HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD

ANNUAL REPORT

2018

A report to the National Security Adviser of the United Kingdom

July 2018

HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD ANNUAL REPORT

Part I: Summary

1. This is the fourth 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, whose parent company is a Chinese headquartered company which is now one of the world's largest telecommunications providers.
2. HCSEC has been running for seven 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 telecommunications market. Through HCSEC, the UK Government is provided with insight into Huawei's UK's 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.
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. The structure of the Oversight Board has not changed significantly, but membership has changed in the year 2017-18. Mainly, this is due to staff rotations in both HMG and Huawei positions.

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

i. **New secure premises for HCSEC are on track**; the previously reported acquisition of new premises for HCSEC has experienced some commercial delays, but remains broadly on track for completion in late 2018;

ii. **Technical issues have been identified in Huawei's engineering processes,** leading to new risks in the UK telecommunications networks;

iii. **The GCHQ Technical Competence Review found that the capability of HCSEC has improved in 2017**, and the quality of staff has not diminished, meaning that technical work relevant to overall mitigation strategy can be performed at scale and with high quality;

iv. **The fourth independent audit of HCSEC's ability to operate independently of Huawei HQ has been completed**, with – again – no high or medium priority findings. The audit report identified two low rated finding and two advisory issues, relating to record keeping and the retention of auditable information. Each issue has an agreed rectification plan, 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 the Government and the company.

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

i. It is evident that HCSEC continues to provide unique, world-class cyber security expertise and technical assurance of sufficient scope and quality as to be appropriate for the current stage in the assurance framework around Huawei in the UK.

ii. The HCSEC Oversight Board is assured that the Ernst & Young Audit Report provides important, external reassurance that the arrangements for HCSEC's operational independence from Huawei Headquarters is operating robustly and effectively, and in a manner consistent with the 2010 arrangements between the Government and the company.

iii. However, identification of shortcomings in Huawei’s engineering processes have exposed new risks in the UK telecommunication networks and long-term challenges in mitigation and management.

6. The Oversight Board concludes that in the year 2017-18, HCSEC fulfilled its obligations in respect of the technical work required of it by NCSC.

7. Due to areas of concern exposed through the proper functioning of the mitigation strategy and associated oversight mechanisms, the Oversight Board can provide only limited assurance that all risks to UK national security from Huawei’s involvement in the UK’s critical networks have been sufficiently mitigated. We are advising the National Security Adviser on this basis.

This page is intentionally left blank

HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD 2017 ANNUAL REPORT

Part II: Technical and Operational Report

This is the fourth annual report of the Huawei Cyber Security Evaluation Centre 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

1. This is the fourth 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, whose parent company is a Chinese headquartered company which is now one of the world's largest telecommunications providers.

2. HCSEC has been running for seven 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's 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.

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. The structure of the Oversight Board has not changed significantly, but membership has changed in the year 2017-18. Mainly, this is due to staff rotations in both HMG and Huawei positions.

4. This fourth 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.

5. The report is set out as follows:

I. Section I sets out the Oversight Board terms of reference and membership;

II. Section II describes HCSEC staffing, skills, recruitment and accommodation;

III. Section III covers HCSEC technical assurance, prioritisation and research and development;

IV. Section IV summarises the findings of the 2016-17 independent audit;

V. Section V brings together some conclusions.

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

1.1 The HCSEC Oversight Board was established in early 2014. It meets quarterly under the chairmanship of Ciaran Martin, the Chief Executive of the UK National Cyber Security Centre (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.

1.2 The role of the Oversight Board is to oversee and ensure the independence, competence and overall effectiveness of HCSEC 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.

1.3 The Oversight Board's scope relates only to products that are relevant to UK national security risk. Its remit is two-fold:

- 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.

1.4 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 main objective of the Oversight Board remains 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 ISC.

The Board's objectives for HCSEC

1.5 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 security and engineering competence.

The HCSEC Oversight Board: Business April 2017- March 2018

1.6 In its two meetings since the publication of the 2017 Annual Report, the Oversight Board has:

- Provided regular corporate updates on Huawei UK
- Discussed future technology trends and how they may affect the work of the Oversight Board;
- Been supplied with regular updates on HCSEC recruitment, staffing and accommodation plans;
- Received updates on the HCSEC technical programme of work and its progress and received a detailed report on technical visits to Huawei HQ in Shenzhen by the NCSC Technical Director and technical team, some with UK operators, to discuss technical issues;
- Taken evidence around the root causes of the problems achieving binary equivalence and agreed a programme of work towards remediation;
- Taken evidence of redelivery of source code packages, the basis of which was detailed in the previous report;
- Taken evidence on the security risks engendered by Huawei's lifecycle management of critical components and written to the National Security Adviser based on this;
- Commissioned a fourth HCSEC management audit of the independence of the Centre.

~~~~~
~~~~~

SECTION II: HCSEC Staffing

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

Staffing and skills

2.2 A change was made to the senior management team in HCSEC. A long serving member of the HCSEC team, who has demonstrated excellent technical knowledge during his tenure, was appointed as Director Solutions and Programme, overseeing the execution of technical operations in HCSEC. His appointment to the senior management team is welcomed by the Board. The leadership team continues to work well together, leading HCSEC and engaging with Huawei in a constructive manner.

2.3 The NCSC leads for the Government in dealing with HCSEC and the company more generally on technical security matters. The NCSC, on behalf of the Government, 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.

2.5 Staffing at HCSEC has increased in line with expectations for the year 2017. By the end of the calendar year, the staff numbers were almost as predicted with, once again, only one position not filled (taking 'offer accepted' as the point of employment). Due to uncertainty around the binary equivalence work, it was unclear precisely what skills were needed to support this work and so a conscious decision made to not fill the three extra posts committed to by Huawei and preserve the headcount for 2018.

2.6 It remains critical that HCSEC continues to recruit technical cyber security specialists to manage attrition and succession. This continued excellent progress has been driven by the ongoing personal involvement of HCSEC leadership and represents a significant amount of work.

2.7 Again, a significant number of potential recruits were sifted out due to clearance requirements. Furthermore, three candidates that passed initial sifting and were employed by HCSEC subsequently failed DV clearance and were removed from the centre. The small risk associated with these staff was adequately managed through the supervision and oversight provided during their probationary employment period.

Accommodation

2.9 The 2017 report spoke of the successful search for new accommodation for HCSEC to cope with the expansion of HCSEC's operation. The delays alluded to in that report came to pass for reasons associated with the building configuration and the logistics of the move. However, the process has been successfully concluded and the move to the new premises should be completed during 2018Q4. These delays are not in any way the result of Huawei HQ's inaction or interference.

2.10 The new accommodation will allow for concurrent reference networks to be put in place, allowing solution evaluations to proceed at pace. It also allows for increased development activity to help manage the significant number of products needing assessment.

2.11 Overall, good progress has been made on staffing and skills during 2017. Quarterly monitoring by the Oversight Board has shown no causes for concern in the number of staff and their skills. The delay to the new accommodation is unfortunate but has in no way affected the ability of HCSEC to discharge its functions this year.

~~~~~
~~~~~

Section III: HCSEC Technical Assurance

2017 is the seventh year of the Government's extended risk management programme for Huawei's involvement in the UK telecommunications market. In the previous two years, the Oversight Board chose to publish, exceptionally, more details of the technical assurance work undertaken as part of this programme. This report builds on the previous three reports. The Oversight Board's intent is to provide detailed technical assessment only periodically and when issues specifically warrant it. This year there have, once again, been technical issues that specifically warrant inclusion in the report due to their direct impact on the ability of the Oversight Board to provide assurance to the National Security Advisor. It is to be welcomed that despite difficulties, Huawei has continued to work closely with NCSC and HCSEC and provided access and information when requested.

Evaluation Process

3.1 HCSEC's assessment programme in 2017 continued the product and solution evaluation split which proved successful in previous years. In 2017, 27 product evaluations were completed, 5 solution evaluations were started, with 3 being completed during the reporting period. The evaluations covered products and architectures for 4 UK operators.

3.2 The last Oversight Board report detailed issues with a particular evaluation, concerning the virtualised SMSC. Regardless of the issues, the operator chose to deploy the solution with an expectation that they would upgrade to the next version to be evaluated by HCSEC. The operator has not yet chosen to upgrade the system to a version that could be evaluated by HCSEC.

3.3 The NCSC has a stated intent of HCSEC performing a product evaluation on every relevant product in the UK at least every two years. HCSEC's product evaluation pipeline is configured to achieve this. Huawei have provided long term headcount for the evaluation and infrastructure build teams and the Oversight Board is confident that continued attention from HCSEC seniors will ensure that there are sufficient appropriately skilled staff to maintain the NCSC intent. HCSEC staff must be capable of achieving security clearance and have the requisite skills, meaning the pool of available talent is small.

3.4 The previous Oversight Board report described a group set up by NCSC to discuss the management of the risks around the Huawei Mobile Virtual Network Operator (MVNO) solution in the UK. Over 2017, this has been expanded and its scope broadened to cover wider supply chain risk management issues in the telecoms sector as a whole.

3.5 The evaluation process continues to find a significant number of point vulnerabilities and more strategic architectural and process issues. Huawei continues with their remediation work; the feedback provided by HCSEC to Huawei R&D continues to be of high quality and the HCSEC technical staff continue to assist the Huawei R&D teams in their remediation efforts.

Prioritisation and programme build

3.6 The risk-based prioritisation scheme detailed in previous Oversight Board reports has continued to be applied during 2017.

3.7 The programme build process remains broadly as previous years. The operators, NCSC and HCSEC collaboratively prioritise the work of HCSEC. This is necessary to balance the sometimes-competing constraints and requirements for the best benefit of the UK, for example not allowing a particular operator to dominate the programme of work due to commercial pressures. 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 lightweight process involving the NCSC and the relevant operators is used to manage and approve any modifications.

3.8 Little has changed in terms of high level prioritisation of equipment, although the scale and scope of Huawei’s 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. The results of HCSEC’s work is reported directly to the operators and they are expected to feed them into their corporate risk management processes.

Configuration Management and Binary Equivalence

3.9 The previous Oversight Board report spoke to two significant issues. The first of these was the extraction by Huawei HQ of a subset of source code from configuration managed repositories for onward delivery to HCSEC. The second was the failure of Huawei R&D to repeatably build a product to a consistent binary. As described in the previous Oversight Board report, this means that any assurance provided by the overall risk management strategy, and therefore the Oversight Board, is currently limited.

3.10 The Oversight Board agreed with Huawei HQ a timetable for the redelivery of all source code for the products previously delivered to HCSEC, with all code having been redelivered by December 2017. The redelivery of code packages was completed three months ahead of the deadline.

3.11 HCSEC have observed that all new packages contain more code. If the Binary Equivalence Programme completes and is successful, then HCSEC should be able to verify that all products build to the binary running in the UK network. It is important that this work is completed quickly.

3.12 The last report talked about rescoping the division of effort between HCSEC and Huawei R&D, with Huawei R&D expected to take on more of the mandrolic work to show binary equivalence, leaving HCSEC to perform a verification function.

3.13 This rescoping started with Huawei R&D performing some work to understand the underlying issues observed by HCSEC in performing repeatable builds for products. This work showed that the underlying engineering and build process was not repeatable.

3.14 Huawei R&D was asked by NCSC and HCSEC to perform analysis of four specific products from different product groups which showed that the underlying engineering issues, including the failure to reproduce builds, are consistent across the various product lines.

3.15 HCSEC have worked with Huawei R&D to try to correct the deficiencies in the underlying build and compilation process for these four products. This has taken significant effort from all sides and has resulted in a single product that can be built repeatedly from source to the General Availability (GA) version as distributed. This particular build has yet to be deployed by any UK operator, but we expect deployment by UK operators in the future, as part of their normal network release cycle. The remaining three products from the pilot are expected to be made commercially available in 2018H1, with each having reproducible binaries. The engineering changes have not yet been integrated into the wider development process. A second batch of products has been selected by NCSC, the operators and HCSEC and work on these should complete by the end of 2018H1, with all remaining products to follow. Assuming the continued success of the initial trials, it is the NCSC and Oversight Board expectation that this will be completed by mid 2020.

3.16 It is the NCSC intent that all products deployed in the UK will have repeatable builds and that HCSEC will be able to routinely show equivalence between the binary installed in UK networks and the binary that can be built from the source code held by HCSEC. This verification should be completed for every product version deployed in the UK that has been assessed by HCSEC. It is important that all products can be built in this way to enable the risk-based approach to HCSEC's prioritisation of work.

3.17 The Chairman of the Oversight Board had previously written to the National Security Adviser in February explaining the issue. Details of the next phase of this work were presented to the Oversight Board at the March meeting where the Board approved the plan. Work continues to remediate the engineering process issues in other products that are deployed in the UK, prioritised based on risk profiles and deployment volumes. This work should give us the ability to provide end-to-end assurance that the code analysed by HCSEC is the constituent code used to build the binary packages executed on the network elements in the UK.

3.18 Until this work is completed, the Oversight Board can offer only limited assurance due to the lack of the required end-to-end traceability from source code examined by HCSEC through to executables use by the UK operators.

Third Party Component Support Issue

3.19 A technical visit to Shenzhen was scheduled for September 2017 for NCSC, HCSEC and the UK Operators to discuss with Huawei HQ the progress around source code redelivery to HCSEC and binary equivalence. Previous technical visits have discussed Huawei's management of third party components imported as part of a product build, both commercial and open source. During a review of the programmes of work being undertaken, NCSC identified that not all components are managed through this process and, in particular, security critical third party software used in a variety of products was not subject to sufficient control.

3.20 It is now apparent that third party software, including security critical components, on various component boards will come out of existing long-term support in 2020, even though the Huawei end of life date for the products containing this component is often longer. Huawei has provided the Oversight Board with data on the extent to which this affects the UK deployments. NCSC has determined how the issue directly affects the security and reliability of deployed products and has provided the Oversight Board its opinion that this issue limits the ability of HCSEC's efforts to contribute to the overall assurance strategy in a sustainable manner.

3.21 There have been a number of detailed technical discussions between Huawei R&D and HCSEC, some including NCSC. These discussions are working towards a full understanding of the problem, a short-term mitigation plan and a more strategic fix for the underlying cause of the problem. However, there is a significant risk in the UK telecoms infrastructure if Huawei and the operators are unable to support these boards long-term.

3.22 A range of technical and contractual solutions are being discussed between the operators, NCSC, HCSEC and Huawei R&D. Any short-term mitigation obviously needs to be cognisant of the realities of the UK telecoms networks and the operators' testing and release cycles.

3.23 It is expected that the Oversight Board will receive an update on progress at its June meeting, to be held at Huawei's facilities in Shanghai, with NCSC and HCSEC working with Huawei technical teams on the detailed plans.

Summary of NCSC Technical Competence Review

3.24 The work of HCSEC in 2017 has continued capability development in the underpinning tooling necessary to provide assurance and technical security artefacts to the UK operators at the scale necessary given Huawei's position in the UK market. Through 2017, HCSEC has continued to find issues in Huawei products, demonstrating their continued ability to discover weaknesses in the Huawei product set.

3.25 HCSEC continues to have world class security researchers who are creating new tools and techniques to provide assurance in the complex sphere of telecommunications, while taking into account Huawei's unique engineering and security processes.

3.26 The work conducted by HCSEC on the binary equivalence, build process and subsequent understanding of the recurrent third party component management and support problem shows that they are competent in the field to the level necessary to independently verify Huawei R&D claims and satisfy the Oversight Board requirements.

3.27 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 with the UK operators.

Conclusion: technical assurance

3.28 NCSC still believes that the assurance model including HCSEC is the best way to manage the risk of Huawei's involvement in the UK telecommunications sector. The model is predicated on industry good practice security and engineering in Huawei. Overall, given this account, the NCSC has advised the Oversight Board that it is less confident that NCSC and HCSEC can provide long term technical assurance of sufficient scope and quality around Huawei in the UK. This is due to the repeated discovery of critical shortfalls, including but not limited to BEP and the third party component support issue, in the Huawei engineering practices and processes that will cause long term increased risk in the UK. These risks are not due to any issue with HCSEC's staffing and capabilities. Obviously, significant work will be required in managing these risks both short term and long term. The Oversight Board will be looking to HCSEC to continue to ensure that Huawei are making appropriate remediations and to advise the Oversight Board, the UK operators and the NCSC of any issues arising.

3.29 A further medium-term issue that the Oversight Board must take account of is the shift in architecture and technology brought about by things like software defined networking, virtualisation, MVNO proliferation and edge compute architectures such as 5G, along with changes in the operational models of many telecommunications operators. NCSC will need to revisit the technical assessment, including how HCSEC contributes to mitigation, and advise the Oversight Board on what mechanisms may be appropriate to continue to gain the required assurance in the use of Huawei equipment in the UK telecommunications environment.

~~~~~
~~~~~

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 fourth year running, the Board commissioned and considered an audit of HSCEC's required operational independence from Huawei HQ. This was 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. 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

4.2 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, that is until November 2019. E&Y's Annual Management Audit was conducted in accordance with the International Standard on Assurance Engagements (ISAE) 3000.

4.3 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 agree the scope and key issues for review. This phase was completed by November 2017;

ii. A second phase to run a rehearsal audit of the design and operation of the controls in place to support the independent operation of HCSEC. This phase was completed during November 2017;

iii. A final audit phase comprising the full year end audit during December 2017, with the report presented to the NCSC, HCSEC and Huawei HQ in February 2018 and the full Oversight Board in March 2018.

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:

- 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;
- Assess the technical capability of HCSEC, the competency of individual staff or the quality of the performance of technical testing;
- 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 January 2018 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 by an experienced Manager and led by Senior Manager. A Partner with Technology and Assurance subject matter knowledge acted as quality reviewer, and a second review of the final report was performed by an Ernst & Young Executive Director.

4.7 In summary, Ernst & Young concluded that there were no major concerns about the independent operation of HCSEC. The audit report's principal conclusion said:

"With the exception of the findings below [two findings rated as 'Low']*, the controls evaluated were considered to be effective as per the control descriptions and agreed test procedures. In some instances, it was noted that there is the opportunity to further strengthen the control regime or to improve the efficiency of the audit process and these have been noted below as "advisory" recommendations as opposed to identified control deficiencies."*

4.8 The audit report identified two control weaknesses within the HCSEC control environment for the Board to consider. The weaknesses were both rated as "Low", meaning that action should be considered to reduce an exposure which results in a limited impact to some aspects of the independent operation of HCSEC, but which in itself would be unlikely to compromise the independence of HCSEC overall. There were another two advisory issues, which were noted as potential minor improvements in the overall control regime. The audit findings were presented to the Board in its March meeting with an Ernst & Young Partner in attendance to brief the Board. The Oversight Board discussed each of the identified weaknesses and advisory notes in the audit and agreed an approach for each one.

Control Weakness

4.9 In summary, the area of control weakness identified, and the agreed response, relate to the following area:

i. Request and Retain Evaluation Plan Sign-Off

4.10 The evaluation plan, which outlines which products will be tested at which points of the year, is discussed with the NCSC when it is being created. Discussion with HCSEC management identified that the plan was presented to the NCSC at a scoping meeting but no evidence that this plan was approved was available. This is a repeat finding from last year.

4.11 Following review and agreement of the evaluation plan with NCSC, HCSEC should ensure that they obtain a formal confirmation that the evaluation plan is fit for purpose and retain this in their records. This should take the form of either written approval (e.g. via email) from NCSC or in the form of agreed minutes following a meeting with NCSC hosted by HCSEC. The process has been further updated such that the NCSC Technical Director for Telecoms now has delegated authority to sign off the evaluation plan, with an escalation route when necessary which will hopefully address the issue.

ii. Budget setting and ongoing financial review

4.12 The audit identified that the agreed process for establishing and approval of HCSEC's budget for the year under review had not been fully followed. Formal sign-off from each member of the HCSEC SMT (Senior Management Team) had not been formally obtained.

4.13 This control has historically been performed by HCSEC senior leadership; it is noted that there has been a significant change in senior leadership this year. Going forward, an auditable record of key decisions on the setting of the budget should be retained – particularly the explicit approval of the HCSEC SMT following the final iteration of value.

Advisory Notices

4.11 Two advisory notices were identified by the audit, relating to the recording and retention of specific, auditable information:

i. RFIs returned outside SLA period

4.12 Requests for information made to Huawei were not always returned inside the stated SLA period. In their tests the auditors identified that 4 requests for hardware were completed outside of the stated 12 week SLA period.

4.13 In discussion with HCSEC it was noted that, although specified in the Terms of Reference, the SLA is 'aspirational' and that non-adherence would not necessarily adversely impact evaluation performance. In practice there is "slack" built into the delivery to accommodate late returns. To clarify for the purposes of review, RFIs could be updated to include a “required by” date (of no earlier than the SLA period) with the intention that this is strongly adhered to and escalated when it is breached.

ii. Monitoring of spend versus budget has not been well maintained over the audit period.

4.14 Although testing of controls on expenditure did not identify any evidence that HCSEC spend had been restricted, and accordingly no undue influence exerted on its independent operation, it is difficult to verify if HCSEC spend in the year was within the agreed final budget for 2017.

4.15 Over the course of the year HCSEC made amendments to the set budget value that they track spend against (e.g. for depreciation rather than cash spend on the new premises and staff bonuses); these changes were not clearly documented.

4.16 Internal monitoring, in the form of reconciliation between spend and budget is performed informally and on an ad-hoc basis, and there is no record maintained of these reviews Related, there was also a discrepancy between the values reported by the Huawei UK finance system and those maintained by HCSEC, showing higher spend on the Huawei finance system than that tracked internally by HCSEC.

4.17 Changes to the budget from proposal through to approval should be documented. The final approved budget should be consistent with the figures monitored by HCSEC internally. If errors or accounting corrections are required this should be documented such that there is traceability between the approved value and the actual amount spent in the year.

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 2017.

Overall Oversight Board conclusions of the audit

4.16 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. Four issues – two low rated finding and two advisory issues – have been identified.

~~~~~
~~~~~

SECTION V: Conclusions

5.1 The Oversight Board has now completed its fourth full year of work. Its two meetings and its work out of Committee have provided a useful enhancement of the governance arrangements for HCSEC.

5.2 The key conclusions from the Board's fourth year of work are:

i. It is evident that HCSEC continues to provide unique, world-class cyber security expertise and technical assurance of sufficient scope and quality as to be appropriate for the current stage in the assurance framework around Huawei in the UK

ii. However, Huawei's processes continue to fall short of industry good practice and make it difficult to provide long term assurance. The lack of progress in remediating these is disappointing. NCSC and Huawei are working with the network operators to develop a long-term solution, regarding the lack of lifecycle management around third party components, a new strategic risk to the UK telecommunications networks. Significant work will be required to remediate this issue and provide interim risk management.

iii. The HCSEC Oversight Board is assured that the Ernst & Young Audit Report provides important, external reassurance that the arrangements for HCSEC's operational independence from Huawei Headquarters is operating robustly and effectively, and in a manner consistent with the 2010 arrangements between the Government and the company. The issue identified was rated as low risk and two further advisory issues were identified.

5.3 Overall therefore, the Oversight Board has concluded that in the year 2017-2018, HCSEC fulfilled its obligations in respect of the provision of security and engineering 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. However, the execution of the strategy exposed a number of risks which will need significant additional work and management. The Oversight Board will need to pay attention to these issues.

5.4 Additionally, it is hoped 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

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:

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

2.2 Out of Scope

- All products that are not relevant to UK national risk;
- 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;
- The commercial relationship between Huawei and CSPs; and
- 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 8.

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.

- GCHQ – Chair (Ciaran Martin, CEO NCSC)
- Huawei HQ – Deputy Chair (Ryan Ding, Executive Director of the Board)
- Huawei UK Managing Director
- Huawei UK Communications Director
- HCSEC Managing Director
- Cabinet Office Director, Cyber Security, National Security Secretariat
- NCSC Technical Director
- Whitehall Departmental representatives: (Deputy Director, Head of Telecoms Security, DCMS, Head of Cyber Policy Hub, Office for Security and Counter Terrorism, 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.

5. Meeting Frequency and Topics

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

[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.

- 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.

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

- 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:

- 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.

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

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

- 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 2016-2017 Audit and current status

The 2017-2018 Audit reviewed progress against addressing the following issue that was highlighted in the 2016-2017 report. The issue was rated as “Low”.

iii. Request and Retain Evaluation Plan Sign-Off

The NCSC process was updated to attempt to ensure that the NCSC Technical Director formally signed off the plan in a timely manner. Unfortunately, the finding was repeated in the 2017-2018 audit. The process has been further updated such that the NCSC Technical Director for Telecoms now has delegated authority to sign off the evaluation plan, with an escalation route when necessary.

The two advisory notices were addressed through updating of HCSEC internal processes.