any time after the date this Direction comes into force, must not install any Huawei equipment in any fixed fibre access network if the manufacturing process or supply chain for such equipment has been altered as a result of changes to the United States Foreign-Produced Direct Product Rule announced on 19 May 2020 and 17 August 2020.**

**(4) at any time after the date this Direction comes into force, must not install, or allow to be installed, any Huawei equipment in 5G networks, except where:**

**(a) such equipment has been installed or deployed in [the Public Communication Provider's] network before the time and date this Direction comes into force; and/or**

**(b) such installation is for the purposes of directly maintaining Huawei equipment installed before this date.**

**(5) at any time after the date this Direction comes into force, must not make use of Managed Services provided by or on behalf of Huawei in respect of any network, except where Specialist Maintenance Services are provided by or on behalf of Huawei in relation to Huawei equipment.**

**(6) at any time after 28 January 2023, must not make use of Huawei equipment or any services delivered by or on behalf of Huawei in parts of mobile access networks which could provide service to subscribers located within such Sites Significant to National Security of which the Public Communications Provider had been notified by the Secretary of State on or before the date of this Direction.**

**(7) at all times after 31 July 2023, must restrict the use of Huawei equipment in its 5G networks, so that:**

**(a) Huawei equipment serves at most 35% of each class of 5G Base Station sites on any particular 5G access network, calculated by the method specified at Annex B.1 to this Direction;**

**(b) the network traffic volume passing through Huawei equipment in any particular 5G access network is at most 35% of the total expected network traffic volume for that particular 5G access network, calculated by the method specified at Annex B.2 to this Direction; and**

**(c) in relation to any other functions which are part of the 5G access networks, at most 35% of the network elements from a particular equipment class in any particular network is provided by Huawei, calculated by the method specified at Annex B.3 to this Direction.**

**(8) at all times after 31 October 2023, must restrict the use of Huawei equipment in its Fibre to the Property (FTTP) and other gigabit and higher capable access networks, so that:**

**(a) at most 35% of premises passed by a network are served by Huawei equipment, calculated by the method specified at Annex B.4 to this Direction; and**

**(b) in relation to any other functions which are part of the networks, at most 35% of the network elements from a particular equipment class in any particular network is provided by Huawei, calculated by the method specified at Annex B.3 to this Direction.**

**The Public Communications Provider must provide the Secretary of State with a report on or before 31 July 2023 summarising the steps it has taken, and those further steps it intends to take, in order to ensure compliance with this requirement by 31 October 2023.**

**(9) at any time after 31 December 2023, must not make use of Huawei equipment or any services delivered by, or on behalf of, Huawei in the execution of its Core Network Functions. The Public Communications Provider must provide the Secretary of State with reports on or before 28 January 2023 and on or before 31 July 2023 summarising the steps it has**

**taken, and those further steps it intends to take, in order to ensure compliance with this requirement by 31 December 2023.**

**(10) at any time after 31 December 2025, must not make use of Huawei high data rate intra-core and inter-operator transmission equipment in any part of its core networks.**

**(11) at any time after 31 December 2027, must not make use of Huawei equipment or any services delivered by, or on behalf of, Huawei in any part of its 5G networks.**

**(12) to the extent that use of Huawei equipment or services in any network is not otherwise prohibited by the requirements set out above:**

**(a) the Public Communications Provider must not use Huawei equipment at any time after 14 April 2023 unless:**

**(i) the Security Risk of any such equipment has first been evaluated under the relevant Risk Mitigation Strategy; and**

**(ii) in light of the results of any evaluation mentioned in paragraph 5(12)(a)(i), the Public Communications Provider reasonably considers the Security Risk associated with the equipment has been satisfactorily mitigated given its function. The Security Risk associated with such equipment will be satisfactorily mitigated if its quality and security is of at least comparable quality and security to equivalent equipment produced by or on behalf of other vendors.**

**(b) with the exception of Emergency Patches that are in the Public Communications Provider's reasonable opinion critical to maintaining the security or resilience of the network (to which paragraph 5(12)(c) below applies), the Public Communications Provider must not install modifications to Huawei equipment (including modifications made by means of patches or updates) provided by or on behalf of Huawei at any time after 14 April 2023 unless:**

**(i) the Security Risk of any such modified equipment has first been evaluated under the relevant Risk Mitigation Strategy; and**

**(ii) in the light of the results of any evaluation mentioned in paragraph 5(12)(b)(i), the Public Communications Provider reasonably considers the Security Risk associated with the equipment has been satisfactorily mitigated given its function. The Security Risk associated with such equipment will be satisfactorily mitigated if its quality and security is of at least comparable quality and security to equivalent equipment produced by or on behalf of other vendors.**

**(c) where Emergency Patches are installed and are, in the Public Communications Provider's reasonable opinion, critical to maintaining the security or resilience of the network, the Public Communications Provider must ensure that:**

**(i) the Security Risk introduced by the use of such Emergency Patches are mitigated as far as can reasonably be achieved; and**

**(ii) the ongoing use of such Emergency Patches has been agreed by the Secretary of State following an evaluation of the effectiveness of such mitigation.**

**(d) at any time after 14 April 2023, the Public Communications Provider must not make use of any Huawei equipment within its 5G networks where the notified end-of-support date for that equipment, or any individual component of that equipment, has passed.**

**(e) within one week of the date this Direction comes into force, the Public Communications Provider must provide the Secretary of State with full details of its current and planned use of Huawei equipment within all of its networks.**

**(f) at all times after the date this Direction comes into force, the Public Communications Provider must ensure that any remote access to any**

**of its networks is only granted to Huawei employees or individuals acting on behalf of Huawei where:**

**(i) except for the purposes of providing Specialist Maintenance Services, access is undertaken from within the United Kingdom; and**

**(ii) access is monitored in real time by employees of the Public Communications Provider which the Public Communications Provider reasonably considers to be appropriately skilled to monitor any national security risks arising from such access.**

**(g) at all times <u>after 14 April 2023</u>, the Public Communications Provider must ensure that physical access to its networks is only granted to Huawei employees or individuals acting on behalf of Huawei where such employees or individuals are accompanied and monitored by employees of the Public Communications Provider which the Public Communications Provider reasonably considers to be appropriately skilled to monitor any national security risks arising from the provision of such access.**

**(h) at all times after <u>the date this Direction comes into force</u>, the Public Communications Provider must take all reasonable steps to enable testing and analysis of any Huawei equipment used within its networks as is reasonably required by the NCSC from time to time.**

6. **This Direction shall come into force at 12:01am on 14 October 2022.**

<u>Interpretation</u>

7. In this Direction:

a. '5G network' means a set of all relevant network infrastructure elements for mobile and wireless communications technology used for connectivity and value-added services with advanced performance characteristics, such as very high data rates and capacity, low latency communications, ultra-high reliability, or supporting a high number of connected devices. These may include legacy

network elements based on previous generations of mobile and wireless communications technology such as 4G or 3G. 5G networks should be understood to include all relevant parts of the network.

b. '5G Base Station' means any class of base station supporting or routing functionality added in the Third Generation Partnership Project's Release 15 or later releases, in support of "3GPP New Radio" air interface connections (including between base stations), which provides services with advanced performance characteristics, such as very high data rates and capacity, low latency communications, ultra-high reliability, or supporting a high number of connected devices.

c. 'Core Network Function' means one of the functions listed at Annex A to this Direction.

d. 'Emergency Patches' mean small modifications to products designed to fix specific issues or vulnerabilities.

e. 'Huawei equipment' means any item containing hardware, software or firmware components which are designed, produced, developed, assembled or manufactured by or on behalf of Huawei, and which is intended for use as part of a telecommunications network. A telecommunications network includes the network's operational functions, as well as any carrier-grade or enterprise supporting systems or functions. Under this definition, Huawei equipment does not include:

    - Equipment which is purely passive. 'Passive' equipment is equipment that does not perform any role in the routing or processing of network data. (For the avoidance of doubt, any microprocessor contained in the equipment has no role in the processing of communications signals or user data.)

    - Equipment components without any functionality, such as licence keys.

    - Consumer Product Equipment (CPE).

f. 'Managed Services' are any services where Huawei interacts with any network equipment on behalf of the Public Communications Provider. It does not include

any specialised maintenance support necessary to maintain Huawei equipment where that support can only reasonably be provided by Huawei.

g. ‘National Cyber Security Centre’ or ‘NCSC’ means Government Communications Headquarters acting through the National Cyber Security Centre.

h. ‘Network’ means a “public electronic communications network”, as defined by section 151(1) of the Act.

i. ‘New Huawei equipment’ means Huawei equipment which has not previously been installed or deployed in the Public Communication Provider’s network at the time and date specified at paragraph 6 above.

j. ‘Risk Mitigation Strategy’ means:

    a. the arrangements provided by the Huawei Cyber Security Evaluation Centre (“HCSEC”); or

    b. in the event that the Secretary of State determines that:

        i. HCSEC no longer provides adequate and effective mitigation arrangements, or

        ii. it is disproportionate to evaluate the risks arising out of the use of Huawei equipment under the mitigation arrangements provided by HCSEC in cases where such equipment was installed by the Public Communications Provider prior to the date this Direction comes into force,

    such alternative arrangements as the Secretary of State, having consulted with NCSC, may deem necessary and proportionate.

k. 'Security Risk' means any risk arising out of the current use of the Huawei’s equipment in networks, the ownership and operating locations of Huawei, the equipment quality and transparency of the Huawei’s engineering practices, the past behaviour of the vendor, the continuity of supply, whether the equipment is End-of-Service or End-of-Life, and equipment modifications due to sanctions.

l. A list of 'Sites Significant to National Security' has been provided on a confidential basis to the Public Communications Provider only insofar as this element of the Direction is relevant to the Public Communications Provider.

m. 'Specialist Maintenance Services' means third-line support maintenance for Huawei equipment which only Huawei can provide.

n. The date on which equipment is 'procured' shall be taken to be the date on which the transaction is initiated.

Reasons for the Direction

8. In accordance with section 105Z1(5)(b) of the Act, the Secretary of State considers that this Direction is necessary in the interests of national security for the following reasons.

(1) The Huawei corporate group is headquartered in, and controlled from, China. The Government assesses that the Chinese State and associated actors have carried out, and are expected to continue to carry out, cyber-attacks against the United Kingdom and the United Kingdom's interests. In particular, the Chinese State and its associated actors continue to seek to exploit weaknesses in telecommunications service equipment, and/or in how providers of public electronic communications networks build and operate their networks, in order to compromise their security.

(2) Practices of the Chinese State, coupled with the way in which it operates laws such as the Chinese National Intelligence Law 2017 (amended in 2018), can enable the State to require companies based in China and their employees to engage in activities which are harmful to the United Kingdom. The way in which the rules are operated means such companies can be required to direct their subsidiaries to engage in activities which are harmful to the United Kingdom. Huawei's employees can also be required to comply with directions issued by the Chinese State without the knowledge of Huawei. These powers give rise to a risk that covert and malicious functionality could be embedded in Huawei equipment. This risk will further increase if the United Kingdom's dependency on Huawei for the provision of Fibre to the Property (FTTP)and Mobile networks increases.

(3) The cyber security and engineering quality of Huawei's products and services give rise to a real risk of hostile exploitation and/or systemic failures. In this regard, the Huawei Cyber Security Evaluation Centre Oversight Board has raised significant concerns about Huawei's engineering processes in its 2018, 2019, 2020 and 2021 annual reports. The 2020 Report stated that "*NCSC has now seen evidence of significant issues in Huawei's product quality over a number of years"*. The 2021 Report stated that the Board *"continues to uncover issues that indicate there has been no overall improvement over the course of 2020 to meet the product software engineering and cyber security quality expected by the NCSC"*.

(4) The Secretary of State's concerns over the quality of Huawei's products and services have been exacerbated by sanctions imposed by the United States against Huawei. These sanctions have led to changes to the manufacture of some Huawei products which may have reduced their reliability and made it harder to remedy any deficiencies. Further:

(a) As a result of changes to the United States' Foreign-Produced Direct Product Rule in May 2020 and August 2020, set out in the Export Administration Regulations made under the US Export Control Reform Act 2018, Huawei is unable to purchase or manufacture equipment, in particular semiconductors, where they are designed or produced using specified United States technology, unless companies or persons supplying Huawei with goods containing such technology have applied for, and been granted, a licence to do so by the United States Government. There is a legal presumption of denial of any application for a licence. The Secretary of State is not currently aware of any such licences having been granted in respect of 5G equipment. As a result of this serious impact on Huawei's manufacturing processes and supply chains, Huawei has been forced to manufacture semiconductors and other equipment using unknown and untested tools, which makes the provision of adequate assurance for products manufactured in this way significantly more challenging and potentially impossible.

(b) The ongoing effect of sanctions, the risk of future enforcement and escalation of those sanctions, as well as the expiry in August 2020 of the 'Temporary General License' granted by the United States (which

permitted some supply to Huawei), have affected and continue to have the potential to affect, without advance notice, Huawei's ability lawfully to provide Managed Services (support and maintenance services which are designed to ensure the continued day-to-day operation of networks).

(c) As a result of the impact of US sanctions, Huawei is moving significant aspects of its supply chains to China and is increasingly reliant on the use of Chinese technology. As a result, in its involvement in the United Kingdom's Fibre to the Property (FTTP) and Mobile networks, Huawei is increasingly reliant on unknown and untested components. This raises serious national security concerns.

(5) Huawei has a significant market share in the United Kingdom's FTTP and Mobile Access (MA) networks, estimated in July 2019 at 44% and 35% respectively. In light of Huawei's size and the scale of its operations, it has the ability to increase its market shares in the FTTP and MA networks in a way which creates a significant risk of national dependency. Without intervention, it is highly likely that the United Kingdom will become dependent on Huawei for the provision of FTTP and MA networks. These networks form part of the United Kingdom's critical national infrastructure. Due to the national security concerns set out at sub-paragraphs 8(1) to (4) above, dependency on Huawei significantly increases the potential impact of any systemic failures or hostile exploitation and therefore gives rise to unacceptable risks to national security.

(6) The cumulative national security risks posed by Huawei described above significantly exceed the national security risks posed by the equipment and services provided by other vendors. Huawei's risk profile can only be managed through specific enhanced measures pursuant to a designated vendor direction.

9. The Secretary of State considers that the requirements imposed by the Direction are proportionate to what is sought to be achieved by it, and therefore satisfy the condition at section 105Z1(2)(b) of the Act for the reasons set out below.

***(1) Use of Huawei equipment procured after 31 December 2020 in 5G networks***

10. The Direction requires the overall phasing out and ultimate termination of Huawei's involvement in 5G networks in the interests of national security. The use by public communications providers of Huawei equipment procured after 31 December 2020 in 5G

networks would undermine this overall aim. This requirement ensures that public communications providers remain on the 'pathway to zero' by discouraging them from procuring and installing in their 5G networks new Huawei equipment, and encouraging them to procure new equipment from other vendors.

***(2) and (3) use of Huawei equipment which is affected by changes to the US Foreign-Produced Direct Product Rule***

11. As a result of changes to the United States Foreign-Produced Direct Product Rule, Huawei is unable to continue relying on US technology and software in the design and production of its equipment, in particular semi-conductors. These developments have forced, and will continue to force, significant changes to Huawei's manufacturing processes and supply chains, which in turn means that effective oversight over Huawei equipment supplied to the United Kingdom has been, and will continue to be, more challenging or even impossible.

12. The Secretary of State considers that the national security risks posed by the use of Huawei equipment in fixed fibre access networks is more manageable than in other networks. The Secretary of State therefore considers it is proportionate to prohibit the installation of Huawei equipment affected by changes to the US Foreign-Produced Direct Product Rule in full fibre access networks, but not to prohibit (subject to the remainder of this Direction) equipment that has already been installed on the date this Direction comes into force. This differentiated approach is supported by responses received by the Secretary of State from a technical consultation with fixed network providers in April 2021 on supply chain alternatives to Huawei.

***(4) Installation of Huawei equipment in 5G networks***

13. The Direction requires the overall phasing out and ultimate termination of Huawei's involvement in 5G networks in the interests of national security. The installation by public communications providers of Huawei equipment after the date this Direction enters into force would undermine this overall aim. This requirement ensures that public communications providers remain on the 'pathway to zero' by encouraging them to install equipment produced by other vendors.

14. The Secretary of State also considers it proportionate to exclude from these requirements, first, installation of Huawei equipment which has previously been installed or deployed in

public communication providers' networks; and, secondly, installation of Huawei equipment for the purposes of maintaining other Huawei equipment.

***(5) Receipt of Managed Services***

15. Managed Service arrangements give Managed Service providers significantly higher levels of access to networks and/or sensitive data transmitted via or stored in such networks than most other service relationships. The level of access is such that a Managed Service provider has the potential to cause major network disruption and/or access quantities of sensitive data on a scale which undermines national security. In light of this threat, the Secretary of State considers that the national security risk of Huawei providing Managed Services is unmanageable. This risk has been further exacerbated by a series of United States sanctions imposed on Huawei, which have affected, and continue to have the potential to affect, without advance notice, Huawei's ability lawfully to undertake any Managed Service arrangements.

16. The Secretary of State considers that it is necessary to bring this requirement into effect as soon as possible upon the issuing of the Direction given the seriousness of the security risks of using Huawei Managed Services.

***(6) Sites Significant to National Security***

17. This element of the Direction is required because there are locations where pure metadata about the number, type and distribution of devices connected to public communications providers' local base stations could be used to establish information which could pose a significant risk to the United Kingdom's national security.

18. The Secretary of State has sought to balance the risk of Huawei having access to parts of mobile networks which could provide service to subscribers located at Sites Significant to National Security with the need to provide public communications providers sufficient time to change their vendor arrangements without suffering from the risks associated with rapid vendor change.

19. Pursuant to section 105Z1(6) of the Act, the Secretary of State is not required to specify the reasons for the Direction if, or to the extent that, the Secretary of State considers that doing so would be contrary to the interests of national security. Because public disclosure of the Sites Significant to National Security would give rise to national security risks, they have not been set out in this Direction but have been provided on a confidential basis

to the Public Communications Provider only insofar as the Public Communications Provider will be subject to this element of the Direction.[2]

***(7) 35% cap on use of Huawei equipment in 5G access networks; and (8) 35% cap on use of Huawei equipment in FTTP and other gigabit and higher capable access networks***

20. These elements of the Direction are necessary to reduce public communications providers' dependence on Huawei in all networks in the medium-term and to place them on a path to removing Huawei equipment from 5G networks in the longer term. However, placing the cap at lower than 35% or introducing an earlier deadline would risk the resilience of UK networks, given the current lack of diversity of supply in the market and the impact that the Covid-19 pandemic has had on providers' ability to remove Huawei equipment from their networks. The Secretary of State has therefore sought to balance the imperative of reducing Huawei equipment with the need to protect the medium-term resilience of the UK network, and has sought to avoid imposing a requirement which providers are unable to comply with in the timeframe specified.

21. As part of the element of the Direction relating to use of Huawei equipment in FTTP and other gigabit and higher capable access networks, the Secretary of State has also required the Public Communications Provider to summarise progress it has made by 31 July 2023. This will enable the Secretary of State to monitor and manage the ongoing national security risk posed by the use of Huawei equipment in these networks and ensure providers meet the 31 October 2023 deadline for compliance with the underlying requirement.

***(9) Use of Huawei equipment or any services delivered by, or on behalf of, Huawei in the execution of Core Network Functions***

22. The network 'core' is where critical functions are carried out and where the most sensitive data about a network's users is stored. Disruption to public communications providers' Core Network Functions could lead to significant interference with the operation of the network, including widespread loss of services, and significant data breaches. Because of the importance and sensitivity of the Core Network Functions, Huawei's cyber-security risk profile cannot be managed.

[2] The Secretary of State has not provided a list of Sites Significant to National Security to any public communications provider who will not be subject to this element of the Direction. Those who will be subject to this element of the Direction have been notified only of the Sites Significant to National Security which affect them.

23. Pursuant to this Direction, the Secretary of State has given the Public Communications Provider until 31 December 2023 to phase out Huawei involvement in its Core Network Functions. This provides sufficient time for the Public Communications Provider to switch to new vendors without incurring the risks associated with rapid vendor change or the risk of non-compliance with the Direction, whilst also balancing the risks of allowing providers to retain Huawei involvement in Core Network Functions in the short-to-medium term.

24. As part of this element of the Direction, the Secretary of State has also required the Public Communications Provider to summarise progress it has made by 28 January 2023 and again by 31 July 2023. This will enable the Secretary of State to monitor and manage the ongoing national security risk posed by Huawei's involvement in providers' Core Network Functions and ensure providers meet the 31 December 2023 deadline for compliance with the underlying requirement.

25. The Secretary of State also considers it proportionate, for the purposes of this requirement, to exclude high data rate transmission equipment from the definition of interconnection equipment at Annex A to this Direction, as this function is deemed to be less critical to national security than the other functions listed under 'Core Network Functions'. Accordingly, the Secretary of State has addressed the risk to network security posed by Huawei in relation to high data rate transmission equipment by way of a separate requirement (see below).

***(10) Use of Huawei high data rate transmission equipment***

26. High data rate transmission equipment is of crucial importance to the overall operation and functioning of the network. Interference with such equipment could therefore cause major network disruption, including widespread loss of services, which would undermine national security. Huawei's cyber-security risk profile cannot be managed in the medium to long term. However, against the national security risks arising from the continuing use of Huawei high data rate transmission equipment, the Secretary of State has had to balance the practical difficulties faced by providers and the impact on network resilience and network stability arising from rapid vendor change. For these purposes, "High-data rate transmission equipment" does not include equipment used at Cell Site Gateways or to provide Ethernet Backhaul Direct services.

***(11) Ending Huawei involvement in 5G networks by 31 December 2027***

27. The Secretary of State has sought to balance national security risks with the need to provide the Public Communications Provider with sufficient time to transition to new vendors. Because 5G networks will be of an even greater importance to the United Kingdom by 2027, and because of the expected availability of more reliable alternative vendors by this date, the Secretary of State considers that Huawei's presence in the United Kingdom's 5G networks beyond 31 December 2027 will constitute an unmanageable and unnecessary national security risk.

28. Further, as explained at paragraph 11 above, Huawei equipment, for which the manufacturing process or supply chain has been affected by changes to the United States Foreign Direct Product Rules, will be produced using untried and untested components which would not be capable of being subjected to adequate oversight. As a result, public communications providers will only be able to rely on stockpiles of equipment and parts unaffected by United States sanctions to maintain Huawei involvement in their 5G networks. The Secretary of State considers that, after 31 December 2027, there will no longer be enough spare equipment and parts of a sufficiently high security standard. As a result, there are significant national security risks of allowing public communications providers to continue with Huawei involvement in any element of their 5G networks after this date. Though the existing supply of equipment and spares of a sufficiently high security standard may be exhausted after 31 December 2027, the Secretary of State considers that a longstop date is needed to ensure market certainty and long-term network security.

***(12) use of Huawei equipment or services in any network not otherwise prohibited by this Direction***

29. The Public Communications Provider will still, in certain circumstances, be able to use Huawei equipment and services after this Direction takes effect, but only where the national security risks of such use are insignificant or can be effectively mitigated to a level that the Secretary of State accepts; or where the national security risks of ending Huawei involvement in networks outweighs the risks of continued involvement, for example where rapid vendor change is likely to cause network disruption.

30. Whilst the Public Communications Provider has overall responsibility to manage the national security risks associated with the use of Huawei equipment and services, in meeting those responsibilities, it will be able to make use of the relevant Risk Mitigation Strategy.

31. As at the date of the Direction, the Secretary of State anticipates (subject to the rest of this paragraph) that the Risk Mitigation Strategy will continue to be provided by the analysis undertaken by HCSEC. HCSEC plays a key role in ensuring Huawei equipment and services can be used by the Public Communications Provider in a way that minimises risks to the UK's national security, and currently no other vehicle provides a comparable level of risk mitigation. However:

    (1) should HCSEC no longer be capable of effectively evaluating the quality and security of equipment, whether that is in relation to individual pieces of Huawei equipment (including modifications to Huawei equipment) or categories of such equipment more widely; or

    (2) where it is disproportionate to evaluate the risks arising out of the use of Huawei equipment under the mitigation arrangements provided by HCSEC in cases where such equipment was installed by the Public Communications Provider prior to the date that this Direction comes into force,

    the Secretary of State will (having consulted with the NCSC) notify affected providers and specify what alternative mitigation strategy is to apply. As at the date of the Direction, the Secretary of State anticipates that, in the first scenario described above, such an alternative mitigation strategy would require the affected provider to take responsibility for carrying out the evaluation of Security Risks being provided by HCSEC as at the date of this Direction.

Signed:

Secretary of State for Digital, Culture, Media and Sport

**12 October 2022**

## ANNEX A: List of Core Network Functions

For all mobile and fixed networks, including 5G networks:

- Internet Protocol Core (including any function which performs Internet Protocol/Multiprotocol Label switching or routing within the core of a provider's network);
- Security Functions;
- Operational Support Systems (OSS) (except to the extent necessary to support any Huawei equipment deployed in a provider's network);
- Management and Authentication;
- Authorisation and Audit (AAA) functions;
- Virtualisation infrastructure (including Network Function Virtualisation Infrastructure (NFVI));
- Orchestrator and controller functions (including Management and Network Orchestration (MANO) and Software Defined Networks (SDN) orchestrators/controllers);
- Network monitoring and optimisation;
- Interconnection equipment (high data rate intra-core and inter-operator transmission equipment has been removed from this definition as it is subject to its own control) ;
- Internet gateway functions; and
- Lawful Intercept related functions.

For all 5G networks:

- 5G core database functions;
- 5G core-related services including but not limited to:
    - Authentication Server Function (AUSF),
    - Access and Mobility Management Function (AMF),
    - Unstructured Data Storage Function (UDSF),
    - Network Exposure Function (NEF),
    - Intermediate NEF (I-NEF),

    - Network Repository Function (NRF),
    - Network Slice Selection Function (NSSF),
    - Policy Control Function (PCF),
    - Session Management Function (SMF),
    - Unified Data Management (UDM),
    - Unified Data Repository (UDR),
    - User Plane Function (UPF),
    - UE radio Capability Management Function (UCMF),
    - Application Function (AF),
    - 5G-Equipment Identity Register (5G-EIR),
    - Network Data Analytics Function (NWDAF),
    - Charging Function (CHF),
    - Service Communication Proxy (SCP),
    - Security Edge Protection Proxy (SEPP),
    - Non-3GPP InterWorking Function (N3IWF),
    - Trusted Non-3GPP Gateway Function (TNGF),
    - Wireline Access Gateway Function (W-AGF); and
- Future 5G core functions as specified by 3GPP TS 23.501.

## ANNEX B: calculation of the 35% caps

The following methods are based on the NCSC's FAQs in relation to its January 28 2020 'advice on the use of equipment from High Risk Vendors (HRVs) in UK telecoms networks', as the FAQs stood on the date this Direction was published.

### Annex B.1: calculation of the 35% *site* cap for 5G access networks

Firstly, providers should classify their sites based upon type (e.g. small cells, macrocells). For example, the ITU has defined five basestation classes within ITU-T K.100. These classes (E0, E2, E10, E100, E+) determine where and how the equipment should be deployed.

Secondly, for each class, providers should determine the size of two sets:

$S_{[class]}$: the set of sites supported by the provider of a particular 'class' that are providing Rel-15 or later features or functionality to handsets/UEs. Note that this could include upgraded 4G sites.

$S_{[class]}$(Huawei) the subset of sites within '$S_{[class]}$' where a non-passive function of the basestation is provided with the involvement of Huawei equipment.

Based upon these sets, providers should ensure that, for every class, the following equation is true:[3]

$$\frac{\#S_{[class]}(Huawei)}{\#S_{[class]}} \leq 0.35$$

In other words, for each class, the percentage of Huawei-supported sites is at most 35%. Correspondingly, at most 35% of small cells and at most 35% of macro cell functions may be provided by Huawei equipment.

Only the sites operated by the provider should be included in this calculation. Consequently, RAN-sharing agreements do not impact this calculation.

For the avoidance of doubt, the cap applies to any site defined as a 5G Base Station. Hence if a site offers any 5G functionality, it is included in the cap. 'Dynamic Spectrum Sharing' across 4G and 5G is a 5G feature and hence sites with this capability are included in the cap. However, if it

[3] Where '#S' is used to denote the size of the set 'S'.

is capable of offering 5G functionality, but these features are disabled, it is not included in the cap.

**As an example**, if a provider has 20,000 macro cell sites (class E+) and has updated or upgraded 6,000 of them to support Rel-15 or later features ($\#S_{E+} = 6000$). If additionally, the provider has 2,000 small cells (class E10) and installed or upgraded 1,000 of them to Rel-15 or later features ($\#S_{E10} = 1000$). Then:

$$\#S_{E+}(Huawei) \leq 0.35 \cdot \#S_{E+} = 2100$$

And:

$$\#S_{E10}(Huawei) \leq 0.35 \cdot \#S_{E10} = 350$$

Hence, the provider may have up to 2100 Rel-15 or later macro cell sites with non-passive components from Huawei, and at most 350 Rel-15 or later small cell sites with non-passive components from Huawei.

Providers should also ensure that traffic quantities and equipment quantities are also within the cap, as described in Annex B.2 and Annex B.3

**Annex B.2: calculation of the 35% *traffic* cap for 5G access networks**

The traffic cap should be calculated based on the total traffic passing through '5G' base stations over a year. It is based on the traffic routed over the network from UEs within the following two sets:

U: The set of UEs where the provider's RAN is offering features or functionality defined in 3GPP Rel-15 or later.

U(Huawei): The subset of UEs within 'U' where some non-passive aspect of base station connectivity has the involvement of Huawei equipment. To be clear, where a UE is supported by multiple base stations, involvement of Huawei equipment in either function would cause the UE to be within the set. In the case of 5G Option 3A, this would apply if Huawei equipment is involved in either the eNB signalling anchor, or the gNB carrying 5G traffic.

Based on these sets, providers should ensure that the following equation is true:[4]

$$\frac{\sum_{year} |U(Huawei)|}{\sum_{year} |U|} \leq 0.35$$

This applies to traffic going over the provider's RAN regardless of the destination core network, or the customer relationship. Traffic from another provide's RAN is not included in the calculation, but MVNO or RAN-share traffic going over the provider's own RAN is included.

For the avoidance of doubt, the traffic quantities are only calculated for handsets offering any of the functionality added in the 3GPP's Release 15 or later, regardless of whether the handset uses that offered functionality. Hence, it will generally be calculated based on the amount of traffic going through the '5G sites' as identified in accordance with Annex B.1. However, if a UE is passing traffic through both 4G and 5G sites (e.g. 5G's Non-Stand Alone Option 3), that UE has been offered a 5G feature and all that UE's traffic should be included in the cap, regardless of whether the traffic is routed through a 4G or 5G base station.

As an example, if the provider routes 10PB of data over a year, from UEs which are being offered Rel-15 or later features by the network, then $\sum year|U|=10PB$. In this case:

[4] Using the notation that |U| is the traffic routed over the network from UEs within the set U, and $\sum year|U|$ is the traffic routed over the network throughout a year from UEs within the set U.

$$\sum_{year} |U(Huawei)| \leq 0.35. \sum_{year} |U| = 3.5PB$$

Consequently, over the course of that year, the provider may route up to 3.5PB from UEs offered Rel-15 or later functionality, where the support of a Huawei function is utilised.

Where the precise traffic quantities cannot be calculated, then the use of reasonable, unbiased estimates of traffic quantities over network elements are sufficient.

Providers should also ensure that site numbers and equipment quantities are also within the caps, as described in Annex B.1 and Annex B.3.

**Annex B.3: calculation of the 35% cap for network elements from a particular equipment class of 5G, FTTP and other gigabit or higher capable fixed access networks**

This cap is intended to apply to physical quantities of equipment. Providers should determine the size of two sets:

$E_{[class]}$: the set of the provider's physical equipment of a particular 'class' performing a function within the 5G access network or the FTTP and other gigabit or higher capable fixed access networks.

$E_{[class]}$(Huawei): the subset of physical equipment within 'E[class]' where a non-passive function of the equipment is provided with the involvement of Huawei equipment.

Based upon these values, providers should ensure that, for every class, the following equation is true:[5]

$$\frac{\#E_{[class]}(Huawei)}{\#E_{[class]}} \leq 0.35$$

Only the provider's equipment should be included in this calculation. Other providers' equipment should not be included, even if the provider uses this equipment to support part of their network.

Classes of equipment are deployment dependent, but as an example, the following may be appropriate equipment classes:

5G: gNB DU, gNB CU, gNB small cell, etc.

GPON: ONT/ONU, OLT ports

Providers of fixed networks should also ensure that premises passed are also within the cap as described in Annex B.4. Providers of 5G networks should also ensure that site numbers and traffic quantities are also within the caps, as described in Annex B.1 and Annex B.2.

Given the element of the Direction set out in 5(9) above, providers must not use Huawei equipment to provide NFVI and hence the 35% cap is not relevant to the physical infrastructure or hypervisor.

[5] Where '#E' is used to notate the size of the set 'E'.

The use of virtual Huawei functions should then be limited based on number of premises (for fixed access networks as described in Annex B.4), and number of sites and traffic quantities (for 5G networks as described in Annex B.1 and Annex B.2).

**Annex B.4: calculation of the 35% cap of premises passed by FTTP and other gigabit and higher capable access networks**

Providers should determine the size of two sets:

P: The premises passed by the provider using gigabit and higher capable access networks. Typically, each premise will have a unique customer termination point (e.g. ONTs) attached to the network.

P(Huawei): the subset of premises within 'P', where a non-passive function of the access connection (e.g. OLT port) is provided with the involvement of Huawei equipment.

Based on these sets, providers should ensure that the following equation is true:[6]

$$\frac{\#P(Huawei)}{\#P} \leq 0.35$$

As an example, if a provider provides a fibre service to 20m homes, presumably with the potential to support 20m active ONTs, then:

$$\#P(Huawei) \leq 0.35.\ \#P = 7m$$

Meaning that at most 7m homes may be served by Huawei equipment.

Providers should also ensure that equipment quantities are also within the cap as described in Annex B.3.

[6] Where '#P' is used to denote the size of the set 'P'.

## ANNEX C: Summary of requirements imposed on the Public Communications Provider

This table summarises the requirements imposed on the Public Communications Provider by this Direction. It is used for explanatory purposes only. It does not form part, nor is it intended to provide a comprehensive description, of the requirements imposed.

| Paragraph reference | Description of requirement | Date the requirement applies from |
|---|---|---|
| 5(1) | Not to make use of any Huawei equipment in 5G networks if such equipment was procured after 31 December 2020. | Date the Direction enters into force |
| 5(2) | Not to make use of any Huawei equipment in any network, except for fixed fibre access networks, if the manufacturing process or supply chain for such equipment has been altered as a result of changes to the United States Foreign-Produced Direct Product Rule announced on 19 May 2020 and 17 August 2020. | Date the Direction enters into force |
| 5(3) | Not to install any Huawei equipment in fixed fibre access networks if the manufacturing process or supply chain for such equipment has been altered as a result of changes to the United States Foreign-Produced Direct Product Rule announced on 19 May 2020 and 17 August 2020. | Date the Direction enters into force |
| 5(4) | Not to install Huawei equipment in 5G networks after the date the Direction enters into force, except: (a) where equipment has previously been installed in the network, or (b) installation is required for directly maintaining Huawei equipment installed before this date. | Date the Direction enters into force |
| 5(5) | Not to make use of Huawei Managed Services in respect of any network after the date the Direction enters into force, except for Huawei Specialist Maintenance Services provided in relation to Huawei equipment already installed in the network. | Date the Direction enters into force |
| 5(6) | Not to make use of Huawei equipment or services in parts of mobile access networks which could provide service to subscribers located at Sites Significant to National Security after 28 January 2023, but only where the Public Communications Provider has been provided with a list of such sites which affect it on or before the date of this Direction. | 28 January 2023 |
| 5(7) | 35% cap on use of Huawei equipment in 5G access networks after 31 July 2023. | 31 July 2023 |

| | | |
|---|---|---|
| 5(8) | 35% cap on use of Huawei equipment in FTTP networks, and other gigabit and higher capable access networks after 31 October2023 (with a 31 July 2023 reporting requirement). | 31 October 2023 |
| 5(9) | Not to make use of Huawei equipment or services in the execution of Core Network Functions after 31 December 2023 (with 28 January 2023 and 31 July 2023 reporting requirements). | 31 December 2023 |
| 5(10) | Not to make use of Huawei high data rate transmission equipment in any part of the networks after 31 December 2025. | 31 December 2025 |
| 5(11) | Not to make use of Huawei equipment or services in any part of its 5G network after 31 December 2027. | 31 December 2027 |
| 5(12) | Requirements regarding use of Huawei equipment and services not otherwise prohibited by the Direction. | Various |