HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD

ANNUAL REPORT

2021

A report to the National Security Adviser of the United Kingdom

June 2021

Foreword

This annual report covers the period January 2020 to December 2020.

This page left intentionally blank

HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD ANNUAL REPORT

Part I: Summary

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

1.2 HCSEC has been running for ten 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.

1.3 The HCSEC Oversight Board, established in 2014, is chaired by Lindy Cameron, 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.

1.4 The Oversight Board has now completed its seventh 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.

1.5 The key conclusions from the Oversight Board's seventh year of work are:

1.6 **The NCSC Technical Competence Review found that HCSEC continues to provide world class expertise** in the analysis of telecommunications products. Despite significant challenges, HCSEC have effectively managed the impacts of the COVID-19 pandemic and the US Entity Listing of Huawei, ensuring that the work of HCSEC will be able to continue into the future.

1.7 In 2020, **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;

1.8 **Sustained progress has been made during 2020 on remediating the point-issues found in previous reports.** That includes considerable progress on the rectification of boards containing an old and out-of-mainstream-support component, and progress on binary equivalence, fixed access issue, and vulnerability management in line with expectations.

1.9 Nonetheless, cognisant of the impact of COVID-19, the work of HCSEC continues to uncover issues that indicate there has been **no overall improvement over the course of 2020 to meet the product software engineering and cyber security quality expected by the NCSC**.

1.10 The role of the Oversight Board is described in its terms of reference, and those terms of reference are unchanged. Matters relating to the new Telecommunications Security Bill (the "TSB") and enforcement of any Designated Vendor Direction issued under it are not directly within the scope of the Oversight Board. However, if enacted in line with the ministerial intent, the TSB will fundamentally change the landscape for network security, and in doing so the context in which HCSEC will operate. The NCSC anticipates that the new security obligations in the TSB will result in improvements in the security of all vendor equipment. Separately, the designated vendor provisions in

the Bill will provide a robust framework to manage risks arising from vendors' equipment in UK networks, including the types of strategic issues with Huawei equipment highlighted below.

1.11 **The seventh independent audit of HCSEC's ability to operate independently of Huawei has been completed by Ernst & Young and reported four observations.** The HCSEC Oversight Board has concluded that the report provides important external reassurance from a globally respected company and satisfied the Oversight Board that the arrangements for HCSEC's operational independence from Huawei Headquarters operated robustly and effectively during 2020 and in a manner consistent with the 2010 arrangements between the Government and the company.

1.12 Among these observations, the auditors noted that there was a **delay in the issue of the Letter of Authority to HCSEC** at the end of 2020. This has since been rectified and ensures that HCSEC can continue to operate independently of Huawei headquarters during 2021.

1.13 The Oversight Board want to reemphasise that it is vital that the NCSC be able to decide freely, in its sole discretion, which products are analysed by HCSEC. That discretion should not be constrained legally or practically. As a consequence of uncertainty around the Bill a contractual matter this year had the effect of practically limiting that discretion. The Oversight Board's position is that no contractual arrangements, nor negotiations should unduly constrain the NCSC's decision making. Huawei understands the Oversight Board's position.

1.14 Overall, **HCSEC continues to provide effective, independent oversight of Huawei products in the UK, and remains an essential component of the UK's mitigation strategy**. Noting that some of the issues highlighted in this summary will also impact HCSEC in 2021, the Oversight Board will continue to oversee and ensure that independence in 2021, seeking to ensure that the issues are satisfactorily resolved and do not result in any impact to HCSEC's independence.

Page Break

This page is intentionally left blank

Page Break

HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD 2020 ANNUAL REPORT

Part II: Technical and Operational Report

2.1 This is the seventh 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, have any loci in this process otherwise.

Introduction

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

2.3 HCSEC has been running for ten 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.

2.4 The HCSEC Oversight Board, established in 2014, is now chaired by Lindy Cameron, who succeeded Ciaran Martin in October 2020 as the Chief Executive Officer of the NCSC and is 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.

2.5 This seventh 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.

2.6 The report is set out as follows:

1. Section I sets out the Oversight Board terms of reference and membership;
2. Section II describes HCSEC staffing, skills and recruitment.
3. Section III covers HCSEC's effectiveness;
4. Section IV summarises the findings of the 2020 independent audit;
5. Section V brings together some conclusions.

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

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

3.2 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.

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

I. 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
II. second, the independence, competence and therefore overall effectiveness of HCSEC in relation to the discharge of its duties.

3.4 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

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

1. To provide security evaluation coverage over a range of UK customer deployments as defined in an annual HCSEC evaluation programme;
2. To continue to provide assurance to the UK Government by ensuring openness, transparency and responsiveness to Government and UK customer security concerns;
3. 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;
4. 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 January 2020 - December 2020

3.6 This report covers the technical work undertaken from January 2020 until December 2020. In its four meetings in 2020, the Oversight Board has:

1. Received regular corporate updates on Huawei UK;
2. Discussed future technology trends and how they may affect the work of the Oversight Board;
3. Received regular updates on HCSEC recruitment and staffing;
4. Commissioned a seventh HCSEC management audit of the independence of the Centre.
5. Considered the impact on HCSEC of the changes to the U.S. Entity Listing of Huawei during 2020.
6. Overseen the transfer of the HCSEC business unit to a new entity, Cyber Security Evaluations Ltd (CSEL)
7. Discussed mitigation strategy, specifically within the context of the UK Government's supply chain decisions and the Telecommunications (Security) Bill.

~~~~~
~~~~~

SECTION II: HCSEC Staffing

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

Staffing and skills

4.2 The 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.

4.3 There were no failures in the DV process this year. As noted in this year's audit report, there have been some delays to the clearance process for new entrants this year due to the impacts of the COVID-19 pandemic.

4.4 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 2 resignations and 2 new recruits with final head count remaining consistent to the start of the year at 39 against a budgeted of 40+2 (the +2 is to allow for flexibility).

4.5 It remains critical that HCSEC continues to recruit technical cyber security specialists to manage attrition and succession. HCSEC and the 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 2021.

~~~~~
~~~~~

Section III: HCSEC's Effectiveness

5.1 2020 is the seventeenth year of the Government's active management of Huawei's presence in the UK's telecommunications networks, the tenth year of the Government's extended risk management programme for Huawei in the UK and the seventh year of the Oversight Board. The Board's role is to oversee and ensure the independence, competence, and overall effectiveness of HCSEC.

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

1. The first provides an evaluation of the functional effectiveness of HCSEC; HCSEC's technical capability to effectively analyse Huawei's products.

2. The second evaluates the *strategic* effectiveness of HCSEC; as a function of the UK's mitigation strategy for Huawei equipment, based on the evidence provided by HCSEC's analysis.

Section III(a): HCSEC's Functional Effectiveness

HCSEC Programme Build and Prioritisation

6.1 The programme build process remains broadly the same as in previous years. The UK operators, the 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 2020, and the relative priority of equipment has remained consistent.

6.2 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.

6.3 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.

6.4 Modifications were necessary during 2020 as a result of the COVID-19 pandemic impacting HCSEC's productivity.

HCSEC Evaluation Processes

6.5 HCSEC's assessment programme in 2020 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 the 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.

6.6 Additionally, this year HCSEC have trialled new forms of report which serve to demonstrate the support that HCSEC can provide to Huawei, the NCSC and UK operators in meeting the NCSC's putative future requirements.

6.7 In 2020 the evaluation schedule was clearly severely disrupted by the Covid-19 lockdown and associated restrictions. Although the anticipated evaluation schedule for 2020 was impacted, HCSEC delivery represented a reasonable cross section of the UK telecoms live environment, encompassing a fair distribution of products and networks.

6.8 The delivery of both volume and quality is a testament to HCSEC's drive and dedication with 30 reports being produced by the end of the year, consisting of:

1. 24 x Product Evaluations. This included three reports to test a new process and reporting format designed to support Huawei, NCSC and UK operators in meeting NCSC's putative future requirements.
2. 5 x Solution Evaluations
3. 1 x Software Quality Report

HCSEC Analysis

6.9 HCSEC continues to have world-class security analysts in the complex sphere of telecommunications. This year, despite the challenging conditions with Covid-19, they have continued to provide unique insights into Huawei products giving the UK telecoms community a detailed understanding of the software engineering and cyber security risks associated with Huawei equipment.

Impact of the COVID-19 pandemic

6.10 Due to the sensitivity of the work undertaken by HCSEC, the core of HCSEC's work can only be undertaken within HCSEC's secure accommodation. Lockdowns and

social distancing reduced the building's occupancy, and reduced the time that HCSEC staff could spend on core work.

6.11 However, when not doing core work, teams continued to develop tools, perform research, and perform other supporting work. It is likely that this investment will increase the efficiency of HCSEC's work in future years.

Impact of US Entity Listing and Cyber Security Evaluations Limited (CSEL)

6.12 It was reported in last year's Oversight Board report that Huawei UK, including its then business unit HCSEC, had been placed onto the US Entity List in May 2019. These trade sanctions were further tightened and expanded during 2020.

6.13 As noted in the 2020 Oversight Board report, being added to the Entity List had an impact on HCSEC's productivity during 2020. On agreement between Huawei and the NCSC and as the only option to sustain HCSEC's operation, on 1 November 2020, the HCSEC business unit was transferred to a new entity. CSEL is not on the US Entity List. The sole purpose of CSEL is as a vehicle to hold the HCSEC business unit. The processes and controls that are in place to ensure the operational independence of HCSEC from Huawei HQ remain unchanged. These processes and controls continue to be audited by Ernst & Young.

HCSEC Reporting

6.14 Despite the difficult operating circumstances, the HCSEC evaluation process continues to identify and report point vulnerabilities. Strategic architectural and process issues continue to be noted in HCSEC's reports. These are similar to those identified in previous reports.

UK Government Policy Announcements and future evaluations

6.15 On 28th January 2020 Government announced the conclusions from the final part of its Telecoms Supply Chain Review. This set out a framework of measures which UK telecoms operators were advised to apply when using vendors within their networks which were deemed to present a heightened risk. One such measure was the existence and adherence to a bespoke, vendor-specific mitigation strategy, designed and overseen by the NCSC. In the case of Huawei, this includes, amongst

other mitigations, the continued work of HCSEC, as part of the pre-existing arrangements put in place to manage the risks presented by Huawei's presence in the UK.

6.16 A further policy announcement was made on 14th July 2020 following a review of the impact of changes made by the United States in May 2020 to their foreign-produced direct product rules [1] . NCSC guidance accompanying this policy announcement rescoped the existing mitigation strategy for Huawei and advised operators to cease the procurement of certain products[2]. This new advice was based on the NCSC's concern that the rule changes would impact HCSEC and NCSC's ability to provide sufficient assurance for some products. This will likely significantly reduce the number of new products that operators submit to HCSEC for evaluation in future years.

Conclusion

6.17 HCSEC continues to provide world-class expertise in the analysis of telecommunications products. Despite significant challenges, HCSEC have managed to sustain its critical function and continue to be productive. HCSEC have effectively managed the impacts of the COVID-19 pandemic and the US Entity Listing of Huawei, ensuring that the work of HCSEC will be able to continue into the future.

[1] https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027#:~:text=Digital%20Secretary%20Oliver%20Dowden%20said,equipment%20from%20our%205G%20networks%E2%80%9D.

[2] https://www.ncsc.gov.uk/information/5g-and-us-sanctions-round-up

Section III(b): HCSEC's Strategic Effectiveness

7.1 During 2020, the HCSEC Oversight Board, the NCSC and Huawei have discussed the following topics to the extent that they refer to HCSEC's Strategic Effectiveness:-

- Mitigation strategy and its relationship to the DCMS Supply Chain Review and the Telecommunications (Security) Bill.
- Remediation of critical out-of-mainstream-support component.
- Binary equivalence
- Fixed Access Issue
- Vulnerability management.

7.2 In previous years the Oversight Board and the NCSC have engaged with Huawei on a range of other issues relating to HCSEC's strategic effectiveness including:

- Product version management and single build.
- Configuration management
- Product software engineering and cyber security quality
- Component management (other than remediation of past issues)
- The company's internal transformation programme which seeks to respond to these (and other) issues.

7.3 For this reporting period, the work of HCSEC continues to uncover issues that indicate there has been no overall improvement over the course of 2020 to meet the product software engineering and cyber security quality expected by the NCSC. However, these are long-term, systemic changes intended to address risks arising for UK networks from on-going serious and systematic defects in Huawei's software engineering and cyber security competence. The Government's introduction of the Telecommunications (Security) Bill should provide a framework within which to address these strategic risks differently.

7.4 The Telecommunications (Security) Bill is intended to raise the bar of security in telecoms networks, including for all telecoms network equipment. The overall security framework in the Bill is intended to ensure that these basic security issues are not endemic in any vendor's products. It will also provide a framework within

which to manage risks arising in relation to Huawei equipment specifically. The role of the Oversight Board is described in its terms of reference, and those terms of reference are unchanged. Matters relating to the TSB are not directly within the scope of the Oversight Board. However, if enacted in line with the ministerial intent, the TSB will fundamentally change the landscape for network security, and in doing so the context in which HCSEC will operate.

7.5 Notwithstanding the legislative framework, Government has indicated that the presence of Huawei equipment in the UK's carrier networks must continue to be linked to the existence of an NCSC-approved mitigation strategy, including the work done by HCSEC. As such, the NCSC considers that HCSEC will remain an essential component in the management of the risks arising from the use of Huawei equipment in UK telecoms networks, including risks due to equipment quality.

7.6 The NCSC's view is that the new legislative regime together with an evolved Huawei mitigation strategy will significantly reduce many of the strategic risks highlighted in previous reports.

7.7 Huawei has stated to the Board that it looks forward to the publication of the new detailed technical standards and security requirements in accordance with the Bill, so that vendors such as Huawei can continue to support operators.

Remediation

7.9 As noted in previous reports, Huawei use an old version of a third-party real-time operating system in products. This component went out-of-mainstream support during 2020.

7.10 Using old and out-of-mainstream-support components within a product leaves those products more vulnerable to exploitation. 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. By the end of 2019, 17% of the impacted equipment boards had been updated and replaced.

7.11 During 2020, Huawei and the UK operators had remediated a further 35% of the impacted equipment boards, with another 23% of the equipment boards reaching the end of their supported life. Going into 2021, of the very large number of boards

originally impacted, Huawei and UK operators remain responsible for remediating the final 25%, specifically the affected boards that continue to be used in UK networks and that remain in support. This remains in line with the 2019 remediation plan agreed between Huawei and the operators.

7.12 Overall, Huawei and UK operators have made considerable progress at remediating the risk during 2020. Given the equipment boards are geographically distributed and physical access is frequently required to rectify the issue, this progress is remarkable within the context of the global pandemic. Based on this progress, while a national-scale risk remains, should further security issues be found associated with this component, the impact will be considerably less than it would have been 2 years ago. Based on Huawei's agreed plans with UK operators, further remediation work during 2021 will successfully bring this risk down to a manageable level.

Binary equivalence

7.13 The 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. During 2020, Huawei have provided products which satisfy this criteria for 8 product builds, in line with expectations.

7.14 Huawei have committed to delivery of binary equivalence across officially released versions of all carrier products sold into UK from December 2020.

Fixed Access Issue

7.15 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.

7.16 All these vulnerabilities have now been remediated. During 2020, Huawei re-wrote some of the relevant protocol handling code and HCSEC have re-examined this protocol handler for any further vulnerabilities.

Vulnerability management

7.17 During 2020, Huawei effectively remediated all vulnerabilities discovered and reported by HCSEC in line with expectations.

NCSC discretion in respect of products to be evaluated by HCSEC

7.18 The Oversight Board want to reemphasise that it is vital that the NCSC be able to decide freely, in its sole discretion, which products are analysed by HCSEC. That discretion should not be constrained legally or practically. As a consequence of uncertainty around the Bill a contractual matter this year had the effect of practically limiting that discretion. The Oversight Board's position is that no contractual arrangements, nor negotiations should unduly constrain the NCSC's decision making. Huawei understands the Oversight Board's position.

Conclusion

7.19 During 2020, Huawei have made strong progress at remediating an out-of-mainstream-support component within products in the UK's networks. Huawei has also made progress, in line with expectations, on binary equivalence, fixed access issue, and vulnerability management.

7.20 Nonetheless, cognisant of the impact of COVID-19, the work of HCSEC continues to uncover issues that indicate there has been **no overall improvement over the course of 2020 to meet the product software engineering and cyber security quality expected by the NCSC**. The NCSC anticipates that the new Telecoms (Security) Bill will improve the security of all vendor equipment and provide a robust framework to manage risks arising from vendors' equipment in UK networks, including the types of strategic issues highlighted above.

7.21 Finally, the Oversight Board want to reemphasise that it is vital that the NCSC be able to decide freely, in its sole discretion, which products are analysed by HCSEC. That discretion should not be constrained legally or practically.

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

8.1 This section focuses on the more general work of the Oversight Board beyond its oversight of the technical assurance provided by HCSEC. For the seventh 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

8.2 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 2022. E&Y's Annual Management Audit was conducted in accordance with the International Standard on Assurance Engagements (ISAE) 3000.

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

I. An initial phase to assess the Control Environment and Design Scope was completed by November 2020;
II. A second phase to run a preliminary review of the design and operation of the controls in place to support the independent operation of HCSEC. This phase was completed during December 2020.

III. A final audit phase comprising the full year end audit during January 2021, with the report presented in March 2021.

The nature and scope of the audit

8.4 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.

8.5 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

8.6 The HCSEC Annual Management Audit March 2021 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.

8.7 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 2020 to 31 December 2020

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 2020 to 31 December 2020
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 2020 to 31 December 2020.

Results of Testing

8.8 The following deviations were identified:

I. Signed Letter of Authority

8.9 The HCSEC Managing Director holds a valid 'Letter Of Authority' from Huawei providing delegated rights to manage Finances, HR, Procurement (amongst other delegated responsibilities) for HCSEC.

8.10 The budget used by HCSEC to manage operations over the course of the year is the same as that approved at the start of the year.

8.11 It was noted whilst a signed Letter of Authority was in place between 1 January 2020 and 20 December 2020, no subsequent Letter of Authority has been issued from 21 December 2020 onwards.

Oversight Board Response:

8.12 There was a delay in the issue of the Letter of Authority to HCSEC at the end of 2020. This has since been rectified and ensures that HCSEC can continue to operate independently in 2021.

II. Recruitment and Staff Management

8.13 All HCSEC staff are obligated to undertake and pass the NCSC-operated security clearance process as a condition of permanent employment. Staff pending clearance for over 12 months are escalated to the NCSC by HCSEC.

8.14 It was noted three staff were not cleared, two having been hired in the last nine months and one staff member who had not been granted clearance after 12

months. This was verbally escalated to the NCSC and is as a result of COVID-19 and the impact on clearance process timelines.

Oversight Board Response:

8.15 The Oversight Board accepts this finding, noting that in line with HCSEC's normal business practices, no uncleared staff were granted access to sensitive data.

III. Evaluation Planning Programme

8.16 HCSEC undertakes an annual planning process which takes into consideration the major implementations expected during the coming year. The plan of work must be approved by the NCSC. Monthly programme updates are held within HCSEC to review progress against the plan of work.

8.17 It was noted programme updates were not held for September, October or December following the updated plan. No updates were available between March – August 2020 due to the impact of the office closure caused by COVID-19 working restrictions.

Oversight Board Response:

8.18 The Oversight Board accepts this finding. HCSEC will ensure that monthly programme updates are held, where practical, regardless of the COVID situation.

IV. RFIs returned outside SLA period

8.19 Requests by HCSEC for software and hardware from Huawei must be delivered within the SLA period as documented in the HCSEC Oversight Board Terms of Reference.

8.20 It was noted six hardware requests (out of nine for the year) were delivered to HCSEC outside the SLA period.

8.21 One further hardware RFI was noted as not having a delivery date available, as at the time of the audit, this was being held in the UK warehouse with delivery to HCSEC offices delayed until the hardware was required.

8.22 Discussion with HCSEC staff and review of programme updates held did not identify any need for escalation regarding these delays.

Oversight Board Response:

8.23 SLA dates are intended to ensure that HCSEC's operational effectiveness cannot be impacted by restricting the timely delivery of equipment. The Oversight Board is satisfied that HCSEC's operational effectiveness was not impacted by this issue during 2020. The Oversight board expects processes to be improved but can accept small deviations provided there is no operational impact.

Prior year issues and Current Status

8.24 Appendix B provides a summary of the issues and observations from the previous year's report published in 2020.

Overall Oversight Board conclusions of the audit

8.25 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 were operating robustly and effectively during 2020, and in a manner consistent with the 2010 arrangements between the Government and the company.

8.26 Four observations were identified by the auditors and accepted by the Oversight Board. The Oversight Board is satisfied that these findings did not impact the independence or operational effectiveness of HCSEC during 2020. Addressing these observations will require process improvements from all parties. Noting that some observations will also impact HCSEC in 2021, the Oversight Board will remain vigilant to maintaining HCSEC's operational independence.

~~~~~
~~~~~

SECTION IV: Conclusion

9.1 HCSEC continues to provide effective, independent oversight of Huawei products in the UK, and remains an essential component of the UK's mitigation strategy. Despite the dual challenges of the COVID-19 pandemic and the US Entity Listing of Huawei, HCSEC's function and effectiveness has sustained during 2020.

9.2 The Oversight Board want to reemphasise that it is vital that the NCSC be able to decide **freely, in its sole discretion, which products are analysed by HCSEC**. That discretion should not be constrained legally or practically. Huawei understands the Oversight Board's position.

9.3 HCSEC continues to uncover issues that indicate there has been **no overall improvement over the course of 2020 to meet the product software engineering and cyber security quality expected by the NCSC.** The NCSC anticipates that the new Telecoms (Security) Bill will improve the security of all vendor equipment and provide a robust framework to within which to manage risks arising in relation to Huawei's equipment specifically. Consequently, assuming the intent of the Telecoms (Security) Bill is delivered, going forward **the NCSC expects to be able to provide improved technical assurance in the security risk management of Huawei equipment in UK networks.**

9.4 **Sustained progress has been made during 2020 on remediating the point-issues found in previous reports**. That includes strong progress on the rectification of boards containing an old and out-of-mainstream-support component, and progress on binary equivalence, fixed access issue, and vulnerability management in line with expectations.

9.5 In advance of the passing of the Telecoms (Security) Bill, the HMG and Industry members of the Oversight Board have reiterated that it is crucial to ensure that HCSEC continues to function appropriately and in accordance with the new legislation. Huawei confirmed to the Oversight Board that HCSEC will continue to operate on the existing model for 2021.Huawei has also stated to the Board that it looks forward to the publication of the new detailed technical standards and security requirements in

accordance with the Bill, so that vendors such as Huawei can continue to support operators.

~~~~~
~~~~~

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

1. 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.

2. Scope of Work

2.1 In Scope

The Oversight Board will focus on:

1. 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.
2. The independence, competence and therefore overall effectiveness of HCSEC in relation to the discharge of its duties.

2.2 Out of Scope

1. All products that are not relevant to UK national risk;
2. 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;
3. The commercial relationship between Huawei and CSPs; and
4. HCSEC's foundational research (tools, techniques etc.) which will be assessed and directed by GCHQ.

3.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.

4. 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 (Lindy Cameron 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[3]. 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

[3] 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.

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.

5. 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.
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.

6. 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.

7. 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.

8. Secretariat

GCHQ will provide the secretariat function.

9. 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 2020 Audit and current status

- **RFIs returned outside SLA period**

This finding remains unresolved with similar finding reported in previous years.