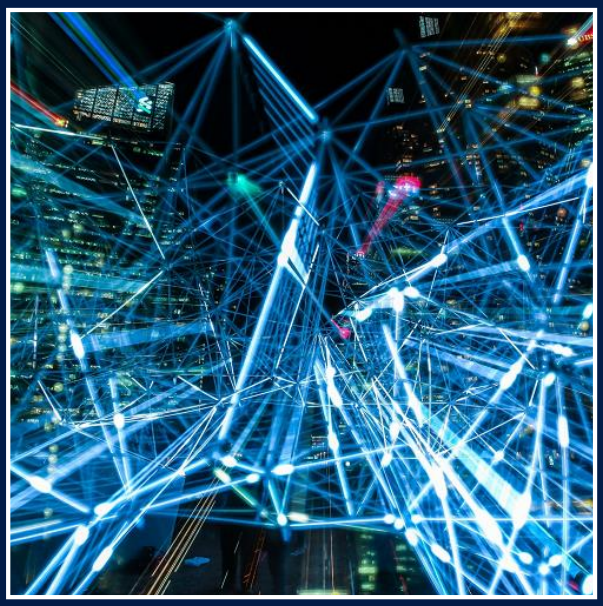
National Cyber Security Centre
a part of GCHQ

Summary of the NCSC's analysis of the May 2020 US sanction



Summary of the NCSC's analysis of the May 2020 US sanction which caused the NCSC to modify the scope of its security mitigation strategy for Huawei

1. Introduction

1. This document explains the NCSC's update to the Huawei security mitigation strategy and how that impacts the use of Huawei equipment in UK networks. This update was driven by the US Foreign-Produced Direct Product Rule Amendment (FDPRA) which significantly increased the extent of US trade sanctions against Huawei and has increased the risk to UK networks.

2. On the 28th January 2020, the NCSC published guidance for the risk management of High Risk Vendors (HRVs) in telecommunications networks[1]. The guidance advised that limits should be placed on the use of HRV equipment in UK networks. The NCSC also advised that equipment from HRVs should only be used when the HRV has in place a specific risk mitigation strategy, designed and overseen by the NCSC.

3. The only bespoke mitigation strategy that the NCSC has agreed to date is with Huawei. Huawei has always been considered higher risk by the UK government for the reasons set out in our HRV advice, and as such a risk mitigation strategy has been in place since Huawei first began to supply UK operators. Since 2010, a set of arrangements have existed between Huawei and Her Majesty's Government (HMG) to mitigate any perceived risks arising from the involvement of Huawei in parts of the UK's critical national infrastructure. A fundamental component of these arrangements is the existence and effective operation of the Huawei Cyber Security Evaluation Centre (HCSEC). HCSEC is a facility in Banbury, Oxfordshire, belonging to Huawei UK, directed by NCSC and overseen by an Oversight Board to ensure independence. HCSEC provides security evaluation for a range of Huawei products used in the UK's telecoms market.

4. This document provides a summary of the NCSC's analysis of the FDPRA, including our analysis of the sanction itself, its impact on Huawei, its impact on the UK's security mitigation strategy and the resulting impact on the security and resilience of UK networks. Based on these impacts, this document explains why an update to the scope of the NCSC's security mitigation strategy is necessary to continue to manage the risks associated with Huawei's presence in UK networks.

[1] https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks

2. Summary of US sanctions

2.1 The May 2019 Entity Listing

5. The US placed Huawei on the Entity List on 16th May 2019[2], a form of trade sanction which put limits on Huawei's access to US technology. A few days later, the US then granted a Temporary General License (TGL), including exemptions for certain types of network maintenance activity. US export control law seeks to control the movement of US technology not just when leaving the US, but also as it moves through global supply chains.

6. Placing Huawei on the Entity List restricted Huawei's access to US and non-US components containing controlled US technology. However, our understanding is that there were two factors that limited the impact of the Entity Listing on Huawei:

    a) Under US export control, there are *de minimis* thresholds such that only equipment containing more than (in most cases) 25% US products or technology is controlled. Huawei concluded that many of the components that they rely upon, and many of Huawei's products themselves, were not controlled.

    b) For those that were controlled, Huawei advised the NCSC and the operators that it had anticipated the US action, and had stockpiled the necessary components prior to being placed on the Entity List[3]. This allowed Huawei the necessary time to redesign products using alternative components reducing the impact on their supply. In many cases, Huawei replaced US components with components designed by Huawei itself (within its HiSilicon subsidiary). Huawei used standard processes for creating and building these designs, processes that we understand contain US and UK technology but that did not require any further transfer of that technology. As Huawei could design its own components it could create its own replacements for the US components that it could no longer access, minimising the impact on the wider product.

7. The above two aspects mitigated the impact of the May 2019 Entity Listing on the security and resilience of UK networks. Despite this, the Entity Listing did increase the risk to the security and resilience of UK networks due to the ongoing use of Huawei in the UK, and the NCSC considered the associated risks. For example:

    a) the NCSC and HCSEC would have to establish whether we could give assurance for Huawei's modified post-Entity List products, and

    b) the Entity Listing increased uncertainty, as it could be subject to changing interpretations, escalated or even removed without warning.

---

[2] https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list

[3] https://www.ft.com/content/0f063f50-5465-4f01-811f-0d0318d5162d

8. By December 2019, HCSEC had begun to analyse the modifications to Huawei products that were made in response to the Entity Listing. The NCSC's initial analysis was that these changes would be manageable for the NCSC to oversee alongside HCSEC. The NCSC took into account the impact of the Entity Listing in our analysis for the DCMS Telecoms Supply Chain Review[4], and remained of the view that despite the ongoing Entity Listing of Huawei, the risk could be mitigated for Huawei's access products. This was reflected in our High Risk Vendor (HRV) advice and Huawei mitigation strategy published in January 2020[5].

2.2 Explaining the May 2020 US Sanctions

9. On 15th May 2020, the US government updated the sanctions against Huawei by amending the Foreign-Produced Direct Product Rule (the FDPRA). This added two new restrictions, which by way of summary prevent (unless a US licence has been obtained):

    a) transfer to Huawei entities of any items produced or developed by Huawei and which are 'direct products' of controlled US technology or software, and

    b) transfer to Huawei entities of any items that are both produced by manufacturing equipment that is the 'direct product' of controlled US technology or software, and where Huawei has been involved in the design.[6]

10. The first appears to restrict the transfer within Huawei, including to HCSEC, of Huawei-produced items which are 'direct products' of controlled US technology or software. The second appears to restrict the transfer of Huawei-designed components that are 'direct products' of controlled US technology or software back to Huawei by Huawei's suppliers. The focus of the US in implementing the rule appears to be to target Huawei's semiconductor production, as the press statement accompanying the announcement of the rule make clear. [7] The rules came into force immediately, but certain transfers are permitted until mid September.

11. This was a significant shift by the US for the following reasons:

    a) The term 'direct product' is not clearly defined but the application of the rule is not limited according to the quantity of controlled US technology in a product. Hence non-US suppliers to Huawei that use any controlled US technology may be impacted. Given how pervasive US technology is across many sectors, it is likely that all of Huawei's suppliers will have to consider the impact of the new rules, regardless of their location in the world.

---

[4] https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference

[5] https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks

[6] The rules are complex and we have only sought to summarise them at a high level here. The full rules can be found here: https://www.federalregister.gov/documents/2020/05/19/2020-10856/export-administration-regulations-amendments-to-general-prohibition-three-foreign-produced-direct

[7] https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts

b) It targets the use of US technology in Huawei's supply chain, rather just within Huawei itself. In many ways this is a very broad sanction. Suppliers will need to decide whether to build US-independent manufacturing processes for Huawei, or to no longer supply them. Consequently, the action could have broad repercussions for the global IT industry. Global companies may decide to isolate themselves from future US sanctions and develop US-independent supply chains.

c) It impacts Huawei's existing designs. Huawei's suppliers can no longer build products for Huawei based on any of Huawei's existing designs that were created using tools containing US technology, even if these designs were created prior to May 2020[8]. This appears to particularly impact processors, such as HiSilicon's own processors which were designed using US and UK technology. Again, given the prevalence of US technology in the relevant tools needed for building semiconductors, it does not appear that a supplier could supply Huawei with a Huawei-designed semiconductor in compliance with US export control law.

d) As HCSEC is also caught by the Entity Listing as part of Huawei UK, a consequence of the sanction is that it may directly inhibit the transfer of both Huawei products and essential product information (such as designs, binaries, etc.) into HCSEC for analysis. Hence, as it stands today, the sanction prevents the functioning of the UK's security mitigation strategy with Huawei.

e) Finally, it demonstrates a further hardening of the US position towards Huawei, setting an even clearer intent. Should this US action be ineffective, in particular if Huawei were to find a workaround, it is likely that the US government would continue to modify its approach until it had successfully had its desired effect on the company.

12. At the same time as announcing the FDPRA, the US government also stated that they may not renew the Temporary General License. We have been informed that this doesn't have any material impact on Huawei's ability to maintain equipment within UK networks at present, but as yet we have been unable to independently verify this.

13. Based upon these factors, the NCSC's initial analysis suggested that the May 2020 FDPRA was significantly more damaging for Huawei than the May 2019 Entity Listing. It also significantly changed the risk to the UK, causing the NCSC to review our previous advice on Huawei from January 2020.

[8] Unless manufacture of the item started prior to 15 May 2020.

3. Impacts

14. It is too early to say with confidence when exactly this US action will disrupt Huawei's supply chain, although there are indications that it is already taking effect[9]. At this time, our estimate is that Huawei's supply will be impacted within the next 3-12 months. The exact timeframe will be largely based upon the quantity of processors and other complex, custom semiconductors that Huawei may have stockpiled, which is not known. However, Huawei has indicated to the NCSC and wider government that it would, exceptionally, ringfence sufficient equipment and spares from these existing stockpiles to satisfy the expected rollout needs for the next five years for two UK operators.

15. We are conscious that the FDPRA is complex and Huawei are still considering the impact on its business. We have set out below our current understanding of the impacts of the FDPRA, and given that understanding we cannot delay in providing updated advice to operators. The potential impacts of the FDPRA on Huawei's equipment, and our ability to assure it, are significant. In the absence of a revision to our January advice, operators are continuing to rely on the Huawei mitigation strategy of January 2020, which was defined prior to the recent US action and which we no longer consider appropriate to mitigate security risks. In particular, we are concerned that operators are making long-term network planning decisions without being aware that they may be unable to replace or upgrade Huawei equipment in the future while adhering to the UK's mitigation strategy. In addition, they could be making procurement decisions now that will bind them to purchasing Huawei equipment and services in the future that will be adversely affected by the FDPRA.

16. In respect of the US measures, we do not believe it likely that the US government will issue individual licences permitting the export of key products from specific manufacturers to Huawei and, given our current understanding of the impacts of the FDPRA, we need to proceed on this basis. We also take into account that the US has clearly signalled its intent such that it is highly likely that if this action fails to have the impact the US are expecting, they will modify their approach until the sanction is effective. That said, we are also conscious that the FDPRA is complex, and may not be in final form, and that Huawei itself is still considering the impact on its business. As we have done in respect of these recent US sanctions, we will continue to periodically review our advice, including where that is required by any change of circumstance or new information.

[9] https://www.mobileworldlive.com/devices/news-devices/huawei-mulls-chip-supply-options-as-us-sanctions-bite/

3.1 Supply

17. Our assessment is that it is highly likely that the FDPRA will disrupt Huawei's ability to supply operators. The NCSC wrote to the UK's major operators on this point in mid-June recommending a series of precautionary steps to limit the impact of this disruption on existing networks. Since then, Huawei has indicated that it has enough spares for existing networks stockpiled in the UK for the short-to-medium term.

18. Huawei's inability to supply operators would impact the UK's ambition for digital connectivity due to a reduction in the availability of equipment and the resilience of UK networks through the reduction of equipment diversity within networks. However, in relation to supply issues specifically, it does not directly impact the UK's mitigation strategy with Huawei.

3.2 Security

19. A critical impact of the US action is on the functioning of HCSEC. Our understanding is that Huawei will be unable to transfer affected equipment, or certain details of that equipment (such as designs, binaries etc.) to HCSEC for analysis while HCSEC remains part of a broader entity (Huawei UK) that is on the Entity List. Consequently, the US action prevents the effective operation of HCSEC. While this persists, the UK's security mitigation strategy for Huawei is not viable. The NCSC is actively working with Huawei to move HCSEC into a separate legal entity which will not be on the Entity List.

20. Assuming this is successful, and also that Huawei is able to maintain or resume some supply to UK operators, the NCSC have considered the broader implications of the FDPRA on the UK's security mitigation strategy for Huawei. There appear to us to be four primary possibilities:

    a) Huawei supply equipment in contravention of US export control, something that Huawei has said it would not do, and the UK government and industry would not accept.

    b) Huawei utilise generic third-party processors rather than existing, Huawei-designed processors.

    c) Huawei, or a third party, design and build equipment largely independent of US technology or tools.

    d) The US government remove or reduce the sanctions against Huawei, which does not appear to be likely.

21. While the first option has been ruled out by Huawei, should Huawei take this route it would likely lead to the US further escalating their sanctions, potentially placing a 'Denial Order' on Huawei (as they did against ZTE for different reasons). A Denial Order could even prevent Huawei from supporting existing equipment, which would have a significant resilience impact on both the UK's and worldwide networks. Should Huawei decide to continue to supply in contravention of

US export control, the risk of disruption to UK networks due to a lack of vendor support is sufficiently high that the UK should not continue to purchase Huawei equipment.

22. For the second option, Huawei will need to redesign their wider product to accommodate generic, third-party processors. While in some cases this will be straightforward, for key components and functionality this will be a major engineering task with performance implications. Under normal circumstances, hardware decisions are made at the beginning of the equipment's design and retrofitting new components into old designs is fraught with risk. Huawei's historical software engineering does not give us confidence in their ability to do this while maintaining product security and resilience. Even if they are successful, it is relatively straightforward for the US to modify its sanction to capture Huawei's use of generic processors and remove this option from Huawei (such as reducing the *de minimis* thresholds).

23. For the third option, designing and building equipment largely independent of US technology or tools within a couple of years presents a truly Herculean task. While we take processors and semiconductors for granted in our everyday lives, their creation is extremely complex and based on decades of research. Huawei or their partners will need to recreate one of the world's most advanced, precision and performance-driven technologies, including design tools and fabrication equipment, to create processors, software and equipment without the use of existing US technology or tools. Once Huawei has built these tools themselves, they will need to use those tools to create products before they can resupply their customers. Under normal circumstances, delivering such a complex, end-to-end process would be discussed in terms of decades, rather than months.

24. From the UK's perspective, should Huawei be successful in this endeavour:

    a) The equipment will have been built with unknown and untested tools, created under extreme time pressures. It is highly likely that the quality issues identified in successive HCSEC Oversight Board reports[10] will increase significantly, and these issues will be harder to remediate.

    b) The scope of HCSEC will need to increase significantly to scrutinise these new and untested tools. Given this, maintaining HCSEC's current capacity to evaluate new equipment does not seem feasible. As has been identified in successive Oversight Board reports, it also does not seem feasible for HCSEC to expand at sufficient scale given the market for security professionals remains highly competitive.

    c) Even with sufficient resource, it may not be feasible for HCSEC to gain confidence in Huawei's newly designed and developed tools and the resulting equipment that they create.

[10] https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019

To our knowledge, such tools and equipment do not exist today in any maturity, and hence are entirely unknown.

25. In summary, the security implications are significant. It will be extremely challenging to gain confidence in Huawei's post-sanction equipment, and it may be impossible. Assuming that continued operation of HCSEC is permitted under US export law, the number of products which HCSEC has the capacity to analyse will be significantly reduced.

3.3 Support and Maintenance

26. The current FDPRA does not impact the support and maintenance of existing equipment. However, given the direction of travel, we cannot rule out the possibility that future action by the US might limit Huawei's support for existing equipment. We also note that the US government suggested in May 2020 that the existing Temporary General Licence that permits maintenance activity may not be renewed in August (we understand that in any event Huawei and the operators believe they do not need to rely on the TGL for their activities).

27. UK operators rely on Huawei for two different types of support and maintenance activities:

    a) managed services which support the day-to-day operation of networks

    b) third-line support to fix sporadic faults in Huawei equipment.

28. Huawei managed services are used in a very small number of cases in the UK. The 2019 Entity Listing increased the risk of disruption to Huawei's provision of ongoing managed services. At the time, the NCSC advised the small number of affected operators of this risk so that they could take mitigating action.

29. Given the ongoing, and escalating, US measures, it is not sustainable for UK operators to continue to rely on Huawei for the day-to-day operation of networks. This is due to the likelihood that a future US sanction could inhibit this essential support at short notice, and in doing so disrupt network services. For this reason, the NCSC has reiterated our advice to operators that they should have a plan in place to change managed service providers at short notice, and reiterated that the formal exclusion of Huawei from managed services is required.

30. For third-line support, the NCSC is recommending to government that a capability is created within the UK to maintain existing Huawei equipment as part of a broader resilience strategy. This would reduce the impact on the UK should a future US sanction result in Huawei being unable to provide essential equipment fixes for a period of time.

4. Update to the Huawei mitigation strategy

31. For the reasons already set out above, the NCSC has significant concerns about the viability of being able to continue to use Huawei's post-FDPRA network equipment in UK networks. We consider that the advice we provided to operators in January is no longer appropriate in light of this unprecedented change. We are therefore updating our mitigation strategy for Huawei.

32. Given the situation outlined above, the risk is sufficiently high for the NCSC to recommend that Huawei's post-FDPRA equipment is not used in the UK at all. However, due to the diversity issues in the telecoms sector, that would have severe negative consequences for the security and resilience of the UK's networks. The NCSC has therefore had to balance these competing risks in providing advice.

33. There are currently three major suppliers to UK mobile access networks (Ericsson, Nokia and Huawei) and two major suppliers to the UK's fixed access networks (Nokia and Huawei[11]). Only having two suppliers into all national mobile networks reduces network resilience and security. Only having one supplier to national fibre access networks has a significant detrimental impact on the security and resilience of UK networks.

34. While there are negative security and resilience consequences to excluding Huawei's post-FDPRA equipment from 5G access networks, the security and resilience risks arising from deploying this equipment are now sufficiently high that the NCSC is recommending that operators should not use this equipment.

35. However, given there is only one alternative supplier of fibre access equipment in the market today, excluding Huawei from fixed networks will likely pose a greater resilience and security risk than their inclusion, at least until a second additional provider has established itself as a supplier to the UK. Subject to technical consultation with FTTP operators, NCSC will therefore continue to seek to mitigate the risk due to fibre access equipment that is sold into the UK for a short transitional period.

36. Consequently, the NCSC's security mitigation strategy for Huawei will only cover:

    a. existing equipment, including existing 5G equipment

    b. any remaining pre-FDPRA equipment[12], including pre-FDPRA 5G equipment

    c. fibre access equipment, subject to consultation with FTTP operators.

37. The NCSC's security mitigation strategy for Huawei will not cover the following equipment, which therefore cannot be used in the UK under the January 2020 HRV policy:

[11] Openreach recently announced that ADTRAN would be a third supplier into its FTTP networks. However, it will take time for this company to scale its supply within the UK.

[12] Equipment that has not been adapted by Huawei to ensure compliance with the FDPRA of May 2020.

a. post-FDPRA 5G access equipment[13]

b. post-FDPRA data transport equipment, such as optical transport and microwave

c. other miscellaneous post-FDPRA equipment not described above (such as power control, etc.).

38. For clarity, the updated mitigation strategy will continue to cover Huawei's pre-FDPRA 5G equipment that is deployed, or about to be deployed, in UK networks today. It will exclude Huawei's future 5G equipment that will be redesigned due to the FDPRA.

39. For post-FDPRA fibre access equipment, we are unable to guarantee that we will be able to mitigate the additional risks, but focusing HCSEC on this limited product set provides the best chance of success. Operators should be aware that we may be unable to gain sufficient assurance in these products to mitigate the risk of their deployment in UK networks, and if this happens, rollouts will be delayed.

40. In making this recommendation we recognise the interplay between national security and resilience. In almost any other circumstance we would recommend excluding Huawei from providing new equipment across both fixed and mobile access networks. Allowing Huawei to continue to supply the UK with fixed access equipment will leave the UK exposed to risk. However, we believe that the substantial negative impact to national resilience should we exclude Huawei from fixed access, due to the shift to a single vendor, outweighs the security and resilience risks of their inclusion at this time. This approach relies upon establishing other vendors within the market with the scale to meet the UK demand during a short transition period.

5. Full removal of Huawei equipment from networks

41. Given the increasing risk associated with Huawei, it is natural that some will argue that the UK should remove the latent risk by removing Huawei equipment entirely from all the UK's fixed and mobile networks. As part of its analysis, the NCSC considered this option in detail and concluded that this would present substantial resilience and security risks for the UK, and that these far outweighed the risk of retaining this equipment within UK networks.

42. The FDPRA has a range of impacts and potential impacts that are not just limited to Huawei equipment. There is an increase in uncertainty for the supply of telecommunications equipment in general. In this environment, it would be perilous for the security and resilience of networks to attempt to replace a significant proportion of the UK's national networks in a short period of time, assuming this were possible. Given the scale of change required, it would also render it almost impossible to improve our operators' security posture against broader cyber threats. As the NCSC has previously highlighted, these broader threats present the most significant risks to our networks today.

[13] Equipment that has been adapted by Huawei to ensure compliance with the FDPRA of May 2020.

National Cyber Security Centre
a part of GCHQ

Summary of the NCSC's analysis of the May 2020 US sanction