HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD

ANNUAL REPORT

2017

A report to the National Security Adviser of the United Kingdom

April 2017

HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD ANNUAL REPORT

Part I: Summary

1. This is the third 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. In 2016, Huawei's annual revenue was 75.1 billion USD.

2. HCSEC has been running for six 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. In December 2016, David Francis joined HCSEC as its new Managing Director, taking over from David Pollington. Mr Francis took up his place on the Oversight Board the same month. Otherwise, membership of the Oversight Board has remained constant during 2016-2017. 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, and advised the National Security Adviser (to whom this report is submitted), allowing him to provide assurance to Ministers, Parliament and ultimately the general public that the risks are being well managed.

4. The Oversight Board has now completed its third 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. **A new Managing Director for HCSEC took office in December 2016** by way of a managed move. The agreed candidate, Mr David Francis, was an employee of Huawei whose previously held GCHQ DV clearance has been renewed; he is an accomplished technical leader and the process by which he has been brought on board has been judged to be successful;

ii. **New secure premises for HCSEC have been acquired**; the Heads of Terms agreement is expected to be signed in April and Huawei HQ has approved the budget for the new building, including fit out. The increased space allows for expansion of HCSEC's operations, will ensure future product evaluations can be completed at pace and will mean more development activity can take place to help manage the growing number of assessments needed;

iii. **A more sustainable arrangement has been reached on the division of effort on binary equivalence between HCSEC and Huawei R&D**, resulting in HCSEC being better able to perform the verification function while maintaining sufficient independence, scope and oversight to provide the NCSC and the operators appropriate assurance;

iv. **The GCHQ Technical Competence Review found that the capability of HCSEC has improved in 2016**, and the quality of staff has not diminished, meaning that assurance is able to be provided at scale, and metrics are improved;

v. **Excellent progress has been made on recruitment**, with staffing at HCSEC having increased in line with expectations. This has been driven by the significant personal involvement of HCSEC leadership, demonstrating commitment to improvement at key levels of the business;

vi. **The third 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 one low rated finding and two advisory issues, all relating to 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 two key conclusions from the Oversight Board's third 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. Assurances are still required around binary equivalence but changes in resourcing should allow greater and more sustainable progress here.

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. The single formal finding was rated 'low' by the auditors.

6. Overall, therefore, the Oversight Board concludes that in the year 2016-17, HCSEC fulfilled its obligations in respect of the provision of assurance that any risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated. We are content to advise 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 third 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 third 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. In 2016, Huawei's annual revenue was 75.1 billion USD.

2. HCSEC has been running for six 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. In December 2016, David Francis joined HCSEC as its new Managing Director, taking over from David Pollington. Mr Francis took up his place on the Oversight Board the same month. Otherwise, membership of the Oversight Board has remained constant during 2016-2017. The Oversight Board continues to include a senior executive from Huawei as Deputy Chair, as well as senior representatives from across Government and the UK telecommunications sector.

4. This third 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 new 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, Robert Hannigan, 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 that 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**. This has undergone minor revision to clarify process since the last report, through the addition of section 7, but 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 in 2016 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 competence.

The HCSEC Oversight Board: Business April 2016-March 2017

1.6 In its four meetings since the publication of the 2016 Annual Report, the Oversight Board has:

- Managed the transition of Oversight Board arrangements from GCHQ to the NCSC;
- Assured the transition to the new Managing Director of HCSEC;
- 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, some with UK operators, to discuss technical issues;
- Discussed the implication of technical analysis undertaken by HCSEC. This technical analysis intended to understand the root cause of why HCSEC was unable to demonstrate binary equivalence;
- Commissioned a third 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 new Managing Director for HCSEC took office in December 2016 following the departure of the incumbent, Mr David Pollington, who moved on for personal reasons. Given the short time available to replace Mr Pollington, it was agreed with Huawei HQ to fill the MD post through a managed move. The agreed candidate, proposed by the NCSC Technical Director, Dr Ian Levy, and agreed by Huawei HQ, was Mr David Francis, a current employee of Huawei who has previously held GCHQ DV clearance for a number of years, including during previous employment at a cyber security firm.

2.3 Mr Francis is an accomplished technical leader, having held a number of operational leadership roles across the cyber security field. While Mr Francis has held a DV clearance in the past, his DV clearance was not current at the time of his appointment. Mr Francis's clearance was reinstated on 14th March 2017 and the NCSC believes the residual risk in the intervening period has been very small and manageable.

2.4 The transition between Mr Pollington and Mr Francis was actively managed by the NCSC and Huawei to allow the transition to proceed effectively, ensuring Mr Francis had independent financial authority at the appropriate time. The HCSEC team, led by the HCSEC Technical Director and supported by the rest of the HCSEC senior team, also effectively worked to ensure a smooth handover. Work was undertaken to minimize the impact of Mr Pollington's departure. As the Huawei European Cyber Security Officer, Mr Francis's existing understanding of the work of HCSEC and relationships with the UK operators was helpful in minimizing the effects of the transition. The process for bringing the new MD on board was judged by the Oversight Board to be successful.

2.5 The NCSC, having subsumed GCHQ's role 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 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.

2.6 Staffing at HCSEC has increased in line with expectations for the year 2016. By the end of the calendar year, the staff numbers were almost as predicted with only one position not filled (taking 'offer accepted' as the point of employment). This excellent progress has been driven by the personal involvement of HCSEC leadership and represents a significant amount of work.

2.7 It is likely that staff numbers will need to further increase in 2017 to accommodate the binary equivalence work and the underpinning infrastructure and tooling to manage that going forward, as discussed in Section III. However, these new posts are likely to require more general software engineering skills, rather than deep cyber security knowledge. It remains critical that HCSEC continues to recruit technical cyber security specialists to manage attrition and succession.

2.8 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 In the 2016 Oversight Board report, mention was made of the search for new accommodation for HCSEC. That search was successfully concluded in October 2016 and the Heads of Terms agreement is in process with the new landlord at the time of writing and expected to be signed in April. There is one remaining issue to be

resolved with respect to power in the building. Huawei HQ has approved the budget for the new building, including fit out, and the increased space allows for significant expansion of HCSEC's operations. There have been some unforeseen delays in the process of HCSEC taking on the building, due to negotiations with the landlord. These delays are not in any way the result of Huawei HQ's inaction or interference.

2.10 The increased scope of operation allows 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 2016. Quarterly monitoring by the Oversight Board has shown no causes for concern in the number of staff and their skills, but has uncovered a slight delay in the procurement of the new accommodation. This has not yet affected the delivery of HCSEC's plan in support of the UK Government's risk management strategy and we believe that much of that time can be made up during build.

~~~~~
~~~~~

Section III: HCSEC Technical Assurance

2016 is the sixth year of the Government's extended risk management programme for Huawei's involvement in the UK telecommunications market. Last year, 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 two reports. The Oversight Board's intent is to provide detailed technical assessment only periodically and when issues specifically warrant it.

Evaluation Process

3.1 HCSEC's assessment programme in 2016 continued the product and solution evaluation split which proved successful in 2015. In 2016, twenty product and four solution evaluations were performed, covering products and architectures for five UK operators.

3.2 There were issues with one of the solution evaluations, namely the SMSC solution. This solution contains an early implementation of a virtualisation technology and could not be configured in HCSEC in a way that matched the operator's intended deployment. There were also significant delays in the operator's deployment timeline and debate around precisely which version the operator wished to deploy. By mutual agreement between HCSEC and Huawei R&D, the solution evaluation was abandoned in favour of a lightweight threat assessment and a product evaluation on one sub-component. The operator chose to deploy the solution regardless, with an expectation that they would upgrade to the next version which will be evaluated by HCSEC. This is ongoing.

3.3 The NCSC has a stated intent of 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, with a small recruitment deficit in the evaluation staff that needs to be overcome to achieve this in a sustainable way. There is a dependency on the lab system build team which will need to grow in order to sustain the pipeline of work, by ensuring that representative systems are available when needed.

3.4 During 2016, the NCSC has organized regular technical discussions related to security evaluation among NCSC, HCSEC and seven UK operators. An initial area of focus is the new single Huawei MVNO (mobile virtual network operator) platform which, in the opinion of the NCSC, requires specific risk management due to the extensive use of Huawei Radio Access Network equipment in the UK operators. The risks would be broadly similar for any vendor which provided both significant radio access network equipment and the underpinning MVNO platform. The combined risks are likely greater than the individual ones and mainly pertain to the host operator's network, rather than individual MVNO participant networks.

3.5 HCSEC were able to decide to attend these technical security discussions without reference to Huawei HQ and could provide expert advice to the group, as requested by the NCSC, again without reference to Huawei HQ. This shows a level of independence from Huawei HQ, as anticipated and expected by the Oversight Board.

3.6 Significant effort was expended in 2016 by HCSEC, under NCSC direction, to fully understand the potential configuration management issues raised in last year's Oversight Board report. This has had a transitory effect on the number of evaluations performed, as detailed later in this report.

Prioritisation and programme build

3.7 The risk based prioritisation scheme detailed in the previous Oversight Board report has continued to be applied during 2016.

3.8 As the proportion of Huawei equipment into the UK operators is broadly stable, little has changed in terms of high level prioritisation of equipment.

3.9 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 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.

Configuration Management and Binary Equivalence

3.10 The previous Oversight Board report spoke to the difficulty of achieving binary equivalence – that is the process of assuring that the source code received and analysed by HCSEC is uniquely that used to build the binaries present in the network elements operated by the UK operators. Part of the issue was the inability for HCSEC to consistently and easily reproduce a full product binary from the received source code.

3.11 Under NCSC direction, HCSEC performed a focused set of works to understand the root cause of the inability to reproduce binaries from the source provided.

3.12 The result of this work was twofold. Firstly, it produced evidence of the variable engineering quality and repeatability of the underlying build process. While this appears to be different for each product group, on average the build processes are not conducive to the repeatable, deterministic production of binaries. Huawei HQ have accepted that work needs to be done to make the build process repeatable, of consistent quality and with end-to-end integrity, in order to support the binary equivalence requirements.

3.13 Secondly, the work proved the fact that the source code delivery process in Huawei HQ was inconsistent across operator versions and releases. For clarity, the delivery team in Huawei HQ had been extracting a subset of source code from the configuration managed repositories for onward delivery to HCSEC. Further discussion with Huawei HQ showed that the process limited the source code delivery to that for features procured by the UK operators, this being a subset of the code required to build the binary installed on the network elements.

3.14 While this process explains the technical artefacts that have been observed over the last two years, it also means that the work of HCSEC has provided less than ideal assurance to the operators, as part of their risk management regimes. The incomplete delivery of source code obviously means that HCSEC cannot provide

assurance or risk management artefacts for the additional code. While this is a matter of significant concern, the NCSC does not believe this process is in any way malicious, but is based solely on Huawei supplying source code for the features procured and used by UK operators. This opinion is based on a targeted analysis of previously received source code and corresponding binary.

3.15 Regardless, Huawei HQ, NCSC, HCSEC and the UK operators have agreed a timetable for the redelivery of complete source code and analysis of the differences. Based on an initial analysis, which suggests that the additional code is for features not procured by UK operators (despite being present in the installed binary), the NCSC does not believe that this will show any detriment to UK national security. However, we cannot be sure until the entire codebase is redelivered in full and analysis performed. The redelivery process is intended to be complete by December 2017 and is staged according to the risk the specific products attract. The source code for the most risky and potentially impactful products (as defined by the HCSEC risk mapping) will be redelivered first. Subsequent analysis will determine whether any national security risks have been admitted by previous processes, although NCSC currently believe this is unlikely.

3.16 Importantly, this agreement has also rescoped 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. The NCSC believes this is a more sustainable arrangement requiring a smaller uplift in resources in HCSEC while maintaining sufficient independence, scope and oversight for HCSEC to provide the NCSC and the operators appropriate assurance. The NCSC and the Oversight Board will be reviewing the updated arrangements regularly to ensure they perform optimally in the context of the UK's enhanced risk management regime.

Issue Resolution and Communication

3.17 The 2015 Oversight Board report spoke to the importance of the relationship between HCSEC and Huawei R&D and PSIRT in China for the management and resolution of issues.

3.18 HCSEC has traditionally had a very strong relationship with the wider Huawei R&D teams, this having been built over a number of years. The recent work around binary equivalence and the source code delivery process has been difficult for all concerned, due to misunderstandings between the teams involved around the complex and subtle technical issues.

3.19 However, all teams involved now have a common view of the issues and there is an agreed way forward for the work. The fact that this agreement is in place is testament to the strength of the relationship between HCSEC and the wider Huawei R&D teams and we expect the relationship between the teams to recover fully.

Summary of NCSC Technical Competence Review

3.20 The work of HCSEC in 2016 has further increased capability 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.

3.21 HCSEC continues to have world class security researchers who are creating new tools and techniques to provide assurance in the complex sphere of telecommunications. They are also creating repeatable, automated metrics which are used to inform the operators as to the general quality of - and engineering and security artefacts around - Huawei products.

3.22 The work conducted by HCSEC on the binary equivalence project shows that they are competent in the field to the level necessary to satisfy the Oversight Board requirements.

3.23 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

3.24 Overall, given this account of the technical assurance work of HCSEC to date, the NCSC has advised the Oversight Board that it is confident that HCSEC is providing technical assurance of sufficient scope and quality as to be appropriate for the current stage in the assurance framework around Huawei in the UK. Obviously, significant work is needed to provide assurance as to the completeness of redelivered source code and any potential impacts differences may have. The Oversight Board will be looking to HCSEC to continue to make progress on the analysis of the complete code and to advise the Oversight Board, the UK operators and the NCSC of any issues arising from that analysis. This may require a small uplift in personnel numbers to ensure that this is sustainable.

~~~~~
~~~~~

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 third 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 2016;
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 by December 2016;
iii. A final audit phase comprising the full year end audit, with the report presented to the NCSC, HCSEC and Huawei HQ in January 2017 and the full Oversight Board in March 2017.

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 2017 comprised a rigorous evidence-based review of HCSEC processes and procedures. The audit report was produced by a team of four DV cleared staff from Ernst & Young; the fieldwork was conducted by an experienced Manager and led by an Executive Director. 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 one 'Low' rated finding, the controls evaluated were considered to be effective as per the control description and agreed test procedures."

4.8 The audit report identified one control weakness within the HCSEC control environment for the Board to consider. The weakness was 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. However, although requested at the time by HCSEC, formal sign-off by the NCSC of the plan was not provided. Evidence of discussion (with Ian Levy) was available and retrospective confirmation of sign-off from the NCSC was made available during the Audit. Progress against the plan is discussed between the NCSC and HCSEC. Following review and agreement of the evaluation plan with the NCSC, HCSEC should ensure that they obtain a formal confirmation that the evaluation plan is fit for purpose and retain this in their records.

Advisory Notices

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

i. Maintain rigour in auditable information

4.12 It was observed during this year's work that there had been a general improvement in the quality of recorded information and the efficacy of the controls in place. However, in a few specific instances there are further improvements that could be made to the information recorded. Specific instances where the quality of auditable information could be further improved:

- Recording both contractors and permanent staff on the recruitment log (rather than just permanent hires);
- Recording information requests (RFIs) relating to research projects (such as BEP), and which are not subject to the Annual Management Audit separately to those pertaining to evaluation projects, which are subject to the Annual Management Audit;
- Ensuring that information relating to staff clearances is accurate and complete.

ii. Clearance outcome notification retained

4.13 When a new member of staff fails to obtain security clearance, the notification from the NCSC is not formally retained. In the year reviewed, three staff members failed to receive security clearance and so were dismissed. Although it was established through the audit process that staff were removed expediently, the lack of a formal record of the date on which the NCSC notified HCSEC that staff had failed to receive security clearance made it more difficult to validate the staff member being removed in a timely manner. HCSEC should ensure that the NCSC provides formal communication of decisions not to grant security clearance and that these are retained for audit purposes. The information retained would only need to show the

date on which HCSEC were notified and would not include any details as to why clearance was not granted[1].

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 May 2016.

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. Three issues – one low rated finding and two advisory issues – have been identified.

~~~~~

[1] For clarity, the reason to not granting a clearance is never shared outside the security vetting team; this is Personnel Security's standard practice and ensures the confidentiality of personal information is maintained.
~~~~~

SECTION V: Conclusions

5.1 The Oversight Board has now completed its third full year of work. Its four 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 third 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. Assurances are still required around binary equivalence but changes in resourcing should allow greater and more sustainable progress here.

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. 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 2016-2017, 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. Additionally, it is hoped that this report continues to add to Parliamentary – and through it, public – knowledge of the operation of the arrangements.

~~~~~
~~~~~

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 Executive Director
- HCSEC Managing Director
- Cabinet Office Director, CGSD
- Cabinet Office Deputy Director, CGSD
- NCSC Technical Director
- Whitehall Departmental representatives: (Deputy Director, Head of Telecoms Security & Resilience and Business Intelligence Unit, DCMS, Director of the Office for security and Counter Terrorism, Home Office)
- Current CSP representatives: BT CEO Security; Director Group External Affairs, 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[2]. 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.

[2] 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 2015-2016 Audit and current status

The 2016-2017 Audit reviewed progress against addressing the following four issues that were highlighted in the 2015-2016 report. All issues were rated as "Low".

i. Baseline evaluation plan is not formally signed off by the Oversight Board

The Oversight Board agreed that GCHQ (now NCSC) would sign off the evaluation plan, mainly due to the potential commercial issues of presenting the full plan with industry members present.

ii. Requests for Information (RFI) returned outside of the specified Service Level Agreement (SLA)

The RFI process was updated as described in the previous audit and no exceptions were raised in the subsequent operation.

iii. HCSEC MD Bonus is set at the discretion of the Huawei UK CEO

In response to last year's issue the MD's Bonus is now associated with a set of KPIs which were discussed as part of the audit and will also be included in the scope of next year's review. It has also been a recognised risk since the establishment of HCSEC and the Oversight Board continue to accept this as reasonable. The Risk and Control Matrix was updated to reflect this agreement and so there were no audit findings reported this year.

iv. CESG PGP key was not operational for a period of approximately 4.5 months preventing direct electronic receipt of evaluation reports

Internal processes were updated to ensure this issue does not recur.

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