HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD

ANNUAL REPORT

2019

A report to the National Security Adviser of the United Kingdom

March 2019

HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD ANNUAL REPORT

Part I: Summary

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

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

3. The HCSEC Oversight Board, established in 2014, is chaired by Ciaran Martin, the Chief Executive Officer of the NCSC, and an executive member of GCHQ's Board with responsibility for cyber security. The Oversight Board continues to include a senior executive from Huawei as Deputy Chair, as well as senior representatives from across Government and the UK telecommunications sector. The structure of the Oversight Board has not changed significantly, but membership has changed in 2018. Mainly, this is due to staff rotations in both HMG and Huawei positions.

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

    i. **New secure premises for HCSEC completed** - the previously reported acquisition of new premises for HCSEC had experienced some commercial delays, but has now completed successfully and the new facilities are fully operational;

    ii. **The NCSC Technical Competence Review found that the capability of HCSEC has improved in 2018**, and the quality of staff has not diminished, meaning that technical work relevant to the overall mitigation strategy can be performed at scale and with high quality;

    iii. **The fifth 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, relating to delivery of information and equipment within agreed Service Level Agreements. Ernst & Young concluded that there were no major concerns and the Oversight Board is satisfied that HCSEC is operating in line with the 2010 arrangements between HMG and the company;

    iv. **Further significant technical issues have been identified in Huawei's engineering processes,** leading to new risks in the UK telecommunications networks;

    v. **No material progress has been made by Huawei in the remediation of the issues reported last year,** making it inappropriate to change the level of assurance from last year or to make any comment on potential future levels of assurance.

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

i. In 2018, **HCSEC fulfilled its obligations** in respect of the provision of software engineering and cyber security assurance artefacts to the NCSC and the UK operators as part of the strategy to manage risks to UK national security from Huawei's involvement in the UK's critical networks;

ii. However, as reported in 2018, **HCSEC's work has continued to identify concerning issues in Huawei's approach to software development** bringing significantly increased risk to UK operators, which requires ongoing management and mitigation;

iii. **No material progress** has been made on the issues raised in the previous 2018 report;

iv. The Oversight Board continues to be able to provide **only limited assurance** that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK;

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

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

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

This page is intentionally left blank

HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD 2018 ANNUAL REPORT

Part II: Technical and Operational Report

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

Introduction

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

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

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 fifth 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 2018 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 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 as part of the overall mitigation strategy in place to manage the risks presented by Huawei's presence in the UK and to advise the National Security Adviser on that basis. The National Security Adviser will then provide assurance to Ministers, Parliament and ultimately the general public as to whether the risks are being well managed.

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

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

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 remit and objectives of the Oversight Board remain unchanged. The Oversight Board is responsible for providing an annual report to the National Security Adviser, who will provide copies to the National Security Council and the Intelligence and Security Committee of Parliament (ISC).

The Board's objectives for HCSEC

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 software engineering and cyber security competence.

The HCSEC Oversight Board: Business April 2018-February 2019

1.6 This report covers the technical work undertaken from January 2018 until December 2018. The Oversight Board meeting in March 2018 was covered in the previous report. In its five meetings since the publication of the 2018 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 a detailed report on technical visits to Huawei HQ in Shenzhen and Shanghai by the NCSC Technical Director and technical team, some with UK operators, to discuss technical issues;
- Taken further evidence around the root causes of the significant software engineering and cyber security problems that came to light last year;
- Taken further evidence on Huawei's proposed remediation for the significant software engineering and cyber security problems, and judged them to be inadequate;
- Commissioned a fifth 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 The NCSC leads for HMG in dealing with HCSEC and the company more generally on technical security matters. The NCSC, on behalf of HMG, sponsors the security clearances of HCSEC's staff. The general requirement is that all staff must have Developed Vetting (DV) security clearance, which is the same level required in Government to have frequent, uncontrolled access to classified information and is mandatory for members of the intelligence services. New recruits to HCSEC are managed under escort during probation pending completion of their DV clearance period, which is typically six months.

2.3 Staffing at HCSEC has increased in line with expectations for the year 2018. By the end of the calendar year, staff numbers were 38 (taking 'offer accepted' as the point of employment).

2.4 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.

2.5 Once again, this year a significant number of potential recruits were sifted out due to clearance requirements. Furthermore, one candidate that passed initial sifting and was employed by HCSEC subsequently failed DV clearance and was removed from the centre. The small risk associated with this person was adequately managed through the supervision and oversight provided during their probationary employment period.

Accommodation

2.6 The previous report spoke of a successful search for new accommodation for HCSEC to cope with the required expansion, but also of delays in its completion. 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 was successfully concluded this year. All HCSEC staff transitioned to the new facility and IT and representative customer networks were installed by November 2018. The incurred delays were not in any way the result of Huawei HQ's inaction or interference.

2.7 The new facility has been designed to accommodate securely the sensitive work that HCSEC undertakes, whilst also ensuring that Huawei intellectual property protection standards are addressed. The building has been assessed as sufficiently secure by HMG security teams and has also gained accreditation by Huawei HQ teams for its suitability to hold all Huawei source code.

2.8 The new accommodation will support the deployment of concurrent reference networks, allowing both product and solution evaluations to proceed at pace. It also facilitates increased development activity to support the significant number of products needing assessment.

2.9 It should be noted that HCSEC's 2018 budget is 160% of the 2017 budget, although a proportion of this is related to moving costs and other one-off charges.

2.10 Overall, good progress has been made on accommodation, staffing and skills during 2018. Quarterly monitoring by the Oversight Board has shown no cause for concern in the number of staff and their skills. The delay to the new accommodation is unfortunate but the move has been completed successfully with no significant impact on the work of HCSEC.

~~~~~
~~~~~

Section III(a): HCSEC Technical Assurance

3.1 2018 is the fifteenth year of the Government's active management of Huawei's presence in the UK's telecommunications networks, the eighth year of the Government's extended risk management programme for Huawei in the UK and the fifth year of the Oversight Board. In the previous four reports, the Oversight Board included some of the underlying technical detail concerning the results of evaluations conducted of Huawei products that year. This was necessary to enable the Board to provide clear and comprehensive assurance to the National Security Adviser. This report, covering Oversight Board activities between March 2018 and February 2019 but reporting on technical work between January 2018 and December 2018, updates the technical position laid out in the previous reports and, where necessary, elaborates further in order to explain the conclusions the Oversight Board has reached on technical assurance and HCSEC effectiveness, as well as its views on how the risks identified can be mitigated in the future. The Oversight Board considers it necessary to provide the technical detail contained in this report in order to fulfil its reporting function. In particular, the Oversight Board considers that provision of this detail is necessary to explain and substantiate its decision to reduce the level of assurance compared to previous years and also to help those operators not currently represented on the Oversight Board to understand the risks they may face in their networks. This section comprises NCSC's report to the Oversight Board and is split into two parts. The first provides an overview of the work performed by HCSEC and the high-level findings taken from this, along with conclusions about the technical assurance and HCSEC's effectiveness. The second part provides detailed technical information intended to help readers understand why the conclusions here have been reached.

HCSEC Evaluation Process

3.2 HCSEC's assessment programme in 2018 continued the product and solution evaluation split of recent years. In 2018, 39 product evaluations were completed, and 3 solution evaluations were completed, with another scheduled to finish in early 2019. Overall, this is broadly as per the programme agreed at the start of the year. The evaluations covered products and architectures for five UK operators. This tempo was

maintained despite the inclusion of significant amounts of non-evaluation work in support of Oversight Board actions and the move to new premises.

3.3 The NCSC has a stated objective of requiring HCSEC to perform a product evaluation on every relevant product in the UK at least every two years which is, on average, being met. HCSEC's product evaluation pipeline remains configured to achieve this. The Oversight Board is confident that continued attention from HCSEC seniors will ensure that there are sufficient appropriately skilled staff to continue to meet the NCSC objective. HCSEC staff must be capable of achieving security clearance and have the requisite skills, meaning the pool of available talent is small. HCSEC's move to new premises will help service the evaluation pipeline as there is sufficient space and infrastructure to maintain multiple representative networks concurrently, removing much of the tear down and build up time for evaluation work.

3.4 The evaluation process continues to uncover both point vulnerabilities and more strategic architectural and process issues, as detailed later in this section. Huawei continues with their remediation work; the feedback provided by HCSEC to UK operators, NCSC and 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.

HCSEC Programme Build and Prioritisation

3.5 The risk-based prioritisation scheme detailed in previous Oversight Board reports has continued to be applied during 2018.

The programme build process remains broadly the same as in previous years. The UK operators, NCSC and HCSEC set priorities for HCSEC collaboratively. This is necessary to balance the sometimes competing constraints and requirements to achieve the best overall benefit for the UK, for example not allowing any particular operator to unfairly 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 light-touch process involving the NCSC and the relevant operators is used to manage and approve any modifications. As well as servicing the

evaluation pipeline, HCSEC has done significant work in support of the Oversight Board's objective levied in the previous report to support Huawei R&D in its efforts to enhance Huawei's software engineering and cyber security competence and so begin to remedy the underlying issues identified in this and previous reports.

3.6 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, consistently meeting the expectations of NCSC and the UK operators. 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.

Overview of HCSEC Technical Work and High-Level Findings

3.7 Significant technical work has been done in 2018 by HCSEC and also by NCSC, which has undertaken the audit for the Oversight Board envisaged by paragraph 3.3 of the Terms of Reference. Details of that work are provided in the second half of this section, but the high-level conclusions and findings are provided here for convenience.

- Four products have been provided by Huawei to test binary equivalence. Work to validate them by HCSEC is still ongoing but has already exposed wider flaws in the underlying build process which need to be rectified before binary equivalence can be demonstrated at scale. The NCSC has advised the Oversight Board that the priority should be to rectify these underlying flaws as part of Huawei's transformation plan. Unless and until this is done it is not possible to be confident that the source code examined by HCSEC is precisely that used to build the binaries running in the UK networks.
- Due to various build-related issues, it is hard to be confident that different deployments of similar Huawei equipment are broadly equivalently secure. For example, it is difficult to be confident that vulnerabilities discovered in one build are remediated in another build through the normal operation of a sustained engineering process. The ability to do so, and the end-to-end assurance that

a particular source code set is precisely that used to build a particular binary would normally be satisfied as a side effect of a modern software engineering process.

- Huawei's configuration management improvements, which have been driven by the UK community since 2010, have not been universally applied across product and platform development groups or across configuration item types (source code, build tools, build scripts etc). Without good configuration management, there can be no end-to-end integrity in the products as delivered by Huawei, and limited confidence in Huawei's ability to understand the content of any given build or in their ability to perform true root cause analysis of identified issues.
- Huawei continues to use an old and soon-to-be out of mainstream support version of a well-known and widely used real time operating system supplied by a third party. Huawei has separately purchased a premium long-term support agreement from the vendor to address vulnerabilities in a commercially viable manner in the future, but the underlying cyber security risks brought about by the single memory space, single user context security model remain. NCSC believes there is currently no credible plan to reduce the risk in the UK of the use of this real time operating system. Huawei's own equivalent operating system is subject to many of the same Huawei development processes as other components and NCSC currently has insufficient evidence to make a judgement on the software engineering quality and cyber security implications of this component. Furthermore, it employs more modern memory and security models and so integration with the existing product running on the operating system brings risk. This means that moving to this real time operating system may not improve the situation long-term, while bringing integration risk to the UK operators. Work continues between Huawei, HCSEC, the UK operators and NCSC to develop a realistic plan to reduce the long-term risk in the UK networks due to the use of this old, third-party real time operating system. However, NCSC remains concerned about the time elapsed since discovery of this issue without a credible plan being presented.
- Analysis of Huawei's wider software component lifecycle management revealed flaws that cause significant cyber security and availability risks. This

is a significant finding and more detail is provided in the second part of this section. Remediation of the existing codebase where this is an issue and of the flawed processes that allowed it to happen systemically will require significant rectification.

- A software engineering and cyber security trend analysis was performed by HCSEC comparing subsequent major versions of the software for the LTE eNodeB. The later version was intended to incorporate all Huawei's improvements and therefore, on average, should have been objectively better than the previous version. While there were improvements, the general software engineering and cyber security quality of the product continues to demonstrate a significant number of major defects. The NCSC therefore remains concerned that Huawei's software engineering and cyber security competence and associated processes are failing to improve sufficiently.
- The Oversight Board tasked Huawei with providing a plan to remediate the software engineering and cyber security issues in the LTE eNodeB product development and sustained engineering, to be reviewed by NCSC with the support of the UK operators. The plan presented was unacceptable to NCSC and UK operators. The NCSC currently is not confident that Huawei is able to remediate the significant problems it faces.
- In response to the defects identified in its engineering processes Huawei presented to the Oversight Board its intent to transform its software engineering process through the investment of $2 billion over five years. However, this proposed investment, while welcome, is currently no more than a proposed initial budget for as yet unspecified activities. Although formal oversight of Huawei's global transformation plan does not fall within the scope of Oversight Board activities, the Board will wish to see details of the transformation plan and evidence of its impact on products being used in UK networks before it can be confident it will drive change. Unless and until a detailed plan has been provided and reviewed, it is not possible to offer any degree of confidence that the identified problems can be addressed by Huawei.
- HCSEC has continued to find serious vulnerabilities in the Huawei products examined. Several hundred vulnerabilities and issues were reported to UK

operators to inform their risk management and remediation in 2018. Some vulnerabilities identified in previous versions of products continue to exist.

Conclusion: HCSEC Competence

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

3.9 The work of HCSEC in 2018 has continued capability development in the underpinning tooling necessary to provide understanding and technical security artefacts to the UK operators and NCSC. Through 2018, HCSEC has continued to find issues in Huawei products, demonstrating their continued ability to discover weaknesses in the Huawei product set. Furthermore, 2018 has seen HCSEC expend significant effort in analysing Huawei R&D claims and effectively reverse engineering root cause issues out of an exceptionally complex and poorly controlled development and build process. This takes exceptional technical skill and insight.

3.10 HCSEC continues to have world-class security researchers who are creating new tools and techniques to provide the UK community understanding of the software engineering and cyber security implications of Huawei's unique software engineering and cyber security processes in the complex sphere of telecommunications.

3.11 In terms of core cyber security work, the number of vulnerabilities and issues reported to UK operators has risen to several hundred. Given the increase in the number of product evaluations performed in 2018 (39 over 27 in 2017) this number is broadly in line with previous years. Some serious vulnerabilities reported in previous evaluations continue to persist in newer versions.

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

errors, cryptographic weaknesses, default credentials and many other basic vulnerability types. Despite Huawei mandating application of its secure coding standards across R&D, extensive use of commercial static analysis tools and Huawei's insistence that risky code has been refactored, there has been little improvement in the objective software engineering and cyber security quality of the code delivered for assessment by HCSEC and onward to the UK operators.

3.13 The significant risk in the UK telecommunications infrastructure brought about by Huawei's equipment will continue to need to be managed by the UK operators and significant work will be required from all parties involved to reduce that risk in existing equipment over time. NCSC and the UK operators will continue to work with Huawei to create a credible and sustainable remediation plan for the equipment in the UK. Huawei has agreed that the remediation of the equipment in the UK is independent of any other work Huawei may do and will occur in a timely manner. The Oversight Board will judge the effectiveness of HCSEC's part in this as part of normal business. It is not clear that similar plans could be made for equipment new to the UK, as explained in this report.

3.14 These risks are not due to any issue with HCSEC's staffing and capabilities, which continue to be world-class. The Oversight Board will be looking to HCSEC to provide an independent view on any changes Huawei choose to make to their development process and to determine the efficacy of any software engineering and cyber security uplifts on the final products as deployed.

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

Conclusion: Implications for the UK National Security Risk

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

3.17 Given both the shortfalls in good software engineering and cyber security practice and the currently unknown trajectory of Huawei's R&D processes through their announced transformation plan, it is highly likely that security risk management of products that are new to the UK or new major releases of software for products currently in the UK will be more difficult. On the basis of the work already carried out by HCSEC, the NCSC considers it highly likely that there would be new software engineering and cyber security issues in products HCSEC has not yet examined.

3.18 Poor software engineering and cyber security processes lead to security and quality issues, including vulnerabilities. The number and severity of vulnerabilities discovered, along with architectural and build issues, by the relatively small team in HCSEC is a particular concern. If an attacker has knowledge of these vulnerabilities and sufficient access to exploit them, they may be able to affect the operation of the network, in some cases causing it to cease operating correctly. Other impacts could include being able to access user traffic or reconfiguration of the network elements. However, the architectural controls in place in most UK operators limit the ability of attackers to engender communication with any network elements not explicitly exposed to the public which, with other measures in place, makes exploitation of vulnerabilities harder. These architectural controls and the operational and security management of the networks by the UK operators will remain critically important in the

coming years to manage the residual risks caused by the engineering defects identified. These findings are about basic engineering competence and cyber security hygiene that give rise to vulnerabilities that are capable of being exploited by a range of actors. NCSC does not believe that the defects identified are a result of Chinese state interference.

Section III(b): Supporting Technical Evidence

Binary Equivalence and Software Consistency

3.19 It has always been part of the mitigation strategy to ensure that the source code examined by HCSEC is precisely that which is compiled to the binaries executing in UK network equipment. Without a process to show that the source code and build environments examined by HCSEC uniquely produce the binary deployed in the UK's networks, it is impossible to provide end-to-end assurance in the security and integrity of the products in use. Binary equivalence was seen to be an interim step to gaining that assurance in the face of Huawei's extremely complex build process. It is worth noting that the assurance of the source to binary link in no way confers an assurance on either engineering quality or security. The previous Oversight Board report detailed progress on the new process for achieving binary equivalence, that is being able to build a product from source in HCSEC to a binary equivalent to (not necessarily identical to) the General Availability (GA) version produced by Huawei R&D in China. In the previous report, it was recorded that a single product – a broadband head end – had successfully had a repeatable build created and deployment of this version was expected imminently. Unfortunately, no UK operator has been able to deploy this version due to version specific dependencies that cannot be satisfied in the UK deployments today.

3.20 The expectation set in the previous report was that the remaining three pilot products from the LTE, EPC and optical transmission product lines would have become commercially available, repeatable GA builds within the first half of 2018. While binaries have been delivered by Huawei R&D over the course of the year and marked as GA by Huawei, the separate validation work by HCSEC has not completed. The validation work on the EPC product was just beginning at the end of 2018 and the optical transmission product has been rescheduled to begin in 2019. As with all HCSEC programme changes, these were agreed with NCSC on behalf of the Oversight Board.

3.21 HCSEC was tasked with understanding the issues confronting Huawei in creating repeatable builds. The issue in all cases is with Huawei's underlying build process which provides no end-to-end integrity, no good configuration management,

no lifecycle management of software components across versions, use of deprecated and out of support tool chains (some of which are non-deterministic) and poor hygiene in the build environments, many of which cannot be easily recreated by HCSEC. It is unclear whether there is any utility in continuing the binary equivalence programme given the fundamental issues in the underlying build process and the customer management and engineering processes that drive it. HCSEC and NCSC have agreed that effort would be better expended in re-engineering the build process from scratch, as part of a wider software engineering and cyber security transformation. It remains 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, as is usual with a well-managed software engineering process. The recent work with the four pilot products demonstrates that this is currently impractical at any useful scale given Huawei's current build process. The NCSC has advised the Oversight Board that it will only be possible to offer limited assurance for equipment currently deployed in the UK unless and until the build process has fundamentally changed.

3.22 There remain concerns among the UK operator community about the consistency of similarly versioned software as delivered by Huawei. In some cases, builds are tested in operator intended final configuration – which are supplied by operators – before release by Huawei. While this improves reliability in the intended configuration, it may mask the serious issues detailed in this report which will affect network performance when the configurations are perturbed, or vulnerabilities exploited, causing security or availability impacts on the networks. True consistency across operators requires the issues in this report to be remediated.

Configuration Management

3.23 As detailed in the 2018 report, the Oversight Board and NCSC asked Huawei R&D to do more of the mandraulic work required by the binary equivalence programme, with HCSEC moving to a role where it provided validation. As this work progressed, more and more unexpected artefacts were produced by the R&D team. HCSEC were asked to perform an analysis to expose the underlying systemic issues that led to the problems encountered. They discovered the following defects:

- Configuration management of virtual machines used during the build process is poor. Specifically, virtual machines were not clean at build start, with many containing (sometimes irrelevant) source code, artefacts of previous builds and other detritus.
- Configuration management of the build environment – including toolchains – is poor and sometimes non-existent. Tools are installed multiple times in a build environment, or in environments where they are not needed. Many tools are significantly out of support and have undesirable properties, for example non-deterministic compilation or optimization based on environment variable values.
- Configuration management of source code is poor. This manifests in two broad areas. Firstly, configuration management is not applied consistently between development teams. Product code is managed differently to platform code and both are managed differently to third-party components. Secondly, the integration into the overall product architecture is very poor, with multiple copies and versions of components, apparently identically versioned components containing significant differences, circular dependencies between components and some components regressing in version between overall product increments.

3.24 NCSC (then CESG) first demanded proper configuration management from Huawei in 2010 and the company has been investing in the process since then, with earlier Oversight Board reports detailing Huawei's work in this area. However, artefacts have been discovered as a result of the various technical work undertaken during the intervening time suggesting that this roll out has not been consistent across the company and that configuration items have not been rationalised during the work. In 2016, HCSEC wrote a report outlining many of these issues in response to an NCSC request, but these findings were rejected by Huawei at the time. From the subsequent work done by HCSEC and NCSC under the auspices of the Oversight Board, it is now clear that the issues identified in the 2016 report remain and are systemic across the product lines in the company. As a result of these issues, the NCSC has advised the Oversight Board that, at present, there is no end-to-end integrity in the products as delivered by Huawei, and limited confidence in Huawei's ability to understand the

content of any given build or in their ability to perform true root cause analysis of identified issues.

Third-Party Component Support Issue

3.25 Significant effort has been invested by all parties in fully understanding the issue raised in the previous report about support for a particular third-party software component. This issue relates to various old and soon-to-be out of mainstream support versions of a widely used third-party real time operating system, which Huawei has chosen to continue to use within products whose end of life date is significantly longer. Continuing to use products which rely on old software components (including but not limited to the operating system) attracts risk for operators. Furthermore, the operating system in question is based on a single memory space, single user model (as was prevalent at its time of design), which further increases risk as a single vulnerability in any process running under this operating system is sufficient to allow compromise of any component running in the same operating system instance. Huawei has purchased a separate premium long-term support agreement from the vendor to address vulnerabilities in a commercially viable manner in the future, but the underlying cyber security risks brought about by the single memory space, single user context security model remain. It is industry good practice to keep components up to date and to upgrade versions in line with vendor releases. The Oversight Board and UK operators have made it clear that long-term reliance on this operating system in the UK is unacceptable and an upgrade path must be created. At the time of writing, NCSC has not seen a credible plan from Huawei for the mitigation of this issue and an upgrade path to a supportable operating system with a security model appropriate for a modern carrier-grade telecommunications system. Operators will continue to have to do extraordinary work to mitigate the ongoing risk until a credible plan is enacted.

Wider Component and Lifecycle Management Issue

3.26 At the June 2018 Oversight Board meeting, held at Huawei's facility in Shanghai, a technical follow up day was added to the end of the meeting to better understand the wider component and lifecycle management strategy, including the operating system issue detailed above.

3.27 The first piece of work was around Huawei's intent to move off the operating system that is soon-to-be out of mainline support to their own real time operating system, based on the open source Linux kernel. Following its review in Shanghai the NCSC concluded that it did not have sufficient evidence to be confident in the long-term sustained engineering of Huawei's own real time operating system. There are integration risks with the existing application code being ported to a more modern operating system memory and security model. This gives rise to a cross-operator risk which needs careful attention to remediate, especially as new hardware may be required in some cases. Work needs to be done to weigh the known risks of a dated operating system with the risks of a change to a different operating system and all that entails. This is an extremely difficult position for operators. More detail is presented later.

3.28 The second piece of work was to determine whether the wider component and lifecycle management showed similar issues. Since the Oversight Board meeting was held in Shanghai, it was possible to have engineers present to perform actions on the live development systems to show real-time evidence. Huawei presented the intended process and some high-level evidence to show it was being followed. NCSC then selected a commonly used component, the OpenSSL library, and specific queries were performed on the Huawei development database. This showed that there were an unmanageable number of versions of OpenSSL permitted to be used in products, including versions that are not on the main development train, that have known vulnerabilities and that are unsupported. The conclusion reported back to the Oversight Board is that Huawei's basic engineering process does not correctly manage either component usage or the lifecycle sustainment issues, leaving products unsupportable in general.

3.29 The Oversight Board made clear at the September meeting that this was unacceptable and reiterated the demand that had been made over the previous 12 months for Huawei to fundamentally transform its software engineering and cyber security processes.

Improvement Testing on LTE eNodeB

3.30 At the June 2018 Oversight Board meeting, held at Huawei's facility in Shanghai, HCSEC was tasked with performing an analysis of the software engineering and cyber security quality change between two versions of the LTE eNodeB. Under Huawei's planned implementation, the improvement process being carried out was intended to be generally embedded around the time the later release was code complete. Delivery of this report to NCSC was deferred in order to give time for Huawei to provide an improvement plan but was requested by NCSC at the September board meeting due to a lack of progress in identifying underlying root causes or moves to change the development process.

3.31 It would have been unrealistic to expect the later version of the software to be flawless, but NCSC hoped to see a broad and consistent improvement. The review revealed that code duplication has been reduced significantly between the two versions and there was a significant reduction in the number of copies of one open source component. Unfortunately, the general software engineering and cyber security quality of the product continues to demonstrate a significant number of major defects:

- Extensive non-adherence to basic secure coding practices, including Huawei's own internal standard, mandated since 2013, making vulnerabilities much more likely. The extent of this had reduced between versions but remained a cause for concern;
- Extensive incorrect use of safe memory manipulation functions, significantly increasing the likelihood of memory safety vulnerabilities. The extent of this had reduced between versions but remained a cause for concern;
- Extensive misuse of signed/unsigned typing and casting to different variable sizes when performing arithmetic operations including on bounds calculations, significantly increasing the likelihood of integer overflow and underflow vulnerabilities and associated buffer sizing vulnerabilities;
- Poor management of software component imports, making supportability and lifecycle security very difficult;
- Inappropriate suppression of warnings from static analysis tools, potentially hiding vulnerabilities;

- Extensive use of inherently insecure and prohibited memory manipulation functions, further increasing the likelihood of memory safety vulnerabilities. The extent of this had reduced between versions but remained a cause for concern;
- Unmanageable build process, including toolchains that are out of date.

3.32 Two specific examples, taken from the extensive report, illustrate the scale of the issues discovered.

3.33 The report analysed the use of the commonly used and well maintained open source component OpenSSL. OpenSSL is often security critical and processes untrusted data from the network and so it is important that the component is kept up to date. In the first version of the software, there were 70 full copies of 4 different OpenSSL versions, ranging from 0.9.8 to 1.0.2k (including one from a vendor SDK) with partial copies of 14 versions, ranging from 0.9.7d to 1.0.2k, those partial copies numbering 304. Fragments of 10 versions, ranging from 0.9.6 to 1.0.2k, were also found across the codebase, with these normally being small sets of files that had been copied to import some particular functionality. There were also a large number of files, again spread across the codebase, that had started life in the OpenSSL library and had been modified by Huawei.

3.34 In the later version, there were only 6 copies of 2 different OpenSSL versions, with 5 being 1.0.2k and one fork from a vendor SDK. There remained 17 partial copies of 3 versions, ranging from 0.9.7d to 1.0.2k. The fragments from the 10 different versions of OpenSSL remained across the codebase as do the OpenSSL derived files that have been modified by Huawei. More worryingly, the later version appears to contain code that is vulnerable to 10 publicly disclosed OpenSSL vulnerabilities, some dating back to 2006. This shows the lack of maintainability and security resulting from the poor configuration management, product architecture and component lifecycle management.

3.35 The report also analysed the adherence of the product to part of Huawei's own secure coding guidelines, namely safe memory handling functions. The binary image on one of the public-facing processing boards in the eNodeB was analysed for the use of direct invocation of memcpy()-like, strcpy()-like and sprintf()-like functions in their safe and unsafe variants. This board handles communication with untrusted interfaces

and it would be expected to be coded in a robust and defensive manner. This is especially true in this case because of the lack of operating system mitigations.

3.36 In summary:

- There were over 5000 direct invocations of 17 different safe memcpy()-like functions and over 600 direct invocations of 12 different unsafe memcpy()-like functions. Approximately 11% of the direct invocations of memcpy()-like functions are to unsafe variants.
- There were over 1400 direct invocations of 22 different safe strcpy()-like functions and over 400 direct invocations of 9 different unsafe strcpy()-like functions. Approximately 22% of the direct invocations of strcpy()-like functions are to unsafe variants.
- There were over 2000 direct invocations of 17 different safe sprintf()-like functions and almost 200 direct invocations of 12 different unsafe sprintf()-like functions. Approximately 9% of the direct invocations of sprintf()-like functions are to unsafe variants.

3.37 These numbers do not include any indirect invocation, such as through function pointers and the like. It is worth noting these unsafe functions are present in the binary and therefore pose real risk.

3.38 Analysis of relevant source code worryingly identified a number pre-processor directives of the form “#define SAFE_LIBRARY_memcpy(dest, destMax, src, count) memcpy(dest, src, count)”, which redefine a safe function to an unsafe one, effectively removing any benefit of the work done to remove the unsafe functions in the source code. There are also directives which force unsafe use of potentially safe functions, for example of the form “#define ANOTHER_MEMCPY(dest,src,size) memcpy_s((dest),(size),(src),(size))”.

3.39 This sort of redefinition makes it harder for developers to make good security choices and the job of any code auditor exceptionally hard. These are only examples, but show that Huawei’s own internal secure coding guidelines are not routinely followed in this product and, in some cases, developers may be actively working to hide bad coding practice rather than fix it.

3.40 This analysis in total shows that there remain significant issues to be addressed in Huawei's software engineering and cyber security development.

LTE Improvement Plan

3.41 At the September 2018 Oversight Board meeting, board members were becoming increasingly concerned about the lack of progress made by Huawei in remediating the basic issues discovered by HCSEC and NCSC. In particular, the lack of progress in creating a credible plan to mitigate the significant installed base of unsupportable software in the UK over the previous 12 months had become critical. In order to focus effort, the Oversight Board requested a plan to remediate a single product, eventually chosen to be the LTE eNodeB. Huawei were given until October 19th 2018 – subsequently extended to October 26th – to provide a credible plan for the remediation of the eNodeB. The intent was to ensure that discussion could be had between Huawei, HCSEC, the UK operators and NCSC and improvement made before the December Oversight Board meeting where the plan was to be discussed.

3.42 The majority of the document presented was a security analysis of the eNodeB functions, drawn mainly from NIST SP800-187. There was an acknowledgement of the problems that had been discovered by HCSEC and NCSC and some attempts to describe basic remediation, but the document mainly described Huawei's current processes and their intended outcomes, rather than the reality of what had been observed in the shipped products and the underlying root causes. A small section of the report was concerned with a plan for changes to be made to Huawei's development process. Unfortunately, the plan as delivered did not address the scale of the problem encountered and did not fundamentally address the underlying software engineering competence issue. Huawei were given another four weeks to present a plan at a meeting with NCSC and the UK operators. The Huawei presentation at that meeting showed that no substantive progress had been made. At the time of writing, NCSC has seen no credible plan from Huawei for remediation of the eNodeB or any other Huawei product in use in the UK.

Huawei Transformation

3.43 After the meeting to discuss the LTE eNodeB improvement plan, NCSC wrote to Huawei on behalf of the Oversight Board once again seeking a credible plan for both tactical remediation of the products already deployed in the UK and for a wider transformation programme that would make recurrence of these issues less likely in the future. NCSC made clear that without such a plan, there could be no long-term confidence in Huawei's technology or Huawei's ability to support operators in its secure use long-term.

3.44 Huawei accepted the criticism of their software engineering and cyber security processes and promised to invest $2 billion over five years in a company-wide transformation that will contain and mitigate the concerns raised by the Oversight Board. Clearly, any such investment must be supported by a plan which includes measurable outcomes. Although formal oversight of Huawei's global transformation plan does not fall within the scope of the Oversight Board activities and it does not expect to report on wider matters that do not relate to UK cyber security risk, the Board will wish to see sufficient details of Huawei's transformation of its software engineering and cyber security processes to enable it to assess to the extent to which they effectively contain and mitigate the risks it has identified. Sustained evidence of its impact on the products being used in the UK will be required before the Board can reassess its level of assurance, especially given the threat environment and increasing complexity of the technology involved. In the meantime, NCSC will advise the Oversight Board that it can continue to provide only limited assurance in the security of the currently deployed equipment in the UK. NCSC and the UK operators will continue to work with Huawei to create a credible and sustainable remediation plan for the equipment in the UK, independent of any wider Huawei transformation. In extremis, NCSC could direct Huawei as to how to remediate the specific products already in the UK infrastructure outside of Huawei's normal development and support process, allowing for a reduction in the risk present in the UK to a more reasonable level. This is not a sustainable response and only a good practice software engineering and cyber security development process could provide the basis of assurance in the future.

3.45 Importantly, NCSC cannot currently predict the likely technical construction and characteristics of Huawei's future products, created during and after the

transformation. Furthermore, given that Huawei's development process is inconsistent across product groups, NCSC cannot assume that findings from the product portfolio in use in the UK translate to other products. The UK's mitigation strategy for the use of Huawei equipment in the UK telecommunication sector, of which HCSEC and the Oversight Board is one part, expects industry good practice software engineering and cyber security development and support processes as a basis. Huawei currently does not meet that basic expectation. As a result of the operation of HCSEC, the UK operators and NCSC have significant, detailed knowledge of the risks arising out of the currently deployed Huawei equipment. Significant new equipment where the same level of detail is not available and assumptions based on existing knowledge cannot be reused (due to inconsistent development practices), will make that risk management harder.

3.46 Given the scale of the issues, significant and sustained evidence of improvement across multiple versions and multiple products will be necessary to begin to build confidence in Huawei's software engineering and cyber security quality and development processes. A single 'good' build will provide no confidence in the long-term security and sustainability of the product in the real world. Huawei's public statements about their transformation plan state that it will take five years. NCSC's Technical Director considers that this is broadly in line with a best-case estimate. The Oversight Board acknowledges that when it comes to reporting progress on matters relating to UK cybersecurity risk in future annual reports it will continue to take into account any representations from Huawei that particular matters are commercially sensitive and/or do not relate to UK cybersecurity risk. It will continue to pay due regard to any such representations provided always that it is able to properly discharge its obligations to report on risks to UK cybersecurity as required by its terms of reference included in Appendix A.

~~~~~
~~~~~

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 fifth 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. The independent audit does not seek to comment on the quality of any technical work – from either HCSEC or Huawei HQ – and detailed technical findings are not relevant to the independence of operation of HCSEC. This section provides an account of the process by which the audit took place, and a summary of the key findings.

Appointing Ernst & Young as auditors

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 2018;
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 2018;

iii. A final audit phase comprising the full year end audit during December 2018, with the report presented in January 2019.

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 2019 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 a Senior Manager. A Partner with Internal Audit subject matter knowledge acted as quality reviewer, and a second review of the final report was performed by an Ernst & Young Associate Partner.

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 [one finding 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"*

Control Weakness

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

i. RFIs returned outside SLA period

Requests for information made to Huawei were not always returned inside the stated SLA period, which is 12 weeks for hardware and 30 days for software source code. This was reported as an advisory recommendation in the previous audit but has continued into this year.

While there is some 'slack' in the HCSEC plan to accommodate late delivery, HCSEC RFIs should be updated to include a 'required by' date and any breach of delivery should be escalated.

Advisory Notices

4.9 Two advisory notices were also identified by the audit.

i. Review of progress against evaluation plan

4.10 A formal regular review of progress against the evaluation plan has not been continued this year. The review observed that regular SMT meetings were held in which any issues with evaluation progress could be raised, however the weekly evaluation progress report which has been completed in previous years has not been performed.

4.11 The regular reporting of evaluation status should be reinstated. This provides a record of the work of HCSEC and serves to highlight clearly any delays and their causes.

ii. **Rigour of auditable information**

4.12 Sample based testing identified a few instances where records had not been properly maintained – although in each case it was determined that the related control was still operating effectively. The review identified a purchase order that had been processed without all the correct approvals being recorded and some suppliers on the HCSEC supplier list incorrectly marked as inactive when active contracts were in place.

4.13 HCSEC's current processes should be rigorously followed.

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 2018.

Overall Oversight Board conclusions of the audit

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

~~~~~
~~~~~

SECTION V: Conclusions

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

5.2 The Oversight Board has concluded that in the year 2018, **HCSEC fulfilled its obligations** in respect of the provision of software engineering and cyber security assurance artefacts to the NCSC and the UK operators as part of the strategy to manage risks to UK national security from Huawei's involvement in the UK's critical networks.

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

5.4 No material progress has been made on the issues raised in the 2018 report and further issues have come to light in this year's report. **The Oversight Board continues to be able to provide only limited assurance** that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK. The Oversight Board notes in particular the following advice from NCSC:

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

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

iii. That although the review of subsequent major versions of the eNodeB showed improvements in code duplication and a significant reduction in the number of copies of the OpenSSL component, the general software engineering and cyber security quality of the product continues to demonstrate a significant number of major defects.

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

5.6 Huawei's transformation plan could in principle be successful, bringing Huawei's software engineering and cyber security processes up to current industry good practice. Huawei's own public estimates are that this transformation will take three to five years. The Oversight Board would require NCSC assessment of evidence of sustained change across multiple versions of multiple products in order to have confidence in success – a single version of a single product with better objective engineering quality and security does not guarantee a successful and sustainable change across the company, or even in that individual product group.

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

5.8 It should be made clear that the Oversight Board's statement of limited assurance is not a comment on the security of the UK's networks today, which is a matter for individual operators, Ofcom, DCMS and NCSC. It is assurance as to

whether HCSEC can continue to provide security relevant artefacts to inform UK stakeholders as part of the mitigation strategy. The oversight provided for in our mitigation strategy for Huawei's presence in the UK is arguably the toughest and most rigorous in the world. This report does not, therefore, suggest that the UK networks are more vulnerable than last year. Indeed, the significant technical insight provided by HCSEC to the UK operators allows them to plan more effective mitigations. The report from the Oversight Board states only that Huawei's development and support processes are not currently conducive to long-term security risk management and, at present, the Oversight Board has seen nothing to give confidence in Huawei's capacity to fix this.

5.9 These conclusions of the Oversight Board do not presage in any way the review of telecoms supply arrangements in the UK currently being carried out by DCMS on behalf of Government with the aim of ensuring there is an effective policy framework in place for the deployment of secure and resilient 5G and full fibre networks. DCMS has stated that the review will carefully consider the Oversight Board's findings and conclusions on technical assurance, alongside other evidence, in the development of policy. But the review will be based on a diverse set of evidence of which the Oversight Board conclusions are only a part.

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

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

~~~~~
~~~~~

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

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 9.

3.3 Commission Technical Competence Review

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

3.4 Process to Appoint Senior Management Team

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

3.5 Timely Delivery

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

3.6 Escalation / Arbitrator for issues impacting HCSEC

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

4. Oversight Board Membership

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

- 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 2017-2018 Audit and current status

The 2018-2019 Audit reviewed progress against addressing the following two issues and two advisories that were highlighted in the 2017-2018 report.

i. Request and Retain Evaluation Plan Sign-Off

The internal NCSC process was further strengthened to ensure appropriate formal sign-off of the evaluation plan. The 2018 Audit confirmed that the formal approval by NCSC of the HCSEC plan is retained.

ii. Budget setting and ongoing financial review

HCSEC internal processes were updated to address this issue. The 2018 audit confirmed that the HCSEC budget setting process is followed with formal sign-off from each SMT member recorded and retained.

iii. RFIs returned outside SLA period

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

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

HCSEC internal processes were updated to address this issue. The 2018 audit confirmed that regular budget monitoring has been performed with available evidence of monthly review.