HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD

ANNUAL REPORT

2016

A report to the National Security Adviser of the United Kingdom

May 2016

Huawei Cyber Security Evaluation Centre Oversight Board Annual Report

Part I: Summary

1. This is the second 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 2015, Huawei expanded to 170,000 employees globally and were assessed in mid-2015 by an independent consultancy as being on track to meet their 2013 commitment to invest and procure £1.3 billion into the UK economy.

2. HCSEC has been running for five 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. 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 was established in early 2014 on the recommendation of the UK National Security Adviser. Its role is to oversee and ensure the independence, competence and overall effectiveness of HCSEC. Its remit relates only to products that are relevant to UK national security risk. Since it was established, the Board has been chaired by Ciaran Martin, DG for Cyber Security at GCHQ. Its membership comprises senior executives from Huawei, including in the role of Deputy Chair, together with senior representatives from across Government and the UK telecommunications sector. The Oversight Board advises the National Security Adviser (to whom this report is formally 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 second 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 renewed effort on recruitment has been made.** HCSEC has significantly increased the use of recruitment agencies as well as the number of specialist agencies they use. They are also more actively tasking and managing them. Their current staff number 30 with Huawei providing budget for this to rise to 37 during 2016 which is sufficient to meet the 2016 plan. Huawei and HCSEC are looking at ways to help manage the assurance gap brought by the complex deployments in the UK. Recruitment of staff with top end cyber security skills remains challenging but progress is being made with more public engagement, for example through the Security Cleared Jobs Expo;

ii. **A new risk-based prioritisation and evaluation process has been introduced.** Four solution evaluations and ten product evaluations were conducted in 2015, tailored to actual UK deployments of Huawei equipment. Any non-UK evaluations undertaken in 2015 had no adverse effect on UK evaluations.

iii. **HCSEC's cybersecurity capability has continued to improve, finding subtler and more impactful issues**. Compared with 2014, the average number of issues per product has remained broadly static with the total number rising in line with the increased number of products assessed. The number of products assessed rose by 27% this year. The severity profile of these issues has changed, reflecting the improved capability. Three issues that HCSEC has discovered in this year required specific intervention in deployed CSP systems, and these were handled using standard processes between UK Government and CSPs. HCSEC has developed a new issue management system to better allow monitoring and tracking of software defects discovered during HCSEC's work and to enable resolutions to be

pursued with the Product Security Incident Response Team, who also use the tool;

iv. **The GCHQ Technical Competency Review found HCSEC to be a competent and effective organisation.** The review found a significant capability development programme, underpinned by novel cybersecurity research. This programme is kept under regular review by GCHQ and reported to the Oversight Board. This programme of work is core to HCSEC's capability in providing useful risk management information;

v. **HCSEC's Communication with, and influence of, Product Security Incident Response Team (PSIRT) has improved.** The important relationship between HCSEC and PSIRT has improved and is now judged by the Oversight Board to be effective. Issues raised in the first annual HCSEC OB report have been addressed to the satisfaction of the OB;

vi. **The second independent audit of HCSEC's operational independence from Huawei HQ has been completed.** The rigorous audit by Ernst and Young did not identify any high or medium priority findings. It did identify four low priority findings and made two advisory notes in relation to HCSEC cleaners and registration of HCSEC approved recruitment agencies. The Oversight Board believes that none of the findings had a material effect on the operation of HCSEC. The findings will be addressed during the course of 2016;

vii. **The search for better premises by HCSEC is ongoing and Huawei has approved a budget.** Whilst the current premises will not impact the operational capabilities of the centre in the short term, the lack of space available could potentially impact future product evaluations. HCSEC continue to explore a number of options in the Banbury area with the intent that the security of HCSEC's work is maintained.

5. The two key conclusions from the Board's second year of work are:

- The Oversight Board 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. Huawei and HCSEC are looking at ways to help manage the assurance gap brought by the complex deployments in the UK.

- The Oversight Board is satisfied that the Audit report has provided important external reassurance 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. The Audit has provided useful scrutiny of follow up on proposed enhancements to the wider governance environment, as highlighted during the 2014-2015 Audit despite being outside the formal scope.

6. Overall therefore, the Oversight Board concludes that in the year 2015-16 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 2016 Annual Report

Part II: Technical and Operational Report

This is the second annual report of the Huawei Cyber Security Evaluation Centre Oversight Board. The report contains 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 second 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 2015, Huawei expanded to 170,000 employees globally and were assessed in mid-2015 by an independent consultancy as being on track to meet their 2013 commitment to invest and procure £1.3 billion into the UK economy.

2. HCSEC has been running for five 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. 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, an executive member of GCHQ's Board with responsibility for cyber security. In March 2015, David Pollington joined HCSEC as its new Managing Director, taking over from Andrew Hopkins, a former senior manager at GCHQ. Mr Pollington took up his place on the Oversight Board the same month. The membership of the Oversight Board has remained broadly constant during 2015-2016 with the exception of the new Director OCSIA and Deputy Director OCSIA joining the Board. 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 second annual report has been agreed unanimously by the Oversight Board's members. As with last year's report, the OB 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, careers framework, recruitment and retention;
III. Section III covers HCSEC technical assurance, prioritisation and research and development;
IV. Section IV summarises the findings of the 2015-16 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, 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 GCHQ'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**. The main objective of the Oversight Board is to oversee and ensure the independence, competence and therefore overall effectiveness of HCSEC and to advise the National Security Adviser on that basis. 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 2015 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 enhance continually the security capability of Huawei.

The HCSEC Oversight Board: Business April 2015-March 2016

1.6 In its four meetings since the publication of the 2015 Annual Report, the Oversight Board has:

- Reviewed and approved the appointment of the new Managing Director of HCSEC;
- Provided regular corporate updates on Huawei UK, including highlighting three new appointments to their UK Board; Lord Browne of Madingley as an independent non-executive chair and Dame Helen Alexander and Sir Andrew Cahn as non-executive Directors of the Huawei UK 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 a technical visit to Huawei HQ in Shenzhen by GCHQ's Director for Cyber Security and Resilience (Technical) assessing the strategic effect of the work on the security of Huawei's products;
- Commissioned a second HCSEC management audit of the independence of the Centre.

SECTION II: HCSEC Staffing and Careers framework

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

Staffing and skills

2.2 A new Managing Director for HCSEC took office in March 2015 following the retirement of the incumbent MD, Andrew Hopkins. Odgers Berndston recruitment consultancy were appointed to run a process to find suitable candidates within a job specification drafted by Huawei and agreed with GCHQ. Three individuals were selected for interview by joint agreement between GCHQ and Huawei. An interview panel was convened in GCHQ's London office, chaired by Ciaran Martin, Director General for Cyber Security at GCHQ. He was accompanied by Dr Ian Levy, then Technical Director of GCHQ, and John Suffolk, Huawei's Global Cyber Security Officer (and a former Cabinet Office senior civil servant). The outgoing MD, Mr Hopkins, joined the panel in an advisory capacity at the invitation of the Chair.

2.3 David Pollington, formerly of Microsoft, won the competition. Mr Pollington is a renowned cyber security expert with extensive experience in the sector, most recently through twelve years at Microsoft, lately as Director for International Security Relations, Trustworthy Computing Security. Mr Pollington travelled to Shenzhen in January 2015 when his appointment was ratified by Huawei. The National Security Adviser was also formally notified of the competition outcome. Mr Pollington started at HCSEC on 2 March. In his previous work Mr Pollington has had extensive involvement with the Government on cyber security and as a result already held Developed Vetting clearance.

2.4 A significant transition period of six months was agreed to ensure a smooth handover between the outgoing and incoming MDs and to enable Mr Pollington to build essential effective relationships with UK Communications Services Providers. Active steps were taken to ensure the alignment of the Huawei probation period for the new MD with the necessary transition to new financial and management authorities. This included negotiation between GCHQ and Huawei to obtain sufficient

latitude in the corporate processes to allow the transition to proceed effectively, ensuring that Mr Pollington had independent financial authority at the appropriate time. This transition successfully completed in June 2015. The Ernst and Young Audit was deliberately extended to assure the Oversight Board of the effectiveness of the transition. The process for bringing the new MD on board was judged by the Oversight Board to be successful.

2.5 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 the company more generally on technical security matters. GCHQ, 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 during the timeframe of this report. April to November 2015 brought three resignations by staff, including one going to another cyber security job, demonstrating the value that is placed in the wider private sector on HCSEC training and experience. During the course of 2015, HCSEC has put renewed effort into improving its recruitment figures. The centre has expanded its use of recruitment agencies and is more actively tasking and managing them. It has also participated this year in the Security Cleared Jobs Expo in London, a free-to-attend event at which companies from across the country exhibit to attract potential interest in their posts. Interest in joining the Centre has remained high, but a rigorous application process coupled with the requirement to HCSEC staff to achieve DV clearance has resulted in a significant loss of applicants throughout the recruitment process. From April to December 2015, 359 applications for posts were received.

2.7 After sifting applications, 115 phone interviews were conducted resulting in 29 face to face interviews being held. This relatively high application rate resulted in 12 offers being made with nine accepted, one of whom declined just before joining. Of those applicants presented to HCSEC by the recruitment agencies, 67 failed to meet the up-front requirements for DV clearance and would almost certainly have failed SC clearance. Such an apparently high cut down rate is not uncommon in the high-end cyber security market, especially when taking into account the current requirement for DV clearance, which further constrains the available talent pool. HCSEC continues to face a recruitment challenge for the top end cyber security skills. They currently rely on a few very talented people to drive forward the research required to continue to innovate in this space. Despite this, GCHQ opinion is that HCSEC has some world class cyber security researchers and practitioners who are able to produce leading edge research and tools to support the Communications Service Providers doing risk management in their networks. The Oversight Board has been assured by Huawei that it intends to continue investment in HCSEC staffing and capability to help risk manage UK deployments. HCSEC's current staff number 30 with Huawei providing budget for this to rise to 37 during 2016 which is sufficient to meet the 2016 plan. To cope with the ongoing increasing complexity of deployments in UK, Huawei have informed the Oversight Board of their intention, later in 2016, to revisit HCSEC budget based on the products expected to be used by UK CSPs. The Oversight Board hopes this review will help manage the assurance gap brought by the complexity of UK deployments.

HCSEC Careers Framework

2.8 As per Huawei's Letter of Authorisation, HCSEC operates an independent Careers Framework (HCF) for its staff which relates to the Huawei corporate systems for Employment, Remuneration and Benefits, Grading and Appraisal. The HCSEC framework applies only while staff are employed at HCSEC; jobs outside HCSEC do not attract this structure, regardless of the incumbent. The HCF was implemented in 2014 to enable retention and reward of specialist staff, providing a progression pathway for both current staff and recruits.

2.9 The HCF uses conventional "job families" which contain bespoke "role

definitions" relevant to HCSEC work and matches them to the Huawei grade structure for remuneration and promotion purposes. Assignment of individuals to these roles and promotions are based on both core and technical competencies. There are "core competencies" for the behaviour and interaction of people and technical competencies for the skills and expertise of people, relevant to the work of HCSEC. These competencies are assessed twice a year against four levels of performance in order to monitor and develop each individual.

2.10 This framework is operated independently of Huawei UK and HQ, with the exception of the synchronisation of grade levels, salaries and performance markings at the mid-year point and at the end of the year. This synchronisation is achieved by minimal objective exchange of essential grade, performance and reward information, under the authorisation and control of the MD of HCSEC.

2.11 The HCF was used effectively in 2015 and has achieved the staff retention, motivation and attraction necessary to enable the team to grow. HCSEC has promoted four staff in 2015 using the HCF to assess new grades and salary for these staff. Staff morale and recruitment are strongly founded in the practical implementation of HCSEC's objective independence.

Accommodation

2.12 HCSEC accommodation is approaching capacity and needs to expand both lab space and staff work areas to allow simultaneous product and solution evaluation, which is necessary to ramp up assurance to the levels described by the agreed programme of work. The precise design of the expanded facility and the security requirements are to be agreed between GCHQ, HCSEC and Huawei HQ and will be approved by the Oversight Board. Huawei has approved the budget for the expanded facility and the search for premises by HCEC is ongoing. Any expansion plans are subject to contract with the relevant landlord.

2.13 Overall, good progress has been made on staffing and skills during 2015, but the position will need to continue to be monitored at the Oversight Board on a

quarterly basis to ensure delivery of HCSEC's plan in support of the UK Government's risk management strategy.

Section III: HCSEC Technical Assurance

2015 is the fifth year of the Government's extended risk management programme for Huawei's involvement in the UK telecommunications market. Given this milestone, the Oversight Board has chosen to exceptionally publish more technical detail of the work done by HCSEC in support of the UK Communication Service Providers' risk management.

Evaluation Process

3.1 Since it was established, HCSEC has performed security evaluations of products in various contexts. In order to better support UK CSPs, the HCSEC evaluation process has been evolved over the last year. There are now two distinct risk-based evaluation processes, "product evaluations" and "solution evaluations".

3.2 Product evaluations are security evaluations where the test is generally done in isolation, without information about the intended deployment of the product. This type of evaluation is relatively mechanistic and is mainly used to examine point releases of products which are updates to previously evaluated versions (for example the latest version of the MA5600 Multi Service Access Node which has been in service for some time) and some low risk products (such as ATN910 backhaul equipment which is relatively inaccessible to an attacker). Tooling is used for basic robustness testing of external protocols, for testing the declared security baseline and limited automated static code analysis. In addition, and importantly, testing is also carried out using HCSEC developed tools that are specific to Huawei products and technology.

3.3 In order to achieve this, HCSEC has built a new product evaluation team through recruitment and internal redeployment. This team was started in 2015 and the intention is to scale the team to be able to effectively manage the programme of work, subject to current discussions with Huawei around long term staffing and budget. The intent is for the product evaluation team to achieve at least SANS

certification[1] in relevant disciplines. SANS certification will then also be considered as an entry path to the HCSEC careers framework.

3.4 During the pilot phase of product evaluations up to 2015, a significant number of issues were detected, some of which were identified through widely available vulnerability scanners. This continues to demonstrate the value of independent product evaluation by HCSEC in managing risk.

3.5. The Oversight Board remit does not extend to Huawei's practices outside of HCSEC. However, there are interdependencies between HCSEC's work and the wider Huawei corporate processes which the Oversight Board and Huawei have agreed to report on exceptionally. HCSEC's work over the last five years has shown that release versions of Huawei software running in UK CSP systems have exhibited improvement in both code quality and the underlying engineering process. However, they still do not exhibit security and engineering metrics to the level expected of industry good practice. In general, the binaries exhibit high local and global cyclomatic complexity and high code segment duplication rates, usually at the level of translation units. Small changes in version number, for example point releases, do not always correspond to small changes in the code and monotonically increasing versions of the same product are not always related in obvious ways. HCSEC have also reported general security related observations around complexity and redundancy and use of deprecated functions such as unbounded string copies.

3.6 HCSEC will generate useful metrics based on source code in order to measure code quality objectively, which will be shared with the Huawei Security Competency Centre. These will help infer baseline security metrics for internal code quality improvement and UK CSP risk management and to ascertain whether specific enhancements have been made to products. Having seen the nascent technical capability, GCHQ expect these to be included in every product evaluation report going forward. With the enhanced evaluation model in HCSEC, the Oversight Board expects that evaluations will be more contemporaneous with initial deployment and that the gaps in assurance artefacts will reduce over the coming years.

[1] SANS is an internationally recognised cyber security training and certification provider.

3.7 Solution evaluations of products are more adversarial in nature since they seek to accurately emulate the UK CSP environment and architecture for the product under test. Solution evaluations test products in the context of the wider service provider network. Where possible, this emulation includes the use of real world network element configuration, provided by the relevant Communications Service Provider (CSP) to HCSEC. Solution evaluations contribute towards the development of new tools and techniques specific to the work of HCSEC. Their development is generally driven by the need to respond to a specific risk or impact on a UK CSP. HCSEC will work with the UK customer to fully understand the dependencies and risk profile for the individual pieces of equipment in the context of the specific network deployment. This detailed knowledge, coupled with any previous issues reported to R&D and the claimed status of their resolution (including issues in other products that share code or features) will generate a set of 'areas of interest' (AoI) for focussing the effort of the solution evaluation. The evaluation proper is then run as an agile programme, based on the areas of interest. These AoI will evolve as the work progresses, being directed by technical experts. Issues found during HCSEC's work are proactively managed as they are discovered with the CSP, GCHQ and PSIRT at Huawei HQ in China.

3.8 The standing intent, in place since 2012, is to perform four solution evaluations per year due to their complexity and depth of analysis required. Through the programme build and prioritisation process, HCSEC seek to minimize the residual risk of products that have not been assessed or have only ever been subject to a product evaluation. These products will generally attract low risk or not be widely used. However, the long term minimization of risk is contingent on balancing the complexity of UK deployments with HCSEC capacity.

3.9 HCSEC's evaluation process transformation has resulted in a more formal, repeatable methodology that gives consistent and comparable outputs, enabling solution and product evaluations to be performed in parallel. There has been significant improvement in the communication and partnership between HCSEC and the various UK Communications Service Providers. This serves to ensure better

understanding of the real risk in the UK and is something GCHQ are actively encouraging Communications Service Providers to maintain.

3.10 GCHQ's view, conveyed to the Oversight Board, is that the product and solution evaluations have been of consistently high quality and have provided useful risk management information to the UK Government, the CSPs and Huawei. HCSEC has shown that the product evaluation methodology can provide useful baseline assurance artefacts across the breadth of Huawei products deployed in the UK in a relatively automated manner. This will enable HCSEC to provide UK Communication Service Providers with a broad understanding of the engineering and deployment risks as identified by HCSEC, as well as the detailed and specific analysis provided by solution evaluations.

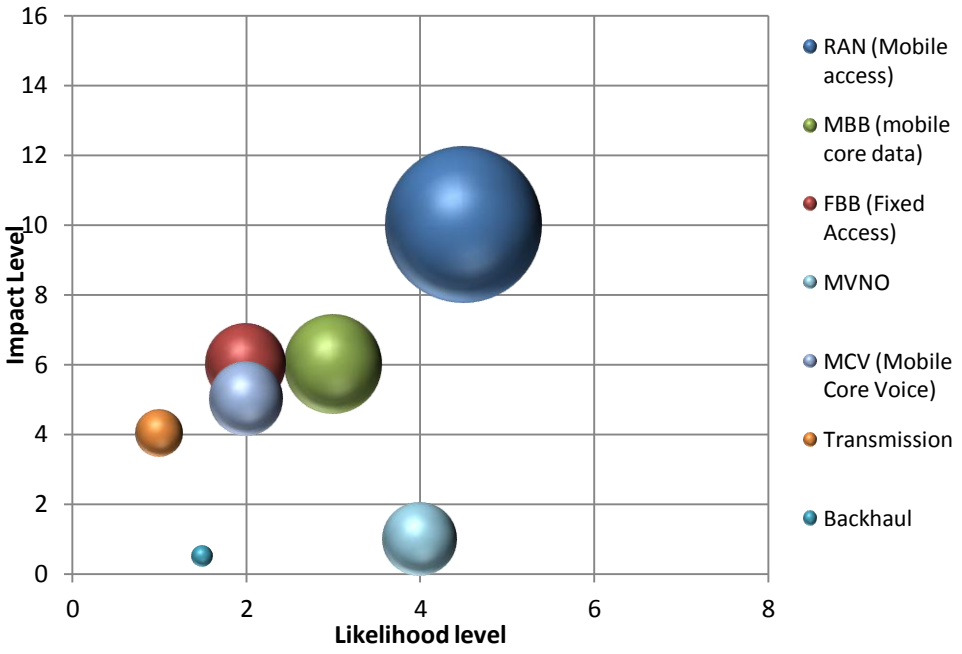
3.11 HCSEC's cybersecurity capability has continued to improve, finding subtler and more impactful issues. Compared with 2014, the average number of issues per product has remained broadly static with the total number rising in line with the increased number of products assessed. The number of products assessed rose by 27% this year. The severity profile of these issues has changed, reflecting the improved capability. Three issues that HCSEC has discovered in this year required specific intervention in deployed CSP systems, and these were handled using standard processes between UK Government and CSPs. HCSEC has developed a new issue management system to better allow monitoring and tracking of software defects discovered during HCSEC's work and to enable resolutions to be pursued with the Product Security Incident Response Team, who also use the tool.

Prioritisation and programme build

3.12 During the course of 2015, HCSEC and GCHQ have engineered a new prioritisation scheme in consultation with the Communication Service Providers. This better directs HCSEC's programme of work and provides an objective process to manage conflicting requirements. The implicit risk assessment contained in this process also provides a rationale for escalation of vulnerabilities and issues when they arise. The prioritisation process is generic, in that it could apply to any vendor, and takes into account the relative market penetration of that vendor in specific

areas, the relative impact compromise of those products may have in various situations, any mitigating factors that may manage the risks and product and vendor diversity in the UK Communication Service Providers. The process seeks to address impact across network functions classed as Fixed Broadband, Mobile Broadband (2G, 3G, 4G), Transmission, Switching and Routing, and the various service layer components. The risk represented by the different types of technology is expressed in terms of the potential impact of a security vulnerability based on the scale of deployment, the sensitivity of information being handled and the likelihood of such a vulnerability being exploited due to the accessibility to the adversary of the equipment or the data flows it processes in the various data planes. This enables different product types to be ranked in priority order. HCSEC is already addressing the complexity of fully featured Mobile Virtual Network Operator (MVNO) enabling products and the evaluation challenges these present.

3.13 Applying this generic process to Huawei's business in the UK, using commercially sensitive as well as public data, HCSEC arrives at risk ratings which are represented in the diagram below where the size of the bubble indicates the degree of risk. Clearly, this shows that significant risk is attracted by the Radio Access Network component and concomitant effort is expended on this part of the system. All of these types of products are considered to be critical to the safe operation of UK telecommunications networks. Inputs to these risk ratings are limited to the functionality of the product in question (for example, a Base Station Controller or a Multi Service Access Node), how that functionality interacts with user, signalling and management planes and the market penetration by a single vendor. Nothing specific to Huawei is used in these risk assessments and they are therefore generic and vendor-independent.



3.14 These data drive the programme build process. GCHQ, on behalf of the Oversight Board, formally signs off the HCSEC programme at the start of every year and progress is tracked, allowing for modifications due to changes in Communications Service Provider rollout programmes. The Oversight Board is informed of programme approval, but does not by default receive full details. This is in order to preserve the commercial confidentiality of the Communications Service Providers – the products they wish to have assurance in discloses their commercial service rollout schedule. This information is therefore highly sensitive. Should there be irreconcilable conflict, the Oversight Board Terms of Reference allow for an Oversight Board meeting to be called at which the industry members are recused to enable the Oversight Board to decide on the best course of action. The new prioritisation scheme is also helping the Oversight Board make informed and rational assessments of the technical decisions that are made between GCHQ and HCSEC. By codifying risk and likelihood in a simple to understand way, the Oversight Board can be assured that effort is being invested in the parts of the system that are most important to the security of the UK.

Issue Resolution and Communication

3.15 A trusted security partnership between HCSEC and the Product Security Incident Response Team (PSIRT) based in Huawei HQ in Shenzhen is essential in order to minimize the risks and impacts that could occur when an issue is found in a fielded product. The 2015 Annual Report highlighted the need for the relationship between HCSEC and PSIRT to develop further to enable effort sharing over managing vulnerabilities. In response to the Board's concerns, HCSEC has worked to re-engineer the relationship with PSIRT and developed an HCSEC issue management system for the raising of issues, issue management and the issue reporting process (to customers) to make it much more relevant to Communications Service Providers, GCHQ and Huawei PSIRT. As a result of the improved relationship, HCSEC has achieved better tracking of issues across versions of products, which has identified some of the issues alluded to in para 3.5. The next step in the evolution of the PSIRT relationship will be to better understand how consistency is maintained regardless of the route of vulnerability disclosure.

3.16 The division of responsibilities between PSIRT and HCSEC has also been reassessed and adjusted. PSIRT is now responsible for notification across Communications Service Providers. If HCSEC identify a vulnerability in an evaluation for a specific CSP, PSIRT now use HCSEC and corporate data to correlate across all UK CSPs and to warn others that may be affected. PSIRT Security Notices, Security Advisories and specific issue mitigation and resolution advice are now all discussed with HCSEC and agreed before release. This approach is specific to vulnerabilities and issues discovered by HCSEC.

3.17 HCSEC also produce Product Advisories, for example notifying R&D and PSIRT of coding deficiencies. This demonstrates good practice that goes some way towards generally improving code quality.

3.18 HCSEC's ownership and management of the process for communications with Huawei PSIRT has resulted in a significant improvement in the process of raising and tracking vulnerabilities and notifying UK Communications Service Providers of the risks.

Summary of GCHQ Technical Competence Review

3.19 The last year has shown further development of the technical capability in HCSEC. Developing technical capabilities is necessary in order to provide assurance to UK CSPs as the complexity of both individual products and the systems they create increases.

3.20 As in all organisations, there is a requirement for underpinning IT capability. The enabling capabilities at HCSEC include the independent desktop system and associated back-end tools to perform automated analysis, the workflow systems to track projects through the evaluation lifecycle and tools to manage the exceptionally complex compilation process required for Huawei products. The development of these tools is intended to free up analysts' time to enable them to do work that cannot currently be automated.

3.21 The portfolio of assurance tools used has also been extended, both for the use of commercial off the shelf tools and proprietary tooling developed in HCSEC. One of the key capabilities for long term assurance is binary equivalence; showing that the source code examined by HCSEC produces the binary software running on network elements in the UK. This is a very challenging requirement given the complex nature of the Huawei build process, but HCSEC's initial work in this area shows promise. The intent is that the Oversight Board can have confidence in knowing that HCSEC's processes have been applied to what will be running on UK deployed equipment over time.

3.22 The HCSEC source code analysis capability now does automated extraction of the functionally-relevant source code from the massive oversubscription of code (i.e. that code which actually contributes to the final build) and builds artefacts that are useful to help analysts derive information, for example control flow graphs and abstract syntax trees, at very large scale. This advanced tooling helps HCSEC find more complex and subtle vulnerabilities in the products.

3.23 HCSEC's research programme has developed tools that search for particular security artefacts across multiple products which helps scale the discovery task. This is being extended to search for more generic vulnerability signatures in product binaries, which will allow automated discovery of certain classes of cybersecurity issue during product evaluations. There are a number of common cybersecurity

techniques that do not immediately apply to telecommunications products and HCSEC are in the process of porting several of them for use in this area.

Effect on product security

3.24 There has been a measurable improvement in the security and quality of code coming from the research and development teams since HCSEC began work to engender improvement in the basic engineering and security processes and capabilities. Over the last five years, HCSEC has observed a marked reduction in basic errors and an improvement in baseline feature hygiene. Code quality has shown signs of improvement, but remains below industry good practice. There remains room for improvement around architectural design. Some of the legacy design decisions will require long term risk management as remediation in running networks is very difficult.

3.25 It is an inevitable feature of technology today that its complexity is increasing. As new technologies with significant potential security impacts are integrated into the products, for example SDN and x86 virtualisation, HCSEC will need to closely monitor implementations and work closely with Huawei R&D to understand the impacts on security in UK deployments.

Conclusion: technical assurance

3.26 Overall, given this account of the technical assurance work of HCSEC to date, GCHQ 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, although more work is needed in many areas. The Oversight Board will be looking to HCSEC to continue to make progress to cover the breadth of deployments in the UK with appropriate assurance artefacts to enable risk management at both Communications Service Provider and national scale, prioritised by the criticality of impact.

~~~~~
~~~~~

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 second 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. For 2015, the Audit's remit was unilaterally extended by GCHQ to consider the recruitment and appointment of the new HCSEC Managing Director. This section provides an account of the process by which the audit took place, and a summary of the key findings.

Appointing Ernst and Young as auditors

4.2 Ernst and 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. GCHQ proposed the use of E&Y for a second year running, given the complexity of ensuring all the relevant confidentiality agreements and clearances were in place. The Oversight Board was content to proceed with E&Y as auditors and asked them to assess what a multi-year approach to auditing HCSEC would entail. 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:

i. An initial phase to assess the control environment and agree the scope and key issues for review. This phase was completed by September 2015;

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 October 2015;

iii. A final audit phase comprising the full year end audit, with the report presented to the Oversight Board in January 2016.

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. GCHQ unilaterally requested that the audit cover the recruitment of the new Managing Director. 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 2016 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 and Young; the fieldwork was

conducted by a highly experienced Senior 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 and Young Senior 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:

'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 and these have been noted as "advisory" recommendations as opposed to identified control deficiencies".

4.8 The audit report identified four control weaknesses within the HCSEC control environment for the Board to consider. All four weaknesses were 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. The audit findings were presented to the Board in its January meeting with an Ernst & Young Executive Director in attendance to brief the Board. The Oversight Board discussed each of the four rated as "Low" in the audit and agreed an approach for each one.

Control Weaknesses

4.9 In summary, the four areas of control weakness identified, and the agreed response, relate to the following areas.

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

4.10 The evaluation plan, which outlines which products will be tested at which points of the year, is not formally signed off by the Oversight Board when it is base-

lined. The audit assessed that if HCSEC was being unduly influenced to change the evaluation plan by Huawei, the Oversight Board may not be in a position to identify this and challenge it effectively. The audit recommended that the Oversight Board should formally sign off the base-lined evaluation plan to demonstrate their understanding and acceptance of the sequencing of work. The Oversight Board should also review progress against plan midway through the year. HCSEC should provide an update to the Oversight Board of any significant deviations in plan during the year and these should be formally recorded in the meeting minutes, with any associated budget and staffing implications being formally owned and signed off by Huawei. It should be noted that GCHQ currently formally signs off the HCSEC evaluation plan.

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

4.11 The audit found that RFIs made to Huawei were not always returned within the stated 15 working day SLA for software or the 21 week SLA for hardware. In sampled tests, they observed that in one instance out of four tested, the requested software information was not made available until 30 days after the RFI had been raised. Additionally, 1 out of 21 hardware requests tested was returned outside the SLA period. In discussion with HCSEC it was noted that the SLA is aspirational, and that non-adherence would not necessarily adversely impact evaluation performance due to some flexibility in the programme build and sequencing. The audit recommended that RFIs should be updated to include a “required by” date with the intention that it is strongly adhered to and escalated when it is breached. Subsequent information has been provided by HCSEC to indicate that technical deliveries did not delay HCSEC evaluations. Huawei have shown that the hardware delay was caused by unanticipated customs delays and the software delay was caused by a previously unknown technical limitation of the transfer system. The Oversight Board accepts that the delays were not caused by Huawei.

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

4.12 The audit assessed that the ability of the Huawei UK CEO to independently set the MD’s bonus provides a vector by which performance of HCSEC could be

influenced. By withholding or awarding the bonus (irrespective of performance), which constitutes a significant element of the reward package, the bonus could be used as a tool to motivate certain behaviours from the MD. This has been a recognised risk since the establishment of HCSEC and the Oversight Board and CESG reconsidered this risk, which they accepted as reasonable. They agreed that the Risk and Control Matrix should be updated to reflect this agreement.

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

4.13 PGP encryption is used by HCSEC when disseminating their evaluation reports as a preventative security measure. This requires HCSEC to hold a valid public key for each of the intended recipients to be able to encrypt the document. Due to the expiry of the key used by CESG from the period 1 July to 20 November it was not possible to send reports to CESG. Reports were still sent to CSPs during this time. In the normal course of events, HCSEC would contact CESG directly to highlight and explain issues in detail, to support discussion with the CSPs. In the absence of these reports, CESG is unable to provide a level of comfort that the reports have been adequately produced, which can serve as a mechanism to detect undue influence. However, the audit observed that if a CSP was dissatisfied with an evaluation report, it would be likely to alert CESG directly. It was also noted that HCSEC raised specific significant issues directly with CESG during this period. The Oversight Board agreed the audit recommendation that CESG should ensure that HCSEC are always in possession of a valid key to allow dissemination of evaluation reports in a timely manner. This is relevant to the continued independence of HCSEC as it ensures an authenticated communication channel between HCSEC and GCHQ, ensuring that GCHQ get unadulterated HCSEC reports.

Advisory Notices

4.14 Two advisory notices were identified by the audit, relating to the supplier used for cleaning services and the register of recruitment agencies.

i. The supplier used for cleaning services was not on the HCSEC preferred supplier list

4.15 HCSEC have their own preferred supplier list, however, audit testing identified that the office cleaning service is provided by a Huawei preferred supplier which is not on the HCSEC list. This is purely an administrative oversight and has been the case since HCSEC was first opened. Whilst this did not breach the control being tested, which related to suppliers of tools used for technical assessments, it was cited as an Advisory Notice as the cleaner has access to secure areas during office hours whilst escorted. The Oversight Board agreed the audit recommendation to review the supplier in question using the preferred process and decide whether to retain this cleaning service as the HCSEC preferred supplier or select an HCSEC approved alternative. Neither GCHQ nor HCSEC are concerned about this point at the present time, but will review it again with the new accommodation in mind.

ii. Register of HCSEC approved recruitment agencies is not regularly updated

4.16 The audit found that the list of recruitment agencies used by HCSEC was not kept up to date in the period under review. Although suitable evidence was found to provide comfort that the agencies reviewed were engaged by HCSEC and not imposed by Huawei corporate, the administrative process to document that the control was working effectively had not been followed correctly. The Oversight Board accepted that the recruitment register should be kept up to date and reflect organisations with which HCSEC maintains a relationship for recruitment purposes, including noting the current status of that relationship.

Prior year issues and current status

4.17 **Appendix B** provides a summary of the issues and observations from the previous year's report, published in January 2015.

Follow up on proposed enhancements to the wider governance environment identified during the course of the 2014/15 audit despite being outside the formal audit scope

4.18 **Appendix C** provides a summary of the status at the time of the 2015-2016 audit of wider issues which may also have a bearing on the independent operation of HCSEC that were raised in the 2014-2015 audit, despite being outside the formal scope for the 2014-2015 audit.

Overall Oversight Board conclusions of the audit

4.19 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 is operating robustly and effectively, and in a manner consistent with the 2010 arrangements between the Government and the company. Four issues of concern – rated collectively as of overall low risk – have been identified. In addition, the audit has provided useful scrutiny of follow up on proposed enhancements to the wider governance environment, as highlighted during the 2014-2015 Audit.

SECTION V: Conclusions

5.1 The Oversight Board has now completed its second 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 second year of work are:

- GCHQ 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, although more work is required in many areas. The Oversight Board will be looking to HCSEC to continue to make progress to cover the breadth of important deployments which are relevant to UK national security risk in the UK with appropriate assurance artefacts to enable risk management at both Communications Service Provider and national scale. To cope with the ongoing increasing complexity of deployments in UK, Huawei have informed the Oversight Board of their intention, later in 2016, to revisit HCSEC budget based on the products expected to be used by UK CSPs.;

- The HCSEC Evaluation process has evolved during 2015 and there are now two distinct evaluation processes for products and solutions. HCSEC has shown that the product evaluation methodology can provide useful baseline assurance artefacts across the breadth of Huawei products deployed in the UK in a relatively automated manner. This will enable HCSEC to provide UK Communication Service Providers with a broad understanding of the engineering and deployment risks as identified by HCSEC, as well as the detailed and specific analysis provided by solution evaluations. A new prioritisation scheme has been engineered to better direct the programme of work and to provide an objective process to manage conflict;

- The Oversight Board is satisfied that the 2015-2016 audit report has provided important external reassurance that the arrangements for HCSEC's operational independence from Huawei Headquarters are operating robustly

and effectively and in a manner consistent with the 2010 arrangements between the Government and the company. Four issues of low concern were identified, all of which were rated as low risk and mitigations are in place. The audit has also provided useful scrutiny of follow up on proposed enhancements to the wider governance environment, as highlighted during the 2014-2015 audit despite being out of the formal scope;

- Although recruitment remains challenging, staffing at HCSEC has increased during 2015 and the Centre has put renewed effort into improving its recruitment figures. The Huawei Careers Framework was used effectively in 2015 and has achieved the staff retention, motivation and attraction necessary to enable the team to grow in 2015. The position on staffing, skills and recruitment will need to continue to be monitored by the Oversight Board on a quarterly basis, as will HCSEC's capacity to manage the complexity of UK deployments.

5.3 Overall therefore, the Oversight Board has concluded that in the year 2015-2016, 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. Additionally, it is hoped that this report continues to add to Parliamentary – and through it – public knowledge of the operation of the arrangements.

~~~~~
~~~~~

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, Director General)
- Huawei HQ – Deputy Chair (Ryan Ding, Executive Director of the Board)
- Huawei UK Executive Director
- HCSEC Managing Director
- Cabinet Office Director, OCSIA
- Cabinet Office Deputy Director OCSIA
- GCHQ Technical Director
- Whitehall Departmental representatives: (Deputy Director Cyber Security and Resilience, Digital Economy Unit, BIS, 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

[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.

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.

- 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. Secretariat

GCHQ will provide the secretariat function.

8. 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.

9. Annex – 1 – MOU on HCSEC Senior Appointments

This MOU will be reviewed and agreed at the first Oversight Board meeting.

It is agreed that GCHQ will lead and direct the senior appointments within HCSEC, in consultation with Huawei. The senior appointments are deemed to be the following positions: HCSEC Managing Director; HCSEC Technical Director and HCSEC Solutions and Programme Director. The process is defined as follows with Huawei meaning Huawei HQ in the case of the appointment of the Head of HCSEC and HCSEC for the other senior appointments.

1) Suitable candidates will be identified by GCHQ and Huawei through a range of recruitment and identification methods as agreed by GCHQ and Huawei.
2) The pool of candidates will be jointly reviewed and candidates not deemed experienced, technically capable or unlikely to obtain the relevant security clearance will be rejected.
3) Shortlisted candidates will be invited to a joint (GCHQ and Huawei) selection panel chaired by GCHQ.
4) Following the interviews GCHQ, jointly with Huawei, will select the most appropriate candidate.
5) The selection of the most appropriate candidate must be a unanimous decision.

Huawei UK agree that no individual who fails to obtain the required security clearance shall be appointed to HCSEC. Subject to that, the terms of employment of any candidate appointed to HCSEC will be determined by Huawei UK.

10. Annex – 2 – SLA between Huawei HQ and HCSEC

This SLA, which contains a description of expectations for how information is delivered to HCSEC, has been removed from this Oversight Board report due to commercial sensitivities. The Oversight Board is content that the SLA is appropriate. A copy is stored on GCHQ systems.

11. Annex – 3- Huawei HQ Letter of Authorisation (Operational Independence) to HCSEC dated 17th July 2015

This letter, which contains a description of the authorities devolved to HCSEC has been removed from this Oversight Board report due to commercial sensitivities. The Oversight Board is content that the arrangement is appropriate. A copy is stored on GCHQ systems.

Appendix B

Issues raised in the 2014-2015 Audit and current status

The 2016 Audit reviewed progress against addressing the following three issues that were highlighted in the 2014-2015 report. All three issues were rated as "Low".

1. Staff who are not yet DV cleared are employed within HCSEC

1.1 The January 2015 report observed that "*four members of staff were working at HCSEC without DV clearance. All four had submitted paperwork and were progressing through the clearance process but at the time of writing the report, they had not finished their probationary periods with HCSEC"*.

1.2 This risk has been **accepted** by the Oversight Board and by CESG. Staff cannot be entered into the DV clearance process until after they have commenced employment with HCSEC. All staff encountered by the audit either held clearance or were awaiting clearance. It has been reconfirmed that staff do not complete their probation period with HCSEC until their DV clearance has been confirmed. The Risk and Control Matrix is being updated to reflect this, and to focus on articulating the controls in place over staff working at HCSEC who are still undergoing the vetting process.

2. Allocation of bonus payments by Huawei

2.1 The 2015 audit report observed that "*Huawei Corporate were able to set bonuses for HCSEC staff without the explicit review or approval from HCSEC management"*.

2.2 This risk has been **closed**. Bonuses are awarded by the HCSEC management team and confirmed (without change) by Huawei Corporate. This reduces the possibility of Huawei Corporate influencing staff through limited/excessive reward.

3. Current HCSEC internal budgeting process does not document formal agreement and sign off from HCSEC contributors.

3.1 The 2015 audit noted that "*the 2014 budget setting process did not document formal agreement and sign off by HCSEC contributors"*.

3.2 This risk has been **closed**. It was observed during the current audit that the HCSEC budget was set and approved by the HCSEC senior management team and further approved by Huawei Corporate.

Appendix C

Follow upon proposed enhancements to the wider governance environment, identified during the course of the 2014-2015 audit, despite being outside the formal scope.

The 2014-2015 audit identified four issues which were outside its scope but which may also have a bearing on the independent operation of HCSEC. A summary of their status at the time of the 2015-2016 audit follows.

1. Use of HCSEC evaluation resources on non-UK product deployments

1.1 The 2015 audit observed that over the 12 months prior to its review, Huawei had carried out evaluations on products to be deployed by non UK customers. These had all been carried out with the knowledge of CESG and at the time of writing the audit had not impacted on the UK evaluation schedule. However, the audit noted that ability of HCSEC to refuse to undertake non UK work or to prioritise UK work over other work for Global Huawei customers was not explicitly delegated to the HCSEC Director in the Letter of Authorisation, meaning that the measures in place were not sufficient to guarantee that this issue would not become a threat to HCSEC's independence in the future. The 2015 audit suggested that an escalation process to notify the Oversight Board of non UK work requests which might compromise the operational independence of HCSEC should be agreed between HCSEC and the Oversight Board.

1.2 This issue remains **open**. The Oversight Board is aware of this potential risk and, with CESG, monitors it closely. Following discussion at the January 2016 Oversight Board meeting, members confirmed that the intention is to further update the Terms of Reference of the Oversight Board to strengthen point 3.6 relating to the Escalation Process (see Appendix A) so as to explicitly allow any member of the Board to escalate to the whole Board a concern about the ability of HCSEC to deliver on its UK evaluation plan as a result of resources being allocated to overseas evaluations.

2. Potential to use the Oversight Board as a point of escalation

2.1 The 2015 audit noted that although constituted as a governance Board, the Oversight Board does not yet have formalised escalation processes to cover the following eventualities:

- A disagreement between the HCSEC Director (or senior staff members) and Huawei over the HCSEC annual budget;
- A breach by Huawei of the provisions of the Letter of Authority, identified by the HCSEC Director or senior staff members;
- A change during the course of the year to the resource levels or tasking of the HCSEC by Huawei which might impact on its mission or its independence.

2.2 The audit noted that unless HCSEC management were able to escalate concerns to the Oversight Board quickly, there was a risk that the HCSEC Oversight Board may not be able to discuss developments which may impact the work of the facility in a timely manner. The Audit assessed that this may impact the ability of the Oversight Board to ensure the independent and effective operation of HCSEC.

2.3 The 2015 audit recommended that the Terms of Reference of the Oversight Board be updated to reflect the following:

- Explicitly enable the Oversight Board to act as a point of escalation and arbitration for the HCSEC, or CESG for budgetary and operational matters, and for disputes over the interpretation or implementation of the Letter of Authority;
- Introduce a process by which a special Oversight Board meeting can be convened.

2.4 This issue is now **closed.** The Terms of Reference for the Oversight Board have been updated with the inclusion of Section 3.6 which allows the Oversight Board to be a point of escalation for concerns of the nature identified in this finding.

3. Communication of key evaluation decisions

3.1 The 2014-2015 audit observed that CESG and HCSEC leadership working together determine what information is required to enable an effective evaluation to be performed. In the course of that determination, CESG and HCSEC may decide to exclude a specific class of information from the evaluation. At the time of writing the audit, the decision as to whether the impact on the evaluation process was acceptable fell to one team within CESG and was not communicated or validated elsewhere. The audit advised that if the Oversight Board was not sighted on risk based decisions by either CESG or HCSEC to reduce or restrict the scope of evaluation testing, they may take a false level of comfort from the evaluation testing that had been performed. The audit recommended that CESG and HCSEC should jointly provide the Oversight Board with an update on restrictions or limitations to planned evaluations which CESG had approved on a risk assessment basis.

3.2 This issue is now **closed**. HCSEC had CESG have undertaken to jointly provide the Oversight Board with an update and restrictions and limitations to planned evaluations. Attesting to the technical robustness of the evaluation process and the appropriateness of decisions taken within this is covered within the scope of the CESG assessment of HCSEC.

4. Definition of "Senior Management" in the Application of Annex 1 of the Oversight Board Terms of Reference – MOU on HCSEC Senior Appointments

4.1 At the time of writing the 2014-2015 audit report, HCSEC leadership and CESG leadership agreed that the HCSEC Senior Management were:

- Andrew Hopkins: HCSEC Managing Director;
- Stuart Begg: HCSEC Technical Director;
- Michael Owens: HCSEC Solutions and Programme Director.

4.2 However, during discussions with HCSEC and CESG, the Auditors observed that the definition of "Senior Management" and therefore which roles fell under the scope of the MOU on HCSEC Senior Appointments, had not been set. The Auditors assessed that should HCSEC expand in future, leading to the creation of new Senior

Management roles, or should roles not currently considered Senior Management become more influential, it may not be clear which to which roles the MOU on HCSEC Senior Appointments applied. The audit assessed that this increased the risk that the MOU is not used when required and recommended that the applicability of the MOU should be clarified by clearly defining which roles are considered senior appointments and updating this in the Oversight Board Terms of Reference.

4.3 This issue is now **closed**. The Terms of Reference for the Oversight Board have been updated to define which roles are considered senior appointments. The ToRs now state that "*The senior appointments are deemed to be the following positions: HCSEC Managing Director; HCSEC Technical Director and HCSEC Solutions and Programme Director*". The Terms of Reference have already been further updated to reflect how the list of roles considered senior appointments will be kept up to date.

~~~~~
~~~~~