# HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD

## ANNUAL REPORT

## 2020

***A report to the National Security Adviser of the United Kingdom***

***September 2020***

## Foreword

The publication of this Oversight Board report has been delayed relative to previous years due to the COVID-19 pandemic and the ongoing significant analytic effort around the effects of US sanctions.

This annual report covers the period January 2019 to December 2019 and therefore does not cover the changes in government policy that happened in 2020. Those decisions and the underpinning technical analyses are detailed on the NCSC website and the Oversight Board has had no input into those decisions.

# HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD ANNUAL REPORT

## Part I: Summary

1. This is the sixth annual report from the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. HCSEC is a facility in Banbury, Oxfordshire, belonging to Huawei Technologies (UK) Co Ltd (Huawei UK), whose parent company, Huawei Technologies Co Ltd, is a Chinese headquartered company which is now one of the world's largest telecommunications providers.

2. HCSEC has been running for nine years. It opened in November 2010 under a set of arrangements between Huawei and Her Majesty's Government (HMG) to mitigate any perceived risks arising from the involvement of Huawei in parts of the United Kingdom's (UK) critical national infrastructure. HCSEC provides security evaluation for a range of products used in the UK telecommunications market. Through HCSEC, the UK Government is provided with insight into Huawei's UK strategies and product ranges. The UK's National Cyber Security Centre (NCSC, and previously Government Communications Headquarters (GCHQ)), as the national technical authority for information assurance and the lead Government operational agency on cyber security, leads for the Government in dealing with HCSEC and with Huawei more generally on technical security matters.

3. The HCSEC Oversight Board, established in 2014, is chaired by Ciaran Martin, the Chief Executive Officer of the NCSC, and an executive member of GCHQ's Board with responsibility for cyber security. The Oversight Board continues to include a senior executive from Huawei as Deputy Chair, as well as senior representatives from across Government and the UK telecommunications sector.

4. The Oversight Board has now completed its sixth full year of work. In doing so it has covered several areas of HCSEC's work over the course of the year. The full details of this work are set out in Part II of this report. In this summary, the main highlights are:

4.4 **The NCSC Technical Competence Review found that the capability of HCSEC has improved in 2019**, and the quality of staff has not diminished, meaning that technical work relevant to the overall mitigation strategy can be performed at scale and with high quality;

4.5 **The sixth independent audit of HCSEC's ability to operate independently of Huawei HQ has been completed.** Ernst & Young concluded that there were no major concerns and the Oversight Board is satisfied that HCSEC is operating in line with the 2010 arrangements between HMG and the company;

4.6 **Limited progress has been made by Huawei in the remediation of the issues reported last year,** making it inappropriate to change the level of assurance from last year or to make any comment on potential future levels of assurance.

5. The key conclusions from the Oversight Board's sixth year of work are:

5.4 In 2019, **HCSEC fulfilled its obligations** in respect of the provision of software engineering and cyber security assurance artefacts to the NCSC and the UK operators as part of the strategy to manage risks to UK national security from Huawei's involvement in the UK's critical networks;

**5.5** However, as highlighted in previous reports, **HCSEC's work has continued to identify concerning issues in Huawei's approach to software development** bringing significantly increased risk to UK operators, which requires ongoing management and mitigation. This is unchanged from last year;

**5.6** **Limited progress** has been made on the issues raised in the previous report;

**5.7** The Oversight Board continues to be able to provide **only limited assurance** that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK. However, this does not suggest that UK networks are more vulnerable than last year.

**5.8** The Oversight Board advises that **it will be difficult to appropriately risk-manage future products** in the context of UK deployments, until the underlying defects in Huawei’s software engineering and cyber security processes are remediated;

**5.9** At present, the Oversight Board has **not yet seen anything to give it confidence in Huawei’s capacity to successfully complete the elements of its transformation programme** that it has proposed as a means of addressing these underlying defects. The Board will require sustained evidence of better software engineering and cyber security quality verified by HCSEC and NCSC;

**5.10** Overall, the Oversight Board can **only provide limited assurance that all risks to UK national security from Huawei’s involvement in the UK’s critical networks can be sufficiently mitigated long-term.**

This page is intentionally left blank

## HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD 2020 ANNUAL REPORT

### Part II: Technical and Operational Report

*This is the sixth annual report of the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. The report may contain some references to wider Huawei corporate strategy and to non-UK interests. It is important to note that the Oversight Board has no direct locus in these matters and they are only included insofar as they could have a bearing on conclusions relating directly to the assurance of HCSEC's UK operations. The UK Government's interest in these non-UK arrangements extends only to ensuring that HCSEC has sufficient capacity to discharge its agreed obligations to the UK. Neither the UK Government, nor the Board as a whole, has any locus in this process otherwise.*

### Introduction

i. This is the sixth annual report from the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. HCSEC is a facility in Banbury, Oxfordshire, belonging to Huawei Technologies (UK) Co Ltd (Huawei UK), whose parent company is a Chinese headquartered company, Huawei Technologies Co Ltd, which is now one of the world's largest telecommunications providers.

ii. HCSEC has been running for nine years. It opened in November 2010 under a set of arrangements between Huawei and HMG to mitigate any perceived risks arising from the involvement of Huawei in parts of the UK's critical national infrastructure. HCSEC provides security evaluation for a range of products used in the UK market. Through HCSEC, the UK Government is provided with insight into Huawei's UK strategies and product ranges. The UK's National Cyber Security Centre (NCSC, and previously GCHQ), as the national technical authority for information assurance and the lead Government operational agency on cyber security, leads for the Government in dealing with HCSEC and with Huawei more generally on technical security matters.

iii. The HCSEC Oversight Board, established in 2014, is chaired by Ciaran Martin, the Chief Executive Officer of the NCSC, and an executive member of GCHQ's Board with responsibility for cyber security. The Oversight Board continues to include a senior executive from Huawei as Deputy Chair, as well as senior representatives from across Government and the UK telecommunications sector. The structure and membership of the Oversight Board has not changed significantly.

iv. This sixth annual report has been agreed unanimously by the Oversight Board's members. As with last year's report, the Board has agreed that there is no need for a confidential annex, so the content in this report represents the full analysis and assessment.

v. The report is set out as follows:

2 Section I sets out the Oversight Board terms of reference and membership;
3 Section II describes HCSEC staffing, skills, recruitment and accommodation;
4 Section III covers HCSEC's effectiveness;
5 Section IV summarises the findings of the 2019 independent audit;
6 Section V brings together some conclusions.

## SECTION I: The HCSEC Oversight Board: Terms of Reference and membership

a. The HCSEC Oversight Board was established in early 2014. It meets quarterly under the chairmanship of Ciaran Martin, the Chief Executive of the NCSC and an executive member of GCHQ's Board at Director General level. Mr Martin reports directly to GCHQ's Director, Jeremy Fleming, and is responsible for the agency's work on cyber security.

b. The role of the Oversight Board is to oversee and ensure the independence, competence and overall effectiveness of HCSEC as part of the overall mitigation strategy in place to manage the risks presented by Huawei's presence in the UK and to advise the National Security Adviser on that basis. The National Security Adviser will then provide assurance to Ministers, Parliament and ultimately the general public as to whether the risks are being well managed.

c. The Oversight Board's scope relates only to products that are relevant to UK national security risk. Its remit is twofold and covers:

   - first, HCSEC's assessment of Huawei's products that are deployed or are contracted to be deployed in the UK and are relevant to UK national security risk which is determined at the NCSC's sole and absolute discretion; and
   - second, the independence, competence and therefore overall effectiveness of HCSEC in relation to the discharge of its duties.

d. The Board has an agreed Terms of Reference, a copy of which is attached at **Appendix A***.* There have been no changes to the terms of reference this year and the remit and objectives of the Oversight Board remain unchanged. The Oversight Board is responsible for providing an annual report to the National Security Adviser, who will provide copies to the National Security Council and the Intelligence and Security Committee of Parliament (ISC).

### The Board's objectives for HCSEC

e. The Oversight Board's four high-level objectives for HCSEC remained consistent with those reported previously and are:

- To provide security evaluation coverage over a range of UK customer deployments as defined in an annual HCSEC evaluation programme;
- To continue to provide assurance to the UK Government by ensuring openness, transparency and responsiveness to Government and UK customer security concerns;
- To demonstrate an increase in technical capability, either through improved quality of evaluations output or by development of bespoke security related tools, techniques or processes;
- For HCSEC to support Huawei Research and Development to continue to develop and enhance Huawei's software engineering and cyber security competence.

### The HCSEC Oversight Board: Business April 2019-March 2020

f. This report covers the technical work undertaken from January 2019 until December 2019. The Oversight Board meeting in March 2019 was covered in the previous report. In its four meetings since the publication of the 2019 Annual Report, the Oversight Board has:

1. Provided regular corporate updates on Huawei UK;
2. Discussed future technology trends and how they may affect the work of the Oversight Board;
3. Been supplied with regular updates on HCSEC recruitment and staffing;
4. Taken further evidence around the root causes of the significant software engineering and cyber security issues that came to light last year;
5. Taken further evidence on Huawei's proposed remediation for the significant software engineering and cyber security issues, and judged them to be inadequate;
6. Commissioned a sixth HCSEC management audit of the independence of the Centre.
7. Overseeing the impact on HCSEC of the U.S. Entity Listing of Huawei in May 2019.

~~~~~
~~~~~

## SECTION II: HCSEC Staffing

2.1 This section provides an account of HCSEC's staffing and skills, including recruitment and retention.

### Staffing and skills

2.2The NCSC leads for HMG in dealing with HCSEC and the company more generally on technical security matters. The NCSC, on behalf of HMG, sponsors the security clearances of HCSEC's staff. The general requirement is that all staff must have Developed Vetting (DV) security clearance, which is the same level required in Government to have frequent, uncontrolled access to classified information and is mandatory for members of the intelligence services. New recruits to HCSEC are managed under escort during probation pending completion of their DV clearance period, which is typically six months.

2.3 Quarterly monitoring by the Oversight Board has shown no cause for concern in the number of staff and their skills. Staffing at HCSEC has seen 6 resignations over the course of the year, with manning levels reduced to, at the lowest point, 34. The final headcount for end of year is 39, against a budget of 40+2 (the +2 to allow flexibility for increased BEP work). However, productivity gains achieved over the previous period allowed HCSEC to maintain the evaluation programme while taking on unplanned additional workload - analysing binary equivalence and software engineering and cyber security quality at the request of NCSC.

2.4 It remains critical that HCSEC continues to recruit technical cyber security specialists to manage attrition and succession. HCSEC and NCSC acknowledge that with demand outstripping supply of appropriately skilled candidates in the general commercial security environment, HCSEC are very likely to see hiring challenges in 2020.

- There were no failures in the DV process this year.

### Accommodation

HCSEC are now established in their new accommodation. This facility is proving its worth, allowing HCSEC to perform simultaneous security testing against operational, representative networks from multiple UK operators. The new facility has seen an increase in productivity and HCSEC has maintained evaluations whilst carrying out the unplanned additional work described above.

~~~~~
~~~~~

## Section III: HCSEC’s Effectiveness

2019 is the sixteenth year of the Government’s active management of Huawei’s presence in the UK’s telecommunications networks, the ninth year of the Government’s extended risk management programme for Huawei in the UK and the sixth year of the Oversight Board. The Board’s role is to oversee and ensure the independence, competence, and overall effectiveness of HCSEC.

To this end, this section comprises NCSC’s report to the Oversight Board on the effectiveness of HCSEC. It is split into three parts:

1. The first provides an evaluation of the *functional* effectiveness of HCSEC; HCSEC’s technical capability to effectively analyse Huawei’s products. It concludes that HCSEC remains competent in the areas of technical security necessary to fulfil its function.
2. The second evaluates the *strategic* effectiveness of HCSEC; as a function of the UK’s mitigation strategy, based on the evidence provided by HCSEC’s analysis. This provides information on the software engineering and cyber security quality of Huawei products relevant to UK’s national security risk. It maintains the conclusions from the previous report. Specifically, that due to on-going serious and systematic defects in Huawei’s software engineering and cyber security competence, NCSC continues to advise the Oversight Board that it can only provide limited technical assurance in the security risk management of Huawei equipment in UK networks.
3. The third part provides the *technical evidence* for this conclusion, updating the supporting technical information provided in the previous report.

The section covers Oversight Board activities between March 2019 and February 2020 but reports on HCSEC’s work between January 2019 and December 2019.

## Section III(a): HCSEC's Functional Effectiveness

Significant technical work has been done in 2019 by HCSEC and also by NCSC, which has undertaken the audit for the Oversight Board envisaged by paragraph 3.3 of the Terms of Reference. The following subsections detail the outcome of that audit.

### HCSEC Programme Build and Prioritisation

The programme build process remains broadly the same as in previous years. The UK operators, NCSC and HCSEC set priorities for HCSEC collaboratively to achieve the best overall benefit for the UK. To support this process, a risk-based prioritisation scheme (detailed in previous Oversight Board reports) has continued to be applied during 2019, and the relative priority of equipment has remained consistent.

Huawei's broad involvement in the UK telecoms sector means there is a significant pipeline of work for HCSEC to manage. At present, HCSEC manages that pipeline well, consistently meeting the expectations of both the NCSC and the UK operators.

The final programme is signed off by the NCSC Technical Director or NCSC Technical Director for Telecommunications on behalf of the Oversight Board and kept under review during the year by HCSEC. Where HCSEC believes modifications to the programme are necessary, a light-touch process involving the NCSC and the relevant operators is used to manage and approve any modifications.

### HCSEC Evaluation Processes

3.1 HCSEC's assessment programme in 2019 comprised three types of evaluation:

1. Solution Evaluation; an in-depth security analysis of UK operator deployments featuring a range of Huawei products.
2. Product Evaluation; security analysis of a Huawei product in isolation.
3. Ad-hoc Assessment Reports; reports, as tasked by the Oversight Board or NCSC, to assess the effectiveness of Huawei's issue remediation and the overall software engineering and cyber security quality of Huawei products deployed in the UK.

In 2019, the scope of HCSEC's evaluations covered products and architectures for five major UK operators. Four solution evaluations were completed covering early 5G RAN releases, a fixed access network and a 4G core network.

HCSEC also completed 42 Product Evaluations. HCSEC continues to meet the NCSC's stated objective that HCSEC will perform a product evaluation on every relevant product in the UK at least every two years.

In addition, HCSEC produced 8 comprehensive assessment reports to analyse the effectiveness of Huawei's remediation of issues (issues described in this report and previous years' reports). These include two software quality reports, four reports into a specific security issue and five reports into binary equivalence.

Overall, this is broadly as per the programme agreed at the start of the year, with the following changes:

1. A number of the assessment reports were requested during the year and hence these were not scheduled into the evaluation plan. HCSEC successfully produced these reports without any major impact on the evaluation plan.
2. The evaluation plan was modified to align with changes in the operators' deployment timescales.

### HCSEC Analysis

HCSEC continues to have world-class security analysts in the complex sphere of telecommunications. This year, they have continued to provide unique insights into Huawei products. providing the UK telecoms community with a detailed understanding of the software engineering and cyber security risks associated with Huawei equipment.

One of the greatest challenges for HCSEC is the scale and complexity of Huawei's products. HCSEC's security analysts would not be able to effectively analyse Huawei equipment without the support of tools to scan the totality of the equipment. Consequently, HCSEC has maintained an on-going programme to develop its toolsets, increasing its technical effectiveness year-on-year. In 2019, HCSEC has further enhanced its toolsets, and it is clear that these tools have helped to increase both the depth of analysis and HCSEC's productivity.

### HCSEC Reporting

The HCSEC evaluation process continues to identify and report both point vulnerabilities and strategic architectural and process issues (as described in Section III(b)).

On discovering an issue in Huawei equipment, HCSEC assesses the impact of the issue. In 2019, HCSEC optimised the existing process for vulnerability reporting to reduce the time spent on low-impact issues which are of little significance to the UK. This new approach will be fully implemented in 2020.

Since 2012, once an issue has been identified and assessed, HCSEC simultaneously reports the results of its work to:

1. NCSC, to assess the national risk.
2. The impacted operators, who are expected to feed this information into their corporate risk management processes.
3. Huawei HQ (including R&D) for remediation

In rare circumstances, where the impact of the vulnerability is of national significance, the release of full details of the vulnerability to Huawei may be delayed to allow the UK community to assess and mitigate the impact. This occurred during 2019.

Through 2019, HCSEC has continued to demonstrate its expertise in finding weaknesses in the Huawei product set. This year, the number of vulnerabilities and issues reported to UK operators has risen significantly beyond the number found in 2018.

The NCSC attributes this growth to HCSEC's increasing effectiveness and the analysis of some specific, poorly written components. NCSC does not view the increase in vulnerabilities as an indicator of a further decline in Huawei's product quality, but it certainly does not indicate any marked improvement or transformation.

The character of vulnerabilities has not changed significantly between years, with many vulnerabilities being of high impact (equivalently, a high base CVSS score and a relevant operational context), including unprotected stack overflows in publicly accessible protocols, protocol robustness errors leading to denial of service, logic errors, cryptographic weaknesses, default credentials and many other basic vulnerability types.

Furthermore, 2019 has seen HCSEC expend significant effort on providing an independent view on Huawei's remediations against a range of issues, at the request of the Oversight Board and NCSC. This takes technical skill and insight, and remains a time-consuming and challenging process due to the complexity of Huawei's equipment.

### Entity Listing

The U.S. Government placed Huawei onto the Entity List in May 2019, later exempting some transactions under a Temporary General Licence, but also adding Huawei UK to the Entity List. This has had two impacts on the functioning of HCSEC:

1. As HCSEC remains part of Huawei UK, HCSEC as an organisation is also on the Entity List as a consequence of the U.S. action. The 2019 listing of HCSEC has had a material impact on its operation, but so far this impact has been manageable. Specifically, in some cases the listing has impeded or delayed the procurement or transfer of security evaluation tools and equipment. However, the U.S. Entity Listing did not impact HCSEC's evaluation schedule during 2019. A more sustainable solution will be necessary going forward.
2. Huawei has advised that it has already started to modify products to adhere to the US controls, replacing US centric components with components designed by other parties. Towards the end of 2019, HCSEC began to analyse these modified products. Initial indications are that HCSEC will need to increase its effort and capability dedicated to analysing hardware to be able to provide equivalent confidence in this new generation of products. The necessary effort required may limit the number of products that can be analysed by HCSEC, and hence the number of products that can be used within the UK.

### Conclusion

The NCSC believes that HCSEC remains competent in the areas of technical security necessary to advise the operators, NCSC and the Oversight Board as to the product and solution risks admitted by the use of Huawei products in the UK telecoms infrastructure. The NCSC's report to the Oversight Board is that HCSEC continues to provide unique, world-class cyber security expertise to assist the Government's ongoing risk management programme around the use of Huawei equipment with the UK operators.

## Section III(b): HCSEC's Strategic Effectiveness

HCSEC is a core component of the UK's mitigation strategy to manage any perceived risks arising from the involvement of Huawei in parts of the United Kingdom's (UK) critical national infrastructure. To enable the Board to provide clear and comprehensive assurance to the National Security Adviser, in the previous five reports, the Oversight Board has provided details of HCSEC's output that impact the UK's mitigation strategy and hence HCSEC's strategic effectiveness. This covers information on the software engineering and cyber security quality of Huawei products relevant to the UK's national security risk.

### Overview of High-Level Findings

3.7 Details are provided in the third part of this section, but the high-level conclusions and findings are provided here

**Product version management**

Huawei continues to maintain multiple product versions for the same product, and continues to provide large patches which modify a significant proportion of the product. Correspondingly, it continues to be necessary for HCSEC to analyse a different codebase for each operator, despite them using the same product. In 2019, HCSEC was required to analyse five different versions of Huawei's 5G basestation across the UK's four operators. Huawei claim that these are from a global product line, but we have no evidence to support this, meaning that HCSEC cannot derive any benefit from international analysis of Huawei products.

**Configuration management**

For specific products used in the UK, Huawei have simplified and made significant improvements to the build process, although issues remain. While a positive outcome, we do not yet have evidence that this is a holistic shift in Huawei's approach, rather than a point-fix for these products. Correspondingly, we do not yet have confidence that this improvement will be sustained.

**Binary equivalence**

HCSEC has now verified binary equivalence across eight product builds. This provides confidence that the specific products deployed in UK networks have been inspected by HCSEC. Huawei have committed to delivery of binary equivalence across officially released versions of all carrier products sold into UK from Dec 2020. Unfortunately, binary equivalence remains a bespoke project, rather than a consistent output of Huawei's build process, as has been recommended by NCSC. Consequently, the NCSC does not have confidence that binary equivalence will be sustainable.

### Product Quality

Major quality deficiencies still exist in the products analysed by HCSEC. Sustained evidence of poor coding practices was found, including evidence that Huawei continues to fail to follow its own internal secure coding guidelines. This is despite some minor improvements over previous years. Huawei has made improvements against certain metrics, and most point-issues identified in previous quality reports have been remediated.

During 2019, HCSEC identified critical, user-facing vulnerabilities in fixed access products. The vulnerabilities were caused by particularly poor code quality in user-facing protocol handlers and the use of an old operating system. The vulnerabilities were a serious example of the issues that are more likely to occur given the deficiencies in Huawei's engineering practices, and during 2019 UK operators needed to take extraordinary action to mitigate the risk. Huawei have since fixed the specific vulnerabilities in the UK, but in doing so, introduced an additional major issue into the product, adding further evidence that deficiencies in Huawei's engineering processes remain today.

In this example, the code quality in these user-facing protocol handlers was sufficiently poor that NCSC has required Huawei to fully rewrite the code, and rearchitect the product's security. Huawei have committed to doing so by June 2020.

### Component management

The major component management issues identified in previous reports remain. Huawei continues to include a wide range of old and duplicate components in products deployed in the UK, and fails to properly manage these components.

As discussed at length in previous reports, Huawei continues to use an old and now out of mainstream support version of a well-known and widely used real time operating system supplied by a third party. During 2019, Huawei have created a remediation plan and have proactively worked with UK operators to move products onto an internally maintained operating system (Huawei RTOS, based on an externally maintained Linux distribution) or to replace the boards. Of the very large number of boards impacted in the UK, 17% had been updated or replaced by December 2019 in line with the remediation plan agreed between Huawei and the operators. Hence despite efforts by both Huawei and UK operators, there remains a significant number of boards containing critical out-of-mainstream support components in UK networks, and Huawei's access to support for this component is likely inhibited by the US Entity Listing. This leaves the UK exposed to risk.

The causes of the on-going risk are as follows:

1. Huawei had inadequate component management and did not align end-of-life dates of components with the end-of-life date of products. Furthermore, Huawei did not identify the issue themselves.
2. Once identified by NCSC, Huawei did not remediate the issue promptly. It took 18 months for network remediation to begin.
3. Remediation of nationally distributed access networks, including product replacement where necessary, takes time and is resource intensive.
4. The issue has been compounded by Huawei being placed on the U.S. Entity List.

The success of the remediation programme is dependent on Huawei actively maintaining Huawei's replacement operating system (Huawei RTOS). NCSC investigated Huawei's plans to manage and maintain Huawei RTOS during 2019 and found that the plans for RTOS were not practically sustainable.

During 2019, further component management issues were identified with Huawei's use of open source components and its vertical integration of components. Some improvements were made by Huawei to rationalise components and reduce the number of duplicated components, demonstrating the company is fixing specific point-issues when directed to do so.

NCSC continues to have no confidence that Huawei will effectively maintain components within its products. It is likely that further issues will occur in the future which will require remediation and potentially product replacement, as is on-going today.

## Transformation

In 2018, Huawei presented to the Oversight Board its intent to transform its software engineering process through the investment of $2 billion over 5 years (completing in 2023). The NCSC reported last year that it has no evidence that this is more than a proposed initial budget for as yet unspecified activities. This year, HCSEC has evaluated individual products, which show some limited improvements in certain metrics. However, the set of significant vulnerabilities in a product that had gone through the transformation programme means that we still cannot have any confidence that these represent a systematic change in Huawei's approach. The Board will require sustained evidence of better software engineering and cyber security quality verified by HCSEC and NCSC.

As set out in last year's report, formal oversight of Huawei's global transformation plan does not fall within the scope of Oversight Board activities. However, it is important that the Board see details of the transformation plan and evidence of its impact on products being used in UK networks before it can be confident it will drive the change needed to address the risks identified. Unless and until a detailed and satisfactory plan has been provided, it is not possible to offer any degree of confidence that the identified problems can be addressed by Huawei.

## Conclusion

NCSC continues to believe that the UK mitigation strategy, which includes HCSEC performing technical work and the Oversight Board providing assurance as two components, is the best way to manage the risk of Huawei's involvement in the UK telecommunications sector. The discovery of the issues in this report are an indication of the model working properly. Huawei continues to engage with this process.

The work of HCSEC summarised above continues to reveal serious and systematic defects in Huawei’s software engineering and cyber security competence. While there have been limited improvements in 2019, the significant deficiencies and associated risks detailed in the 2018 report remain. There is not yet evidence that Huawei is undergoing a significant transformation to sustainably fix these deficiencies.

For this reason, NCSC continues to advise the Oversight Board that it is only appropriate to provide limited technical assurance in the security risk management possible for equipment currently deployed in the UK, since the NCSC has not seen evidence that Huawei software engineering and cyber security will sustainably improve. Even this limited assurance is possible only on the basis that, thanks largely to the work of HCSEC, the defects in Huawei equipment are fairly well understood in the UK. Given that knowledge, in extremis, the NCSC could direct Huawei on remediation for equipment currently in the UK, as happened in one case this year. This should not be taken to minimise the difficulty in doing so or to suggest that this would be a sustainable approach. In some cases, remediation will also require hardware replacement (due to CPU and memory constraints) which may or may not be part of natural operator asset management and upgrade cycles.

Given both the shortfalls in good software engineering and cyber security practice, the lack of visibility of the trajectory of Huawei’s R&D processes through their announced transformation plan, and the product modifications being made as a result of the U.S. Entity Listing, it is highly likely that security risk management for new products will be more difficult.

Poor software engineering and cyber security processes lead to security and quality issues, including vulnerabilities. The increasing number and severity of vulnerabilities discovered, along with architectural and build issues, by the relatively small team in HCSEC is a particular concern. If an attacker has knowledge of these vulnerabilities and sufficient access to exploit them, they may be able to affect the operation of a UK network, in some cases causing it to cease operating correctly. Other impacts could include being able to access user traffic or reconfiguration of the network elements. However, the architectural controls in place in most UK operators limit the ability of attackers to engender communication with any network elements not explicitly exposed to the public which, with other measures in place, makes exploitation of vulnerabilities harder. To the best of NCSC's knowledge, this set of vulnerabilities has not been exploited in the UK. These architectural controls and the operational and security management of the networks by the UK operators will remain critically important in the coming years to manage the residual risks caused by the engineering defects identified. These findings are about basic engineering competence and cyber security hygiene that give rise to vulnerabilities that are capable of being exploited by a range of actors. NCSC does not believe that the defects identified are a result of Chinese state interference.

## Section III(c): Supporting Technical Evidence

This section updates the technical detail laid out in the previous reports and, where necessary, elaborates further in order to explain the conclusions the Oversight Board has reached on technical assurance and HCSEC effectiveness, as well as its views on how the risks identified can be mitigated in the future. In particular, the Oversight Board considers that provision of this technical detail is necessary to explain and substantiate its decision to maintain the level of assurance identified last year and also to help those operators not currently represented on the Oversight Board to understand the risks they may face in their networks.

While Huawei has demonstrated some minor improvements in 2019, the serious and systematic defects in Huawei's software engineering and cyber security competence identified in the previous Oversight Board report remain. Details are provided in Table 1. Fundamentally, the NCSC has no confidence that Huawei has begun on a path to effectively remediate these issues.

The UK's mitigation strategy for the use of Huawei equipment in the UK telecommunication sector, of which HCSEC and the Oversight Board is one part, expects industry good practice software engineering and cyber security development and support processes as a basis. The evidence in Table 1 demonstrates that Huawei currently does not meet that basic expectation. Consequently, the NCSC has advised the Oversight Board that it can continue to provide only limited assurance in the security of the currently deployed equipment in the UK.

### Table 1: Technical detail of issues relating to Huawei's software engineering and cyber security development.

| Issue | Description of issue | 2018 Status (as reported in previous reports and associated context) | 2019 Status |
|---|---|---|---|
| Single Build<br>(Single product trunk with minimal branching) | Proper maintenance of products requires keeping the number of parallel versions of a product (branches) to a minimum. This prevents product maintenance becoming unmanageable. This is common practice for all forms of software development.<br>NCSC expects Huawei to release the same product version to all UK operators so that only a single version need be evaluated by HCSEC. | There remain concerns among the UK operator community about the consistency of similarly versioned software as delivered by Huawei. Noted that Huawei's practice of testing and modifying products based on the operator's configurations while this improves reliability in the intended configuration, it may mask serious issues and increase complexity. | Huawei have stated compliance for some products, but this has not been evidenced.<br>In 2019, five different 5G basestation versions were deployed across the UK's four operators. Huawei claim that these are from a single product line, but the patches against this product line are extremely large. This multiplies |

| | | | |
|---|---|---|---|
| | NCSC expects this same version used in the UK to be widely used internationally. | | the effort required within HCSEC and the complexity of providing any assurance.<br>Huawei claim that these are from a global product line, but we have no evidence to support this, meaning that HCSEC cannot derive any benefit from international analysis of Huawei products. |
| Configuration management of development systems | NCSC expects the development process to be traceable, allowing the cause of issues to be identified. In particular, both code and coders should be traceably linked to binaries. | Acknowledged improvements in Huawei's configuration management has been delivered since the issue was first identified in 2010.<br>However, in 2016 HCSEC identified a range of configuration management defects in Huawei's build processes, including evidence of poor configuration management of virtual machines, build environments and source code. These were observed again by HCSEC in 2018.<br>Concluded that in NCSC's view, Huawei cannot deliver end-to-end integrity in its products, that NCSC has limited confidence in Huawei's understanding of its products or ability to perform root-cause analysis. | Huawei's build processes have been simplified and significantly improved for specific products, but some issues remain.<br>While a positive outcome, we do not have evidence that this is a holistic shift in Huawei's approach, rather than a point-fix. Nor do we yet have confidence that this is a sustainable change. |
| Binary equivalence (BE/BEP) | NCSC expects source code provided by Huawei into HCSEC to be easily linked to Huawei's products deployed in UK, and for any differences to be easily explained.<br>NCSC expects this to be via automated build infrastructure and a simple, single build. | HCSEC first attempted to demonstrate binary equivalence in 2011, but this was not possible as the delivery team in Huawei HQ had been extracting a subset of source code for features procured by the UK operators from the configuration managed repositories for onward delivery to HCSEC. In Dec 2016, Huawei committed to providing full code and build | HCSEC has verified that it can check Binary Equivalence across 8 product builds. Huawei have committed to delivery of binary equivalence across officially released versions of all carrier products sold into UK from Dec 2020. |

| | | | |
|---|---|---|---|
| | | environments and delivering BE across all products.<br>Full code for UK products appears to have been provided since 2017.<br>Binary equivalence verified for one product. Recommended that Huawei re-engineer its build processes to deliver binary equivalence routinely as part of the standard product release cycle, rather than delivering binary equivalence through a bespoke project for the UK. | Binary equivalence remains a bespoke project, rather than a consistent output of Huawei's build process. |
| Product quality | NCSC repeatedly raised a range of quality issues with Huawei between 2011 and 2018. These issues have been acknowledged by Huawei. These issues make security issues in Huawei products more likely, exposing the UK to risk. | In Huawei's 2013 Cyber Security Perspective white paper, published independently by Huawei, Huawei stated:<br>*"…the IPD process shows how cyber security is being built into everyone's daily operations; in this way security becomes everyone's job and something that is done naturally."*<br>Since then, evidence has repeatedly suggested that security policies and specifications in the IPD process have not been implemented consistently across product lines.<br>For example, unsafe functions should not be used by developers, but use of unsafe functions was noted in the 2016 Oversight Board report. The 2018 Oversight Board report highlighted | In 2019, HCSEC again analyzed the quality of the LTE eNodeB product, and the MA5800. This identified that welcome improvements had been made across certain metrics, and point-issues identified in previous reports have been fixed.<br>However, a range of issues were once again found including poor coding practices, including a range of evidence that Huawei is not following its own internal secure coding guidelines, and unsustainable use of third-party components.<br>Hence, the NCSC is yet to see evidence of a significant shift in Huawei's approach to product quality, and we have no confidence that the improvements are sustainable. NCSC has now |

| | | | |
|---|---|---|---|
| | | that unsafe functions were still used extensively, including redefining safe functions to unsafe ones.<br>In 2018, HCSEC analyzed the quality of two versions of the LTE eNodeB. As described in last year's OB report, while this identified some improvements, it also identified an extensive range of defects.<br>Consequently, NCSC's view was that Huawei's own internal secure coding guidelines are not routinely followed and, in some cases, developers may be actively working to hide bad coding practice rather than fix it. The NCSC concluded that there remain significant issues to be addressed in Huawei's software engineering and cyber security development. | seen evidence of significant issues in Huawei's product quality over a number of years. |
| Fixed Access issue | During 2019, HCSEC identified critical, user-facing vulnerabilities in fixed access products. The vulnerabilities were caused by particularly poor code quality in user-facing protocol handlers. NCSC required Huawei to patch the issue, rewrite the impacted protocol handlers, | N/A | Issue patched within agreed timeframe. However, as part of the remediation of the issue, a command line command was added to disable defense-in-depth checks, showing a complete lack of security awareness.<br>Huawei failed to fully rewrite protocol handlers as required, although a significant amount of |

| | | | |
|---|---|---|---|
| | and rearchitect the product's security to fully fix the issue. | | code was updated. No timeframe yet agreed for a full rewrite.<br>Huawei have committed to re-architecting product by June 2020. |
| Remediation of critical out-of-mainstream support component. | Huawei use an old version of a third-party real time operating system in products. This component goes out-of-mainstream support during 2020.<br>Using old and out-of-mainstream-support components within a product leaves those products more vulnerable to exploitation. As an example, the fixed access issue detailed above was more significant due to the use of a near out-of-mainstream support real time operating system which did not have modern security defenses. | In 2018 the oversight board and UK operators made it clear that long-term reliance on this operating system in the UK is unacceptable and an upgrade path must be created.<br>In the 2018 OB report, the NCSC had not seen a credible plan for the mitigation of the issue, nor a suitable upgrade path. | During 2019, Huawei have created a remediation plan and have proactively worked with UK operators to move products onto an internally maintained operating system (Huawei RTOS) or to replace the boards.<br>Of the very large number boards impacted in the UK, only 17% have been updated or replaced in line with the plan agreed between Huawei and the operators. Hence despite efforts by both Huawei and UK operators, there remains a significant number of boards containing critical out-of-mainstream support components in UK networks, and Huawei's access to support for this component is likely inhibited by the US Entity listing. This leaves the UK exposed to risk. |
| Component & Lifecycle management | To ensure that products are secure and reliable, it is important that modern internal and third-party components are used within the product and that these components supported throughout the lifetime of the product. This reduces the likelihood and impact of equipment compromise. | In Huawei's 2013 'Cyber Security Perspectives' whitepaper, Huawei stated:<br>*"(Huawei's) use of a centralised repository allows us to manage the lifecycle of the third-party and open source code. This is extremely important … especially in the event that the third-party or open source component is declared end-of-life by the original developer."* | As part of the 2019 quality report, HCSEC noted limited improvements in component management but major issues remained. Huawei frequently 'in-house' and modify open source code. As some changes were not well-recorded or recommitted to the open source project, this raised serious concerns about the sustainability of these components.<br>HCSEC also observed that based on the open source license, Huawei are required to publish their modifications back to the community. |

| | | | |
|---|---|---|---|
| | | However, as described above, Huawei's failings in its management of internal and 3rd-party components have resulted in some old and out-of-mainstream-support components remaining in the products used in the UK.<br>The 2018 report identified that the component management issues were broader than the operating system, with similar issues appearing for a number of other components investigated by NCSC. Consequently, the NCSC reported to the Oversight Board that Huawei's engineering processes do not correctly manage component usage or lifecycle management, leaving products unsupportable in general.<br>The NCSC also raised concerns about Huawei's ability to maintain its own internal Real-Time Operating System (Huawei RTOS). | Huawei inform us that the user community can request Huawei's modified open source software as per the GPL.<br>During 2019, some improvements were made by Huawei to rationalize components and reduce the number of duplicated and old components, NCSC observed that Huawei continue to vertically-integrate components (e.g. operating system and application) which inhibits component-level patching. NCSC also investigated Huawei's plans to maintain RTOS and found that the plans, at that time, were unsustainable.<br>Consequently, NCSC continues to have no confidence that Huawei will effectively maintain components within its products. It is likely that further issues will occur in the future which will require remediation and potentially product replacement, as is on-going today. |
| Vulnerability management | Products should be built to enable the fast resolution of vulnerabilities. Specifically, components should be linked to products and not duplicated to ensure that any vulnerability in a component can be quickly remediated in all impacted products. | The 2018 report noted that it is difficult to be confident that vulnerabilities discovered in one build are remediated in another build through Huawei's engineering processes. Such an outcome should be delivered through any modern software engineering process. | Vulnerabilities discovered in 2019 were generally remediated effectively. However, there was one example in 2019 where Huawei added a function to disable all defense-in-depth protections as part of remediating a set of vulnerabilities. We believe this was introduced as a consequence of Huawei's poor remediation processes. Due to issues with Huawei's component management, we have no |

| | | | |
|---|---|---|---|
| | | | confidence or evidence that these vulnerabilities will have been sustainably and universally remediated. |
| Transformation | In 2018, the Oversight Board requested a plan to improve the LTE eNodeB product. NCSC made clear that without such a plan, there could be no long-term confidence in Huawei's technology or Huawei's ability to support operators in its secure use long-term.<br>Huawei accepted the criticism and in response, Huawei made a public $2bn commitment over 5 years to transform their processes and rectify their security issues.<br>Formal oversight of Huawei's transformation falls outside the remit of the Oversight Board, but the Board will wish to see sufficient details of Huawei's transformation to enable it to assess whether the identified risks have been mitigated. | Given the scale of the issues described above, the 2018 report stated that significant and sustained evidence of impact on products being delivered into the UK would be required before the board would reassess its level of assurance. | It remains early days, with the five year programme only in its second year, but despite point-fixes, the evidence that the NCSC has shows no sign of genuine transformation:<br>1. The NCSC has not seen a credible transformation plan, nor a reasonable allocation of the committed $2bn investment in transformation.<br>2. During 2019, the 5G product set showed limited improvement over 4G, but no evidence of transformation.<br>3. Given that significant issues were identified during the rewrite of the protocol stacks, Huawei's transformation has not so far ensured that basic issues would be caught.<br>4. The NCSC has no confidence that this is a global transformation, rather than a set of point-actions intended to remediate quality issues in UK products. |

## SECTION IV: The work of the Board: Assurance of independence

4.1 This section focuses on the more general work of the Oversight Board beyond its oversight of the technical assurance provided by HCSEC. For the sixth year running, the Board commissioned and considered an audit of HSCEC's required operational independence from Huawei HQ. This remains the most effective way, in the Board's view, of gaining assurance that the arrangements were working in the way they were designed to work in support of UK national security. The principal question for examination by the audit was whether HCSEC had the required operational independence from Huawei HQ to fulfil its obligations under the set of arrangements reached between the UK Government and the company in 2010. The independent audit does not seek to comment on the quality of any technical work – from either HCSEC or Huawei HQ – and detailed technical findings are not relevant to the independence of operation of HCSEC. This section provides an account of the process by which the audit took place, and a summary of the key findings.

### Appointing Ernst & Young as auditors

a. Ernst & Young LLP (E&Y) were appointed to carry out the first HCSEC audit in 2014, following a rigorous process during which GCHQ invited three audit houses to consider undertaking the management audit and sought their recommendation as to the appropriate audit standard and process to be followed. E&Y undertook the second audit in 2015 and in 2016, at the NCSC's instigation, they were retained to provide audit services for the subsequent three years and this service was extended for 2019. E&Y's Annual Management Audit was conducted in accordance with the International Standard on Assurance Engagements (ISAE) 3000.

b. The Oversight Board agreed a three-stage approach to the audit, which broadly followed that of previous years:

- An initial phase to assess the Control Environment and Design Scope was completed by November 2019;

- A second phase to run a ~~p~~reliminary review of the design and operation of the controls in place to support the independent operation of HCSEC. This phase was completed during November 2109
- A final audit phase comprising the full year end audit during December 2019, with the report presented in March 2020.

### The nature and scope of the audit

4.4 The audit assessed the adequacy and the operation of processes and controls designed to enable the staff and management of HCSEC to operate independently of undue influence from elsewhere in Huawei. The principal areas in scope were: Finance and Budgeting; HR; Procurement; Evaluation Programme Planning; Cooperation and Support from elsewhere in Huawei; and Evaluation Reporting. For all the review areas listed, E&Y took into account that the operation of HCSEC must be conducted within the annual budget agreed between Huawei and HCSEC.

4.5 The Oversight Board agreed some exclusions to the scope of the audit. Specifically, they agreed that the audit would not:

a. Opine as to the appropriateness of the overall governance model adopted to support the testing of Huawei products being deployed in the UK Critical National Infrastructure;
b. Assess the technical capability of HCSEC, the competency of individual staff or the quality of the performance of technical testing;
c. Assess physical access to HCSEC or logical access to its IT infrastructure. Nor would it look at the resilience of the infrastructure in place or at Disaster Recovery or Business Continuity planning.

### Headline audit findings

4.6 The HCSEC Annual Management Audit March 2020 comprised a rigorous evidence-based review of HCSEC processes and procedures. The audit report was produced by a team of DV cleared staff from Ernst & Young; the fieldwork was conducted and led by a Senior Manager. A Partner with Internal Audit subject matter knowledge acted as quality reviewer, and a second review of the final report was performed by an Ernst & Young Senior Partner.

a. In summary, Ernst & Young concluded in all material respects:
   1. The Subject Matter fairly presents that the controls were designed and implemented throughout the period 1 January 2019 to 31 December 2019
   2. The controls related to the control objectives stated in the Subject Matter were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period 1 January 2019 to 31 December 2019
   3. The controls tested were those necessary to provide reasonable assurance that the control objectives stated in the Subject Matter were achieved and operated effectively throughout the period 1 January 2019 to 31 December 2019.

**Results of Testing**

b. In summary, the area of deviations identified, and the agreed response, relate to the following area:

   1. **RFIs returned outside SLA period**
      Requests for information made to Huawei were not always returned inside the stated SLA period. This was reported as an advisory recommendation in the previous audit report but has continued into this year. It was recommended in 2019 report that HCSEC RFIs should be updated to include a ‘required by’ date and any breach of delivery should be escalated.

      Five hardware requests (out of 30) and three software (out of 27) requests were delivered outside the SLA period (defined in the Oversight Board Terms of Reference). Review of HCSEC internal monthly status reports did not identify any escalation or concerns regarding these delays – with one exception. One of the software requests above resulted in a delay to the scheduled review. This delay was escalated by the HCSEC requestor to HCSEC MD for resolution. Following escalation, the required information was provided to HCSEC.

2. **Huawei personnel outside of HCSEC do not have access to reports before they are issued to NCSC and UK operators.**
   In three instances reports were released to Huawei before formally disclosed to the NCSC or UK operations. Each of the issues detailed in the reports were rated 'low' impact by HCSEC. Changes in the issue management system now prevents a Huawei report being generated unless an NCSC/UK Operator report has already been created with simultaneous release to Huawei.

3. **Record of probation**
   One user was incorrectly classified on the HR system as no longer on probation when they were still waiting for confirmation of their NCSC Security Clearance. The audit validated that this individual did not have permission to release evaluated reports.

### Advisory Notices

There were no advisory notices in this year's report.

### Prior year issues and current status

4.14 **Appendix B** provides a summary of the issues and observations from the previous year's report, published in 2019.

### Overall Oversight Board conclusions of the audit

4.15 Taking the audit report in its totality, the HCSEC Oversight Board has concluded that the report provides important, external reassurance from a globally respected company that the arrangements for HCSEC's operational independence from Huawei Headquarters are operating robustly and effectively, and in a manner consistent with the 2010 arrangements between the Government and the company. Three observations have been identified. Given the scope of the audit, this is entirely consistent with the wider findings in this report.

~~~~~
~~~~~

## SECTION V: Conclusions

6.5 The Oversight Board has now completed its work during this period. Its four meetings and its work out of Committee have provided a useful enhancement of the governance arrangements for HCSEC.

6.6 The Oversight Board has concluded that in the year 2019, **HCSEC fulfilled its obligations** in respect of the provision of software engineering and cyber security assurance artefacts to the NCSC and the UK operators as part of the strategy to manage risks to UK national security from Huawei's involvement in the UK's critical networks.

6.7 However, as reported in 2018, HCSEC's work continues to identify **significant, concerning issues** in Huawei's approach to software development bringing significantly increased risk to UK operators, which requires ongoing management and mitigation. Operators will need to take into account the mitigations required as a result of the extensive vulnerability and software engineering and cyber security quality information provided by the work of HCSEC.

6.8 Limited progress has been made on certain issues raised in the 2018 report and further issues have been identified in this year's report. **The Oversight Board continues to be able to provide only limited assurance** that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK. The Oversight Board notes in particular the following advice from NCSC:

**a.** That there remains no end-to-end integrity of the products as delivered by Huawei and limited confidence on Huawei's ability to understand the content of any given build and its ability to perform true root cause analysis of identified issues. This raises significant concerns about vulnerability management in the long-term;

**b.** That Huawei's software component management is defective, leading to higher vulnerability rates and significant risk of unsupportable software;

c. The general software engineering and cyber security quality of the product continues to demonstrate a significant number of major defects. While we have seen some improvements in the basic metrics for some product versions, it continues to be fixes for point-issues identified in previous reports.

6.9 The Oversight Board advises that it will be difficult to appropriately risk manage future products in the context of UK deployments, until Huawei's software engineering and cyber security processes are remediated. As noted in last year's report, **the Oversight Board currently has not seen anything to give it confidence in Huawei's ability to bring about change via its transformation programme** and will require sustained evidence of better software engineering and cyber security quality verified by HCSEC and NCSC.

6.10 Huawei's transformation plan could in principle be successful, bringing Huawei's software engineering and cyber security processes up to current industry good practice. Huawei's own public estimates are that this transformation will take three to five years. The Oversight Board would require NCSC assessment of evidence of sustained change across multiple versions of multiple products in order to have confidence in success.

6.11 The evidence of sustained change is especially important as similar strongly worded commitments from Huawei in the past have not brought about any discernible improvements. The Oversight Board note in particular the commitments first made in Huawei's 2012 cyber security whitepaper (accessible at https://www-file.huawei.com/-/media/corporate/pdf/cyber-security/cyber-security-white-paper-2012-en.pdf) and repeated subsequently. Therefore, significant and sustained evidence will be required to give the Oversight Board any confidence that Huawei's transformation programme will bring about the required change.

6.12 It should be made clear that the Oversight Board's statement of limited assurance is not a comment on the security of the UK's networks today, which is a matter for individual operators, Ofcom, DCMS and NCSC. It is assurance as to whether HCSEC can continue to provide security relevant artefacts to inform UK stakeholders as part of the mitigation strategy. The oversight provided for in our mitigation strategy for Huawei's presence in the UK is arguably the toughest and most rigorous in the world. This report does not, therefore, suggest that the UK networks are more vulnerable than last year. Indeed, the significant technical insight provided by HCSEC to the UK operators allows them to plan more effective mitigations. The report from the Oversight Board states only that Huawei's development and support processes are not currently conducive to long-term security risk management and, at present, the Oversight Board has seen limited evidence to give confidence in Huawei's capacity to fix this.

6.13 The modifications Huawei are making to their products as a consequence of the U.S. Entity Listing of May 2019 are likely to significantly increase the analysis effort required within HCSEC. This may limit the range of products that can be analysed by HCSEC and hence used within the UK.

6.14 The OB's oversight and the work undertaken by HCSEC is an important strand of mitigating the ongoing risk of Huawei, in accordance with NCSC's advice. That mitigation strategy takes into account the work undertaken by HCSEC and ensures that risks are adequately managed.

6.15 Finally, it should also be noted that the Oversight Board wishes to emphasise that it has no remit to direct or influence the purchasing decisions of the UK operators. They must individually manage the risk in their own networks, with support from Ofcom, DCMS and NCSC.

6.16 The Oversight Board hopes that this report continues to add to Parliamentary – and through it, public – knowledge of the operation of the arrangements and the transparency with which they are operated.

~~~~~
~~~~~

## Appendix A: Terms of Reference for the Huawei Cyber Security Evaluation Centre Oversight Board

- **Purpose**

This Oversight Board will be established to implement recommendation two of the National Security Adviser's Review of the Huawei Cyber Security Evaluation Centre (HCSEC). The Oversight Board's primary purpose will be to oversee and ensure the independence, competence and therefore overall effectiveness of HCSEC and it will advise the National Security Adviser on this basis. It will work by consensus. However, if there is a disagreement relating to matters covered by the Oversight Board, GCHQ, as chair, will have the right to make the final decision.

The Board is responsible for assessing HCSEC's performance relating to UK product deployments. It should not get involved in the day-to-day operations of HCSEC.

- **Scope of Work**

### 2.1 In Scope

The Oversight Board will focus on:

4 HCSEC's assessment of Huawei products that are deployed or are contracted to be deployed in the UK and are relevant to UK national security risk.

5 The independence, competence and therefore overall effectiveness of HCSEC in relation to the discharge of its duties.

### 2.2 Out of Scope

4 All products that are not relevant to UK national risk;

5 All products, work or resources for non UK-based deployment, including those deployed outside the UK by any global CSPs which are based in the UK;

6 The commercial relationship between Huawei and CSPs; and

7 HCSEC's foundational research (tools, techniques etc.) which will be assessed

and directed by GCHQ.

- **Objectives of the Oversight Board**

### 3.1 Annual Objectives and Report to the National Security Adviser

To provide a report on the independence, competence and effectiveness of HCSEC to the National Security Adviser on an annual basis, explicitly detailing to what extent HCSEC has met its in-year objectives as set by the Board. This will draw upon the Annual Management Audit, the Technical Competence Review and will specifically assess the current status and the long-term strategy for resourcing HCSEC.

All UK CSPs that have contracted to use HCSEC for assurance in the context of management of UK national risk for deployments shall be consulted.

In the event of a change to the operation of HCSEC, or the emergence of any other factor that affects HCSEC's security posture, HCSEC will report this to the Oversight Board in a timely manner. GCHQ [or any other member of the Oversight Board] shall also be expected to inform the Oversight Board of any factor which appears to affect the security posture of HCSEC.

### 3.2 Commission Annual Management Audit

To assure the continued independence of HCSEC from Huawei HQ, the Oversight Board will commission a management audit to be performed by security cleared UK auditors; this will be funded by UK Government. The scope of the audit shall be as set out in the Huawei HQ Letter of Authorisation (Operational Independence) to HCSEC (as set out in Annex 3), or other agreed standards, as agreed by the Oversight Board. This will include the independence of budget execution and whether HCSEC were provided with the timely information, products and code to undertake their work.

The Oversight Board will ensure the scope of any such audit is appropriate and the auditor shall be agreed by the Chair and Deputy Chair.

The audit report mentioned in section 3.2 and 3.3 shall be treated as confidential information and subject to section 9.

### 3.3 Commission Technical Competence Review

To provide assurance that the functions performed by HCSEC are appropriate in terms of the wider risk management strategy as defined by GCHQ and the CSPs. The Oversight Board will commission GCHQ to undertake an audit of the technical competence of the HCSEC staff, the appropriateness and completeness of the processes undertaken by HCSEC and the strategic effects of the quality and security of Huawei products relevant to UK national security risks. GCHQ as part of the annual planning process will advise HCSEC of any enhancements in technical capability they wish to see developed by them within the year.

### 3.4 Process to Appoint Senior Management Team

The Oversight Board will agree the process by which GCHQ will lead and direct the appointment of senior members of staff of HCSEC. However, the Oversight Board will not be directly involved but will receive updates on any developments from GCHQ.

### 3.5 Timely Delivery

The Oversight Board will agree the formalisation of the existing arrangements for code, products and information to be provided by Huawei HQ to HCSEC to ensure that the completion of evaluations are not unnecessarily delayed.

### 3.6 Escalation / Arbitrator for issues impacting HCSEC

Board members should inform the Oversight Board in a timely manner in the event that an issue arises that could impact the independence, effectiveness, resourcing or the security posture of HCSEC. Under these circumstances the Board may convene an extraordinary meeting.

- **Oversight Board Membership**

The Board will initially consist of the following members. Membership will be reviewed annually. The National Security Advisor will appoint the Chair of the Board. Membership with then be via invitation from the Chair.

I. GCHQ – Chair (Ciaran Martin, CEO NCSC)
II. Huawei HQ – Deputy Chair (Ryan Ding, Executive Director of the Board)
III. Huawei UK Managing Director
IV. Huawei UK Communications Director
V. HCSEC Managing Director
VI. Cabinet Office Director, Cyber Security, National Security Secretariat
VII. NCSC Technical Director
VIII. Whitehall Departmental representatives:(Deputy Director, Head of Telecoms Security, DCMS, Deputy Director Cyber Policy, Serious & Organised Crime Group, Home Office. Current CSP representatives: BT CEO Security; Director Group Security, Vodafone

There will be up to 4 CSP representatives at any one time. CSPs are appointed to represent the industry view on an advisory capacity to the board[1]. In the case of an actual or perceived commercial conflict of interest or prospect of commercial advantage the relevant CSP will be expected to recuse themselves from the relevant board discussion. CSPs that do not sit on the Oversight Board will receive regular updates and information from the Secretariat and they can feed in comments and requirements through the Secretariat. The Secretariat will ensure that no information which would be deemed commercially sensitive between CSPs is circulated to the member CSPs. Non-member CSPs may be invited to attend on an ad hoc basis.

- **Meeting Frequency and Topics**

It is expected that the Oversight Board will meet three times per year, more frequently if required.

i. Meeting One – will be to set the high level objectives of HCSEC as relevant to the scope of the Oversight Board, based on CSP contractually confirmed requirements to HCSEC.

[1] The term 'advisory capacity' is used in relation to the CSP members acting on a personal, industry expert basis rather than representing their companies. They remain full members of the Oversight Board.

ii. Meeting Two – mid-year will be to assess progress of HCSEC in achieving their objectives

iii. Meeting Three – end of year will be to assess the delivery of objectives, and to review the findings of the Annual Management Audit and the Technical Competence Review to develop the annual report for the National Security Adviser.

- **Reporting**

The Oversight Board will provide an annual report to the National Security Adviser addressing the topics set out at paragraph 3.1. The National Security Adviser will provide copies of this report to the National Security Council and a summary of key points to the Chairman of the Intelligence and Security Committee of Parliament. All reports will be classified according to the sensitivity of their contents and will be distributed at the discretion of the National Security Adviser.

- **Modification to the Oversight Board Terms of Reference (TORs)**

The Board's intent is that these Terms of Reference are modified only when absolutely necessary. The following process shall be used to amend the Terms of Reference when necessary:

iv. Any modification to the Terms of Reference requires a specific topic on the Oversight Board Agenda and must be discussed at a face-to-face meeting.

v. The proposed changes and text should be distributed to the OB members at least 7 working days in advance of the meeting;

vi. The proposed amendment shall be discussed at the Oversight Board meeting and may be amended after all members have reached a consensus.

vii. The final text of the amendment shall be formally confirmed in writing by all Oversight Board members.

Upon final agreement, updated Terms of Reference will be distributed to all Oversight Board members.

- **Secretariat**

  GCHQ will provide the secretariat function.

- **Non-Disclosure Obligation**

  Without prejudice to paragraph 6, all information provided to any Oversight Board Member or third-party (together a “receiving party”) in connection with the operation of the Oversight Board shall be treated as confidential information which shall not be copied, distributed or disclosed in any way without the prior written consent of the owner of the information. This obligation shall not apply to any information which was in the public domain at the time of disclosure otherwise than by the breach of a duty of confidentiality. Neither shall it apply to any information which was in the possession of a receiving party without obligation of confidentiality prior to its disclosure to that party. Nor shall it apply to any information which a receiving party received on a non-confidential basis from another person who is not, to the knowledge and belief of the receiving party, subject to any duty not to disclose that information to that party. Nor shall it prevent any receiving party from complying with an order of Court or other legal requirement to disclose information.

## Appendix B

### Issues raised in the 2018-2019 Audit and current status

The 2018-2019 Audit reviewed progress against addressing the following issue and two advisories that were highlighted in the 2018-2019 report.

- **RFIs returned outside SLA period**

  This finding remains unresolved and a similar finding was reported this year.

- **Review of progress against evaluation plan**

  HCSEC internal processes were updated to address the issue. The 2019 audit did not raise any advisories against HCSEC's programme planning.

- **Rigour of auditable information**

  Following greater emphasis within HCSEC, the 2019 audit did not raise any concerns issues or advisories relating to the rigour of auditable information.