

**Designation Notice under section 105Z8 of the Communications Act 2003, designating
Huawei for the purposes of a designated vendor direction**

Background

1. Section 105Z8(1) of the Communications Act 2003 (“**the Act**”) provides that the Secretary of State may issue a notice designating a person for the purposes of a designated vendor direction. A ‘designated vendor direction’ has the meaning given to it by section 105Z1(1) of the Act. Section 105Z8(2) of the Act provides that a designation notice may designate more than one person.

The Designation Notice

2. **The Secretary of State hereby designates each of Huawei Technologies (UK) Co., Ltd. and the list of its affiliated companies specified in the Annex to this Notice (together, “the Huawei corporate group” or “Huawei”) as a person for the purposes of a designated vendor direction.**
3. **In accordance with section 105Z8(3) of the Act, the Secretary of State issues this notice as she considers that this notice is necessary in the interests of national security.**

Reasons for the Notice

4. In accordance with section 105Z8(5) of the Act, the Secretary of State considers that this notice is necessary in the interests of national security for the following reasons.
 - a. 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.

- b. 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's 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.

- c. 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*".

- d. 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:
 - i. 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.

- ii. 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).
 - iii. 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.
- e. 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 4(a) to (d) 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.

- f. 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.

Signed

A handwritten signature in black ink, reading "Michelle Donohoe". The signature is written in a cursive style with a prominent flourish at the end of the last name.

Secretary of State for Digital, Culture, Media and Sport

12 October 2022

DRAFT Designation Notice under section 105Z8 of the Communications Act 2003,
designating Huawei for the purposes of a designated vendor direction

Annex

List of companies affiliated to Huawei Technologies (UK) Co., Ltd

COUNTRY	NAME OF HUAWEI AFFILIATE¹
ARGENTINA	Huawei Cloud Argentina
ARGENTINA	Huawei Tech Investment Co., Ltd.
AUSTRALIA	Huawei Technologies (Australia) Pty Ltd.
BAHRAIN	Huawei Technologies Bahrain
BELARUS	Bel Huawei Technologies LLC, including one alias:— BellHuawei Technologies LLC.
BELGIUM	Huawei Technologies Research & Development Belgium
BOLIVIA	Huawei Technologies (Bolivia) S.R.L.
BRAZIL	Huawei Cloud Brazil
BRAZIL	Huawei do Brasil Telecomunicações Ltda
BURMA	Huawei Technologies (Yangon) Co., Ltd.
CANADA	Huawei Technologies Canada Co., Ltd.
CHILE	Huawei Chile S.A.
CHILE	Huawei Cloud Chile
CHINA	Beijing Huawei Digital Technologies Co., Ltd.
CHINA	Chengdu Huawei High-Tech Investment Co., Ltd.
CHINA	Chengdu Huawei Technologies Co., Ltd.
CHINA	Dongguan Huawei Service Co., Ltd.

¹ Based on the United States Government's Entity List (Supplement No.4 to part 744) as it stood at 10 October 2022

CHINA	Dongguan Lvyuan Industry Investment Co., Ltd.
CHINA	Gui'an New District Huawei Investment Co., Ltd.
CHINA	Hangzhou Huawei Digital Technology Co., Ltd.
CHINA	HiSilicon Optoelectronics Co., Ltd.
CHINA	HiSilicon Technologies Co., Ltd. (HiSilicon)
CHINA	HiSilicon Tech (Suzhou) Co, Ltd.
CHINA	Huawei Cloud Computing Technology
CHINA	Huawei Cloud Beijing
CHINA	Huawei Cloud Dalian
CHINA	Huawei Cloud Guangzhou
CHINA	Huawei Cloud Guiyang
CHINA	Huawei Cloud Shanghai
CHINA	Huawei Cloud Shenzhen
CHINA	Huawei Device Co., Ltd. a.k.a., the following two aliases:— Huawei Device; and Songshan Lake Southern Factory
CHINA	Huawei Device (Dongguan) Co., Ltd.
CHINA	Huawei Device (Shenzhen) Co., Ltd.
CHINA	Huawei Machine Co., Ltd.
CHINA	Huawei OpenLab Suzhou, a.k.a., the following one alias:— Huawei Suzhou Openlab
CHINA	Huawei Software Technologies Co., Ltd.
CHINA	Huawei Technical Service Co., Ltd.
CHINA	Huawei Technologies Co., Ltd. a.k.a., the following two aliases:— Shenzhen Huawei Technologies; and Huawei Technology
CHINA	Beijing Huawei Longshine Information Technology Co., Ltd.

CHINA	Hangzhou New Longshine Information Technology Co., Ltd.
CHINA	Hangzhou Huawei Communication Technology Co., Ltd.
CHINA	Hangzhou Huawei Enterprises
CHINA	Huawei Digital Technologies (Suzhou) Co., Ltd.
CHINA	Huawei Marine Networks Co., Ltd.
CHINA	Huawei Mobile Technology Ltd.
CHINA	Huawei Tech. Investment Co.
CHINA	Huawei Technology Co., Ltd Chengdu Research Institute
CHINA	Huawei Technology Co., Ltd. Hangzhou Research Institute
CHINA	Huawei Technologies Co., Ltd. Beijing Research Institute
CHINA	Huawei Technologies Co., Ltd. Material Characterization Lab
CHINA	Huawei Technologies Co., Ltd. Xi'an Research Institute
CHINA	Huawei Terminal (Shenzhen) Co., Ltd.
CHINA	Nanchang Huawei Communication Technology
CHINA	Ningbo Huawei Computer & Net Co., Ltd.
CHINA	Shanghai Huawei Technologies Co., Ltd.
CHINA	Shenzhen Huawei Anjiexin Electricity Co., Ltd.
CHINA	Shenzhen Huawei New Technology Co., Ltd.
CHINA	Shenzhen Huawei Technology Service
CHINA	Shenzhen Huawei Technologies Software
CHINA	Zhejiang Huawei Communications Technology Co., Ltd.
CHINA	Huawei Technologies Service Co., Ltd.

CHINA	Huawei Training (Dongguan) Co., Ltd.
CHINA	Huayi Internet Information Service Co., Ltd.
CHINA	Hui Tong Business Ltd.
CHINA	North Huawei Communication Technology Co., Ltd.
CHINA	Shanghai Haisi Technology Co., Ltd.
CHINA	Shanghai HiSilicon Technologies Co., Ltd.
CHINA	Shanghai Mossel Trade Co., Ltd.
CHINA	Shenzhen HiSilicon Technologies Co.
CHINA	Shenzhen Huawei Technical Services Co., Ltd.
CHINA	Shenzhen Huawei Terminal Commercial Co., Ltd.
CHINA	Shenzhen Huawei Training School Co., Ltd.
CHINA	Shenzhen Huayi Loan Small Loan Co., Ltd.
CHINA	Shenzhen Legrit Technology Co., Ltd.
CHINA	Shenzhen Smartcom Business Co., Ltd.
CHINA	Suzhou Huawei Investment Co., Ltd.
CHINA	Wuhan Huawei Investment Co., Ltd.
CHINA	Wulanchabu Huawei Cloud Computing Technology, a.k.a., the following one alias:— Ulan Qab Huawei Cloud Computing Technology
CHINA	Xi'an Huawei Technologies Co., Ltd.
CHINA	Xi'an Ruixin Investment Co., Ltd.
COSTA RICA	Huawei Technologies Costa Rica SA, a.k.a., the following one alias:— Huawei Technologies Costa Rica Sociedad Anonima.
CUBA	Huawei Cuba
DENMARK	Huawei Denmark
EGYPT	Huawei OpenLab Cairo, a.k.a., the following one alias:— Huawei Cairo OpenLab.

EGYPT	Huawei Technology
FRANCE	Huawei Cloud France
FRANCE	Huawei France, a.k.a., the following one alias:— Huawei Technologies France SASU.
FRANCE	Huawei OpenLab Paris, a.k.a., the following one alias:— Huawei Paris OpenLab.
GERMANY	Huawei Cloud Berlin
GERMANY	Huawei OpenLab Munich, a.k.a., the following one alias:— Huawei Munich OpenLab.
GERMANY	Huawei Technologies Dusseldorf GmbH
GERMANY	Huawei Technologies Deutschland GmbH, Germany.
HONG KONG	Hua Ying Management Co. Limited
HONG KONG	Huawei Cloud Hong Kong
HONG KONG	Huawei Device (Hong Kong) Co., Limited
HONG KONG	Huawei International Co., Limited
HONG KONG	Huawei Tech. Investment Co., Limited
HONG KONG	Huawei Technologies Co. Ltd.
HONG KONG	Smartcom (Hong Kong) Co., Limited
INDIA	Huawei OpenLab Delhi, a.k.a., the following one alias:— Huawei Delhi OpenLab.
INDIA	Huawei Technologies India Private Limited, a.k.a., the following one alias:— Huawei Technologies India Pvt., Ltd.
INDONESIA	Huawei Tech Investment, PT.
ISRAEL	Toga Networks
ITALY	Huawei Italia
ITALY	Huawei Milan Research Institute
JAMAICA	Huawei Technologies Jamaica Company Limited
JAPAN	Huawei Technologies Japan K.K.

JORDAN	Huawei Technologies Investment Co. Ltd.
KAZAKHSTAN	Huawei Technologies LLC Kazakhstan
LEBANON	Huawei Technologies Lebanon
MADAGASCAR	Huawei Technologies Madagascar Sarl
MEXICO	Huawei Cloud Mexico
MEXICO	Huawei OpenLab Mexico City, a.k.a., the following one alias:— Huawei Mexico City OpenLab.
MEXICO	Huawei Technologies De Mexico S.A.
MOROCCO	Huawei Technologies Morocco
NETHERLANDS	Huawei Cloud Netherlands
NETHERLANDS	Huawei Technologies Coöperatief U.A.
NEW ZEALAND	Huawei Technologies (New Zealand) Company Limited.
OMAN	Huawei Tech Investment Oman LLC
PAKISTAN	Huawei Technologies Pakistan (Private) Limited
PANAMA	Huawei Technologies Cr Panama S.A.
PARAGUAY	Huawei Technologies Paraguay S.A.
PERU	Huawei Cloud Peru
PORTUGAL	Huawei Technology Portugal
QATAR	Huawei Tech Investment Limited
ROMANIA	Huawei Technologies Romania Co., Ltd.
RUSSIA	Huawei Cloud Russia
RUSSIA	Huawei OpenLab Moscow, a.k.a., the following one alias: —Huawei Moscow OpenLab.
RUSSIA	Huawei Russia.
SINGAPORE	Huawei Cloud Singapore
SINGAPORE	Huawei International Pte. Ltd.

SINGAPORE	Huawei OpenLab Singapore, a.k.a., the following one alias: —Huawei Singapore OpenLab.
SOUTH AFRICA	Huawei Cloud South Africa
SOUTH AFRICA	Huawei OpenLab Johannesburg, a.k.a., the following one alias: —Huawei Johannesburg OpenLab.
SOUTH AFRICA	Huawei Technologies South Africa Pty Ltd.
SRI LANKA	Huawei Technologies Lanka Company (Private) Limited
SWEDEN	Huawei Sweden
SWITZERLAND	Huawei Cloud Switzerland
SWITZERLAND	Huawei Technologies Switzerland AG
TAIWAN	Xunwei Technologies Co., Ltd.
THAILAND	Huawei Cloud Thailand
THAILAND	Huawei OpenLab Bangkok, a.k.a., the following one alias: —Huawei Bangkok OpenLab.
THAILAND	Huawei Technologies (Thailand) Co.
TURKEY	Huawei OpenLab Istanbul, a.k.a., the following one alias: —Huawei Istanbul OpenLab.
UNITED ARAB EMIRATES	Huawei OpenLab Dubai, a.k.a., the following one alias: —Huawei Dubai OpenLab.
UNITED KINGDOM	Huawei Global Finance (UK) Limited
UNITED KINGDOM	Huawei Technologies R&D UK, a.k.a., the following two aliases: —Huawei Research & Development (UK) Ltd; and —Huawei Technologies Research & Development (UK)).
UNITED KINGDOM	Huawei Technologies (UK) Co., Ltd., a.k.a., the following one alias: —Huawei Software Technologies Co. Ltd.
BRITISH VIRGIN ISLANDS	Proven Glory Capital Limited
BRITISH VIRGIN ISLANDS	Proven Honour Capital Limited

VIETNAM	Huawei Technologies (Vietnam) Company Limited
VIETNAM	Huawei Technology Co. Ltd.