National Cyber Security Centre
a part of GCHQ

28th January 2020

# NCSC ADVICE ON THE USE OF EQUIPMENT FROM HIGH RISK VENDORS IN UK TELECOMS NETWORKS

---

1. GCHQ's National Cyber Security Centre (NCSC) is the UK's technical authority on cyber security. We support the most critical organisations in the UK, the wider public sector, industry and SMEs as well as the general public. It is part of NCSC's role to highlight potential cyber security risks to the UK's national security and provide advice based on our technical expertise.

2. In that role, NCSC provided detailed security analysis to the Department for Digital, Culture, Media and Sport (DCMS) to underpin its Telecoms Supply Chain Review (SCR), the findings of which were published in July 2019. NCSC analysed the potential risk to the telecoms sector arising out of changes within the telecoms supply chain, the existing security practices employed by UK operators, and the residual risks to the UK. The Review established that effective management of the supply chain is fundamental to achieving a secure telecommunications sector.

3. One of the questions raised by the SCR was how to address the security challenges posed by vendors that pose a higher security risk to UK telecoms networks ("high risk vendors" or "HRVs"). Historically, the involvement of HRVs has been managed on an advisory basis by NCSC, through advice provided to operators. In particular, when operators have approached us about the use of HRVs, NCSC has advised them how best to mitigate the particular risks that they might present. We understand that it is the intention of the Government to seek further statutory powers, as soon as parliamentary time allows, on the basis of which it might require

telecoms operators to take certain steps to manage the security of their current and future networks.

4. However, the Government and NCSC recognise that the market is now at a crucial stage in new 5G and Fibre to the Premises (FTTP) rollout programmes and that industry urgently requires security advice now to support these programmes. The Government has therefore asked NCSC to consider publishing non-binding technical advice to operators in respect of their use of equipment from HRVs. If operators choose to implement this advice, it will enable them to make security choices that will help to protect the security of their own, and the UK's, telecoms networks. For completeness, this advice also covers networks other than 5G and FTTP.

**Background**

5. As the SCR recognised, the telecoms supply chain does not currently work in a way that incentivises good security. That has, to date, driven some poor industry practices. With 5G and FTTP rollouts now underway, network security is currently of paramount importance. Operators have the opportunity now to design and build their next-generation networks to contain attacks and prevent them from corrupting the network's most important functions.

6. We are looking to operators to adopt network security architecture and operational practices that reduce the levels of successful network penetrations and allow intrusions to be identified and managed quickly. This is a fundamental principle of good cyber security practice. It is a certainty that there will be cyber attacks on our telecommunications networks. It is also, in NCSC's view, a certainty that some of these attacks will be successful in compromising those networks.

7. As announced as part of the Telecoms Supply Chain Review, NCSC is preparing guidance on network security for telecoms networks, in the form of the Telecoms Security Requirements (TSRs). They will provide a framework for security in modern telecommunications networks. Proper application of the TSRs by operators will significantly reduce the likelihood of a successful attack and the harm caused when one happens. They will be designed to mitigate a range of national risks to a telecommunications network.

**High risk vendors**

8. The TSRs do not aim to fully mitigate the risks specific to nation state threat actors or high risk vendors. NCSC considers that the particular characteristics of some vendors can cause increased national risk. NCSC considers, therefore, that the market would be assisted by a clear statement of advice setting out how the presence of a particular vendor may increase security risks, what a high risk vendor is and how to manage the particular security risks presented by those vendors.

9. For many years, NCSC has helped operators to manage the use of vendors that pose a greater national security risk. As part of the SCR, NCSC has fed in a non-exhaustive list of criteria which NCSC applies when identifying vendors as HRVs. These non-exhaustive criteria are:

a. The vendor's strategic position/scale in the UK network;
b. The vendor's strategic position/scale in other telecoms networks, in particular if the vendor is new to the UK market;
c. The quality and transparency of the vendor's engineering practices and cyber security controls;
d. The past behaviour and practices of the vendor;
e. The vendor's resilience both in technical terms and in relation to the continuity of supply to UK operators;
f. A number of considerations relating to the ownership and operating location of the vendor, including:
    i. The influence which the domestic state apparatus can exert on the vendor (both formal and informal);
    ii. Whether the relevant domestic state and associated actors possess an offensive cyber capability that might be used to target UK interests;
    iii. Whether a significant component of its business operation is subject to domestic security laws which allow for external direction in a manner that conflicts with UK law.[1]

[1] Domestic state in this context is intended to mean the state where the vendor is headquartered and/or principally operates.

10. There is no exhaustive list of which vendors NCSC would consider HRVs under these criteria; we would encourage operators who are considering introducing new vendors into their networks to discuss that with us as soon as possible.

**Use of HRVs in UK telecoms networks**

11. In order to minimise the additional cyber security risk caused by HRVs, NCSC believe it is necessary and proportionate to limit their presence in networks. This has been NCSC's consistent advice to operators (when they have sought our guidance) and is most operators' existing common practice; that advice is now being formalised and published, as requested by Government. NCSC's advice is that use of HRVs without these restrictions would cause a cyber security risk that cannot be effectively mitigated. We therefore set out our advice as follows:

a. The cyber security risk of using HRVs in the network functions set out below cannot be managed. Therefore, if effective risk management of HRVs is to be undertaken, their products and services should not be used in the following network functions.
    i. For all networks: IP Core, Security Functions, Operational Support Systems (OSS)[2], 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 optimization, Interconnection equipment, Internet gateway functions, Lawful Intercept related functions.
    ii. For 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),

[2] Except to the extent necessary to support any network elements from that HRV deployed within an operator's network, in line with the details set out in this guidance.

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.

iii. For 4G networks: mobile core functions, including Home Subscriber Server (HSS), Packet Gateway (PGW), Policy and Charging Rules Function (PCRF) and, in some cases, the Mobility Management Entity (MME) and Serving Gateway (SGW).

b. Any use of an HRV in other 5G or FTTP network functions should be limited and we consider that a hard cap of 35% of a network equipment type allows for effective cyber security risk management. This cap properly balances two different security and resilience risks; the first being the risk associated with HRVs, the second being the need for a diversity of supply in the market. Specifically:

   i. For FTTP and other gigabit and higher capable access networks[3], at most 35% of premises passed by a network should be served by equipment from an HRV;

   ii. For 5G access networks, at most 35% of expected network traffic volume on any particular network passes through HRV equipment and at most 35% of base station sites nationally on any particular network should be served by equipment from an HRV;[4]

[3] For the purposes of this advice, this includes but is not limited to GPON (ITU G.984 and later), XGS-PON (ITU G9807.1 and later), DOCSIS3 and later, and other technologies that may support gigabit or higher customer connections.

[4] A 5G base station is any base station supporting or routing functionality added in 3GPP Rel-15 (or later releases).

iii. For any other functions in 5G, FTTP and other gigabit or higher capable fixed access networks, at most 35% of the network elements from a particular equipment class in any particular network should be provided by an HRV.

c. For 4G and legacy fixed access networks, NCSC's advice to operators remains unchanged. Two vendors should always be used in the access network. While no specific volume cap has been recommended, NCSC has always expected approximately 50/50 split between vendors in a given network.

d. Operators should never use more than one HRV in any given network; NCSC believes it is not possible to perform effective cybersecurity risk management where two HRVs are present in a network.

e. For access networks, operators should not use equipment from HRVs near certain sites that are significant to national security. In these areas, equipment from HRVs would cause an unmitigable security issue. NCSC has already provided advice to many affected operators, and any others who think their networks may be affected should consult NCSC for guidance via our enquiries team (enquiries@ncsc.gov.uk).

f. Equipment from HRVs should not be used in any manner in sensitive networks, for example those directly relating to the operation of government or any safety-related systems in wider critical national infrastructure[5].

g. Operators should only use an HRV if that HRV has in place a specific risk mitigation strategy, designed and overseen by NCSC. We do not believe that operators are able to manage the national risk the use of HRVs attracts without support from the national cybersecurity authority. It may not be possible to provide such a mitigation strategy in all cases.

[5] Government networks will still be able to operate over appropriate public telecoms networks as required, even those using a HRV, since they are independently secured and do not trust public networks.

12. There are a number of other network functions whose sensitivity is dependent on specific operator architecture and operation models. This sensitivity, and the required controls on HRVs, will need to be determined on a case by case basis. These functions include:

a. those that aggregate significant amounts of personal data such as Business Support Systems (BSS), location-based services, online charging solutions and managed services.
b. Voice systems
c. Logging and backup systems
d. Border network gateways (BNG/BRAS).

NCSC expects to issue further advice on these areas in due course, any operator concerned they may be using a HRV to perform one of these functions should contact the NCSC.

**Huawei**

13. Huawei has always been considered higher risk by the UK government and a risk mitigation strategy has been in place since they first began to supply into the UK. In terms of the HRV criteria set out above, the reasons NCSC continues to consider Huawei a HRV include at least that:

a. Huawei has a significant market share in the UK already, which gives it a strategic significance;
b. it is a Chinese company that could, under China's National Intelligence Law of 2017, be ordered to act in a way that is harmful to the UK;
c. we assess that the Chinese State (and associated actors) have carried out and will continue to carry out cyber attacks against the UK and our interests;
d. our experience has shown that Huawei's cybersecurity and engineering quality is low and its processes opaque. For example, the HCSEC Oversight Board raised significant concerns in 2018 about Huawei's engineering processes. Its 2019 report confirmed that "no material progress" had been made by Huawei in the remediation of technical issues reported in the 2018 report and highlighted "further significant technical issues" that had not previously been identified; and
e. A large number of Huawei entities are currently included on the US Entity List. Although we do not have knowledge as to whether these entities will remain on the US Entity List, this listing may have a potential impact on the future availability and reliability of Huawei's products.

14. The Government has agreed that Huawei should continue to be treated as a HRV and asked us to consider issuing this advice, in particular to help operators mitigate the risk of their use of Huawei in UK telecoms networks. For the avoidance of doubt, this advice does not replace or supplant the role of the Huawei Cyber Security Evaluation Centre, which will continue to be an essential part of the future strategy by which the risks presented by Huawei will be mitigated.

15. From a cyber security perspective, the NCSC advises operators whose Huawei estates currently exceed the recommended level for an HRV, to reduce to the recommended level as soon as practical. We understand that this takes time, but consider that it should be possible for all operators to reduce their use of HRVs to the recommended levels within 3 years.

**Other High Risk Vendors**

16. Huawei is the only HRV which currently has in place a bespoke risk mitigation strategy. An operator which is considering using any other vendor that appears likely, using the criteria outlined above, to fall within the definition of an HRV should contact NCSC for advice at an early stage in its discussions with such a vendor, and have regard to this and previous advice in relation to HRVs. Operators should certainly not assume that all HRVs are Chinese companies and should consider all the criteria above.

**Conclusion**

17. The DCMS SCR has demonstrated the need to change the way we manage security in the UK's telecommunications infrastructure. The TSRs will provide the framework for security in the next generation of the UK's telecommunications networks. The SCR also showed that we need to manage the presence of HRVs in the UK's telecommunications infrastructure more formally and actively. NCSC will continue to feed into any future legislative process and advise government on these matters.

18. This advice, issued by NCSC and supported by DCMS and wider government, formalises NCSC's existing advice and updates this in light of the fact that industry requires

urgent security advice to support the rollout of 5G and FTTP. It recommends to operators the most effective means by which they can reduce the risk to their networks and the UK's national security arising from the presence of HRVs within those networks. NCSC will periodically review and update this advice as necessary.