HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD

1st ANNUAL REPORT

2015

A report to the National Security Adviser of the United Kingdom

March 2015

Huawei Cyber Security Evaluation Centre Oversight Board 1st Annual Report

Part I: Summary

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

2. HCSEC opened in November 2010 and its infrastructure meets the UK Government's standards as a secure facility. It is a crucial part of a set of arrangements agreed earlier that year between the company and HM Government about mitigating any perceived risks to UK national security arising from the involvement of Huawei in parts of the UK's critical national infrastructure. HCSEC provides security evaluation for a range of products and services used in the UK market. Through HCSEC, the UK Government is provided with insight into Huawei 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.

3. The HCSEC Oversight Board was established in early 2014 on the recommendation of the UK National Security Adviser. The Board is chaired by Ciaran Martin, DG for Cyber Security at GCHQ. It comprises senior executives from Huawei, including in the role of Deputy Chair, as well as senior representatives from across Government and the UK telecommunications sector. The role of the Oversight Board is to oversee and ensure the independence, competence and overall effectiveness of HCSEC. By doing so it is then able to advise 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. The Oversight Board's role relates only to products that are relevant to UK national security risk.

4. The Oversight Board has now completed its first 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 Part II of this report. In this summary, the main highlights are:

i. The **technical work of HCSEC as part of its assurance function**. The Board has concluded that the technical assessments conducted have been of consistently high quality and have provided useful risk management information to both the Government and the CSPs;

ii. The **position on recruitment, staffing and skills in HCSEC**. The Board has concluded that HCSEC has a set of good technical staff from a wide range of technical backgrounds, enabling them to meet all their current technical and business requirements. HCSEC has also recently appointed a new MD, in a joint recruitment process with GCHQ. Lessons have been learned from the experience which will contribute towards optimising the process in future. Ongoing challenges around staffing levels and appropriate and timely vetting also need, and will receive, constant, rigorous monitoring and oversight; and

iii. **A rigorous exercise to provide independent assurance of HCSEC's operational independence from Huawei HQ**. The audit, which was conducted by Ernst and Young, covered multiple areas of HCSEC's activities; finance and budgeting, personnel; procurement; evaluation programme planning; cooperation and support from corporate Huawei; and evaluation reporting. In line with audit recommendations, the Board will continue to pay close attention to the issue of achieving prompt DV clearance for HCSEC staff. The audit concluded that there were no major concerns about the independent operation of HCSEC.

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

- On GCHQ’s advice, **the Board accepts that the technical assurance provided by HCSEC was of sufficient scope and quality** to meet its obligations under the 2010 arrangements between the UK Government and the company; and

- **The management audit by Ernst & Young provides sufficient assurance that HCSEC has operated with sufficient independence from Huawei Headquarters** and any other body in a manner consistent with its obligations under the same arrangement. The Board has drawn considerable confidence from Ernst & Young’s statement that “*The HCSEC control environment in place at the time of our work, effectively supports the independent operation of HCSEC, in all material aspects”.*

6. Overall therefore, the Oversight Board concludes that in the year 2014-15 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 1st Annual Report

Part II: Technical and Operational Report

This is the first 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[1]. It is important to note that the Oversight Board has no 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: requirement for this report

1. Huawei Technologies, headquartered in China, is now one of the largest telecommunications companies in the world. It operates in the United Kingdom (UK) as Huawei UK. In 2010, Huawei reached a set of arrangements with the Government of the United Kingdom on how reasonable assurance could be provided that its increasing involvement in the UK's critical national infrastructure did not pose any threat to UK national security. As part of these arrangements, the company established the Huawei Cyber Security Evaluation Centre (HCSEC) in Banbury, Oxfordshire.

2. In response to a 2012 review carried out by Parliament's Intelligence and Security Committee, the UK's National Security Adviser submitted a report to the ISC in December 2013 with various recommendations for enhancing the risk mitigation arrangements. A key recommendation was the establishment of an Oversight Board for HCSEC. The Oversight Board is chaired by Ciaran Martin, an executive member of GCHQ's Board with responsibility for cyber security, and includes a

[1] The paragraphs to which this specifically applies are 2.3 and 3.17 of the Technical and Operational Report and Appendix C para 1.1

senior executive from Huawei as Deputy Chair, as well as senior representatives from across Government and the UK telecommunications sector.

3. The National Security Adviser's review committed the Oversight Board to producing:

> *"An annual review of HCSEC's performance, again overseen by the Board, and delivered to the National Security Adviser, to share with the National Security Council. This annual review should include a technical assessment of delivery, led by GCHQ, and an annual management audit of continuing independence from Huawei headquarters by appropriately vetted auditors. Summaries of both reviews will be passed to the Intelligence and Security Committee [of the British Parliament]."*[2]

4. This is the first such annual report. It has been agreed unanimously by the Board's members. In the course of its preparation it became clear that there was no need for a confidential annex; what follows in this report represents the full analysis and assessment.

5. The report is set out as follows:

I. Part I sets out the nature of Huawei's involvement in the UK and the functions of the Oversight Board;
II. Part II describes the work of the Board in respect of oversight of the technical assurance provided by the work of HCSEC;
III. Part III reports on the Board's consideration of an audit of the independence of HCSEC, and the rest of the Board's work; and
IV. Part IV brings together some conclusions.

[2] Huawei Cyber Security Evaluation Centre Review by the National Security Adviser, December 2013, paragraph 9.

SECTION I: Huawei in the UK: HCSEC and the Oversight Board

Huawei in the UK

1.1 Huawei UK came to prominence in the UK in 2004, after successfully bidding for BT's major network upgrade. Over recent years, Huawei has significantly increased its access into the UK communications market including securing contracts with Vodafone, EE, O2, Talk Talk, Virgin Media and Sky.

1.2 The modern reality is that virtually every telecommunications network worldwide incorporates foreign technology. Most manufacturers have some of their equipment built in China and use technical components from a global supply chain, regardless of the location of their headquarters. That said, as Huawei's customer base in the UK expanded, the UK Government has sought to put in place a mitigation strategy to manage any potential security risks associated with the prevalence of Huawei equipment in UK networks. Towards the end of the last decade, the Government embarked on a series of discussions with Huawei aimed at reaching a mutually acceptable framework for providing assurance that any such risks to UK national security were being mitigated. This culminated in the company and the Government agreeing to a set of arrangements for the governance of Huawei's involvement in the UK in 2010.

The establishment of HCSEC and its relationship with GCHQ

1.3 One of the most important aspects of these arrangements was the establishment of the Huawei Cyber Security Evaluation Centre (HCSEC) in November 2010. HCSEC is a Huawei owned and operated facility in Banbury, Oxfordshire. Its building meets the UK Government's standards as a secure facility.

1.4 Through HCSEC, the UK Government is provided with insight into Huawei UK's strategies and product ranges. In particular, HCSEC provides a route for close analysis of Huawei equipment deployed in the UK and relevant to UK national security, to identify any potential vulnerability.

1.5 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. GCHQ, on behalf of the Government, sponsors the security clearances of HCSEC's staff. The general requirement is that all staff should 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. The current Managing Director of HCSEC, Andy Hopkins, served for 40 years in GCHQ before joining Huawei. Mr Hopkins is due to retire in July 2015, having transitioned to his successor.

1.6 HCSEC is a part of Huawei and is fully funded by the company. Its staff and particularly its Managing Director are naturally required to fulfil their corporate responsibilities. But HCSEC has a primary obligation to meet the requirements of GCHQ in providing assurance on security risks. The technical work carried out under this obligation is summarised in Section II of this report. These arrangements also require HCSEC to have a considerable degree of operational independence from Huawei Headquarters; that independence was the subject of a detailed management audit by Ernst & Young LLP which is summarised in Section III.

Oversight enhancements: The ISC report and the National Security Adviser's response

1.7 In April 2013, the Intelligence and Security Committee of Parliament (ISC) conducted a review entitled 'Foreign involvement in the Critical National Infrastructure: Implications for National Security'. The published report is available at Report on Foreign Involvement in the Critical National Infrastructure. Amongst a number of conclusions arising from the review, the ISC recommended that the National Security Adviser *'conducts a substantive review of the effectiveness of HCSEC as a matter of urgency'*. In particular, the ISC recommended a stronger and more explicit involvement of GCHQ in the oversight of HCSEC and its operations.

National Security Adviser Review

1.8 In response to the ISC Review recommendation, in December 2013, the National Security Adviser conducted a review of HCSEC, focused on its operational independence, including the employment of its staff; its planning and budgetary oversight; how it did its work; and the security around the facility. The review involved visits to HCSEC, interviews with main stakeholders, and examination of documentary evidence.

1.9 The review judged that HCSEC was operating effectively and achieving its objectives and that existing arrangements gave it sufficient independence. It noted that, once systems became established, Huawei's cooperation with HCSEC appeared exemplary. The review concluded that the Centre was the best way of ensuring continued complete access to Huawei products, codes and engineers, without which HCSEC could not do its job. The review also made a clear recommendation for a strengthening of the oversight of HCSEC. Specifically, it recommended the creation of an Oversight Board, chaired by GCHQ, with tightly controlled membership including one or two Whitehall departments, representatives of one or two UK communications service providers (CSPs) and a senior representative of Huawei as the Deputy Chair.

The HCSEC Oversight Board: Terms of Reference

1.10 The HCSEC Oversight Board was established in early 2014. It has met four times to date, under the chairmanship of Ciaran Martin, an executive member of GCHQ's Board at Director General level. He reports directly to GCHQ's Director, Robert Hannigan, and is responsible for the agency's work on cyber security.

1.11 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.

1.12 The Oversight Board's scope relates only to products that are relevant to UK national security. 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; and
- second, the independence, competence and therefore overall effectiveness of HCSEC in relation to the discharge of its duties.

1.13 The Board has an agreed Terms of Reference, a copy of which is 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 HCSEC Oversight Board: Membership

1.14 The Oversight Board comprises predominantly government representatives, but also includes senior representatives from two UK Communication Service Providers (CSPs) acting in an advisory capacity to the Oversight Board[3], as well as three senior representatives of Huawei. The Deputy Chairman is Ryan Ding, Executive Director of the Board and President, Products and Solutions Huawei Technologies. The Huawei UK Executive Director and Managing Director HCSEC are also members. Director of the Office for Cyber Security and Information Assurance at the Cabinet Office is a member, as are senior representatives from the Home Office and from BIS. Two executives from BT and Vodafone are also formal members of the Board. To manage any perceived risks around commercial confidentiality, there is provision in the terms of reference for the CSP representatives to recuse themselves from an Oversight Board meeting on commercial grounds. A full list of Oversight Board members' roles is at **Appendix B.**

[3] The term 'advisory capacity' is used in relation to the CSP members acting on a personal, industry expert basis rather than representing their companies. They remain full members of the Oversight Board.

The Board’s objectives for HCSEC

1.15 As its first business, the Oversight Board, under the chairmanship of GCHQ, has agreed four high level objectives for HCSEC. These 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 the security capability of Huawei continually.

The HCSEC Oversight Board: Business to date

1.16 As well as setting out these objectives, the Board, in its four meetings since its establishment, has:

- formalised its Terms of Reference, set out at **Appendix A**;
- undertaken ongoing monitoring of progress and assurance against an evolving programme of evaluations of key items in the Critical National Infrastructure;
- agreed a process for the appointment of external auditors to carry out an HCSEC management audit, and considered the outcome of that audit;
- agreed a process for selecting a new head of HCSEC on the retirement of Mr Hopkins. The outcome of that process is covered in paragraph 2.17;

- considered what information could most usefully be placed before Parliament, and through Parliament, in the public domain, to provide assurance that the arrangements constitute satisfactory protection for UK national security, principally through the preparation of this annual report.

Discussions between HM Government and Huawei Headquarters

1.17 Although outside the formal work of the Board, in the interests of transparency, this report includes a summary of the discussions between senior Government representatives and the company in January 2015. At the invitation of Huawei HQ, the Chairman of the Oversight Board, Ciaran Martin of GCHQ, together with the then Director of the Cabinet Office's Office of Cyber Security and Information Assurance, James Quinault, and GCHQ's Technical Director, Dr Ian Levy, visited Huawei Headquarters in Shenzhen, China. They met with company leaders and held extensive discussions with Ken Hu, rotating Chief Executive Officer, Ryan Ding, Executive Director and Deputy Chair of the Oversight Board and Chen Lifang, Huawei's Board member for public affairs. They also met with a variety of cyber security specialists working for the company.

1.18 During the visit Huawei presented the delegation with an overview of the Huawei Cyber Security Strategy and a summary of progress made on the implementation of the strategy over the last four years. The Government representatives received continued assurance from Huawei about their commitments to HCSEC and the broader arrangements, and were informed during the visit that the company had agreed to a funding request to move HCSEC to a larger building to facilitate any further expansion. Subsequently the Managing Director of HCSEC is developing appropriate business plans and budget proposals in order to implement an enhanced operational model, agreed with GCHQ Technical Authority, to help overcome current recruitment, operational and accommodation related issues.

~~~~~
~~~~~

SECTION II: The work of the Board: Technical assurance

2.1This section provides an account of the Board's consideration of the technical work of HCSEC as part of its assurance function.

HCSEC's technical assessments

2.2 HCSEC performs what are known as solution evaluations, as well as product evaluations. Product evaluations are security evaluations where the test is generally done in isolation, without information about the intended deployment. Products can be either individual products, such as a Multi-Service Access Node (MSAN), or a product set, for example a Single Radio Access Network (SRAN) which contains, on average, four separate equipment types. Solution evaluations are where the products are tested in the context of the wider service provider network.

2.3 In 2014, HCSEC completed four solution evaluations, with a fifth underway, as well as five product evaluations. It has also completed a small number of evaluations for non-UK networks, which have been previously agreed by GCHQ[4].

2.4 GCHQ's view, conveyed to the Oversight Board, is that these reports have been of consistently high quality and have provided useful risk management information to the UK Government, the CSPs and Huawei.

2.5 Potential vulnerabilities identified during this work are tracked and managed through Huawei's corporate defect tracking system, with continued engagement with the relevant research and development (R&D) teams to ensure they are properly resolved. HCSEC has also provided over 100 reports back to Huawei

[4] HCSEC can undertake work for customers in other countries, subject to Huawei approval, providing it completes in full its obligations within the UK. At present, this non-UK work is undertaken by the same people that perform UK related work, so any such arrangements are currently subject to further agreement by the UK Government. There are currently two active arrangements of this nature. In such cases it is the relevant foreign Government, not the UK Government, that is the beneficiary of the arrangement. Paragraphs 1.1 and 1.2 of Appendix C of this report provide more detail about this arrangement.

R&D in China about security metrics and any practices of concern. This work is part of a wider programme, which the UK Government has strongly encouraged to improve Huawei R&D's engineering and security quality continuously. The Government believes this general increase in the standard of Huawei's cyber security is of value to the UK risk mitigation strategy and is starting to show benefits.

2.6 Over the course of 2014, HCSEC's operational methodology has evolved to look much more at the broader network context and formal threat models. Its internally-developed tools for its response have similarly evolved. In 2014, HCSEC research has delivered a set of tools specifically targeted at Huawei products. These include tools which automate testing, help analysts discover security issues more quickly and identify areas of high risk that should be prioritised for analysis. In technical terms, this has included a vulnerability discovery tool based on abstract syntax trees, taint analysis tools, symbolic execution engines, tools to infer characteristics of binaries (including binary equivalence) and signature-based vulnerability finding for known vulnerabilities, to find repeats across a very diverse code base. Some of these tools are state-of-the-art and are highly efficient because they can automate some activities. This leaves skilled researchers time to do further development and undertake more complex work.

Staffing and skills

2.7 Recruitment remains a problem across the cyber security sector. However, in GCHQ's view HCSEC has a set of good technical staff from a wide range of technical backgrounds.

2.8 Between 2013 and 2014, HCSEC's overall headcount has risen from 21 to 25. It is modelled on expected work from CSPs with an additional headcount provision allocated for contingency. During this period, nine new staff members were recruited whilst five left the organisation. However, recruitment of new staff continues to prove difficult and HCSEC is currently carrying four vacancies. Recruitment to the Centre is hindered by two key factors; the national shortage of cyber security skills (a difficulty that is shared by both government and elsewhere in industry); and the requirement that staff are UK nationals who are able, and willing, to obtain the required clearance (DV). Some new recruits, when asked to complete the security questionnaires for the necessary DV clearance, have resigned at that stage in the process.

2.9 In order to address the recruitment shortfall, HCSEC are proactively engaged with three recruitment agencies and have taken on board a further two specialist recruitment agencies during 2014. The Centre has also taken several other steps aimed at improving the position on recruitment. They have posted five press advertisements for Security Analysts on three separate online job boards (Total Jobs, Indeed and Jobserve) and have also sought personal recommendations for new recruits from existing staff; this approach has successfully resulted in three new joiners. Analyst staff from HCSEC have also manned stands at exhibitions, including CREST (Council of Registered Ethical Security Testers) and the Cyber Security Expo, to attract new interest. They have proactively engaged, through their corporate membership, with the Institute of Information Security Professionals (IISP), including participating in discussions on career frameworks and skills.

2.10 In terms of addressing the longer term recruitment pipeline, HCSEC have funded a sponsorship position for an MSc at Warwick University under the Cyber Security Skills Alliance Sponsorship Scheme, established jointly by the Institute of Engineering and Technology (IET), the British Computer Society (BCS) and the IISP. HCSEC are also considering opportunities such as the development of guest lectures at Warwick University and an industry mentoring scheme for students.

2.11Although HCSEC is not yet fully staffed, it has so far been able to meet all current technical and business requirements and in the course of the audit of HCSEC (which is summarised more fully in the next chapter), Ernst and Young sought and obtained feedback on the Centre’s performance from a number of CSPs who use the facility. The CSPs fed back that whilst it can be difficult for HCSEC to obtain staff with the right technical skills who can understand the business environment into which the technology can be deployed, who can be DV cleared and who are willing to work in Banbury, HCSEC are considered to be doing a good job in developing and retaining capability despite these constraints. In order to sustain the current service levels with the expected workload for 2016, the current vacancies will need to be filled.

2.12 Steps are being taken to address personal development of staff at HCSEC to encourage retention. For example, staff have started to attend well known security research conferences and HCSEC intend to contribute in those fora. A new technical career framework is now in place to support formal technical progression amongst HCSEC staff in order to sustain the growing technical competence of the workforce. Although at an early stage, roll out and implementation of the framework is now underway.

2.13 HCSEC will implement an enhanced operational model in 2015 and 2016. This includes splitting project work into two broad categories; product security testing and detailed solution evaluations. Product security testing will include the running of automated, COTS (Commercial off the shelf) and HCSEC bespoke security tools. These activities do not require the same skill set as existing analyst staff, who will focus on complex in depth analysis security research. This approach is designed to enable HCSEC to recruit from the established, and far greater, UK pool of software testing professionals. As a consequence, HCSEC will continue to deliver against all agreed programmes of work, while also providing a sustainable and scalable team.

Technical relationships with Huawei HQ

2.14 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. There have been recent improvements to the relationship between HCSEC and PSIRT, but the Board would like to see the relationship transition further to enable effort sharing over managing vulnerabilities. Although the current relationship has occasionally caused some tensions, the Board is satisfied that this issue has not had a detrimental effect on the security of UK networks.

Recruitment of a new HCSEC Managing Director

2.15 In its second meeting the Oversight Board agreed a process for finding a new Managing Director of HCSEC to replace Andy Hopkins when he retires shortly. The Board placed on record its gratitude to Mr Hopkins for his first rate leadership of HCSEC in its crucial formative years.

2.16 The agreed process was that Odgers Berndston recruitment consultancy would run a process to find suitable candidates within a job specification drafted by Huawei (given that it is the company that employs and pays for the individual) but agreed with GCHQ. Following that process 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, Technical Director of GCHQ, and John Suffolk, Huawei’s Global Cyber Security Officer (and a former Cabinet Office senior civil servant). Mr Hopkins joined the panel in an advisory capacity at the invitation of the Chair.

2.17 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. He 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 holds Developed Vetting clearance.

2.18 The process for recruiting the new Managing Director was therefore, ultimately, a very successful one. However, in the view of the UK Government, it took too long and was overly complex. Huawei has indicated that it will work with the Government to optimise the process in the future.

Conclusion: technical assurance

2.19 Overall, given this account of both the technical assurance work of HCSEC to date and the position around staffing and skills, GCHQ has advised the Oversight Board that it is confident that HCSEC is providing the technical assurance of sufficient scope and quality as to be appropriate for the current stage in the assurance framework around Huawei in the UK. The position on staffing and skills will need to continue to be monitored as the strategy progresses and the Board will need to continue to review progress on recruitment closely at each meeting. The appointment of a renowned cyber security expert to lead the next phase of the Centre's work is a positive sign that this improvement will continue.

~~~~~
~~~~~

SECTION III: The work of the Board: Assurance on independence and the other work of the Board.

3.1 This section focusses on the more general work of the Board beyond its oversight of the technical assurance provided by HCSEC. In this regard, the most important function undertaken by the Oversight Board in its first year was the commissioning and consideration of 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 in support of UK national security. The audit was an unusual exercise in that the principal question for examination was whether HCSEC had the required operational independence from Huawei HQ to fulfil its obligations under the set of arrangements reached between the UK Government and the company in 2010. This section provides an account of the process by which the audit took place, and a summary of the key findings.

Appointing Ernst and Young to conduct the Management Audit

3.2 GCHQ invited three audit houses to consider undertaking the management audit and to seek their recommendation as to the appropriate audit standard and process to be followed[5]. The Oversight Board also approved a recommendation from GCHQ's procurement team that a single tender approach should be taken[6]. The contract was awarded to Ernst and Young LLP (E&Y).

3.3 The Oversight Board agreed a three stage approach to the audit:

i. an initial phase to undertake the preparatory work involving Ernst and Young, GCHQ and HCSEC agreeing the scope and key issues for review;

[5] The Oversight Board accepted GCHQ's recommendation that audit standard ISAE3000 should be used. ISAE3000 is an internationally accepted auditing standard which is designed to be flexible in the controls it audits, how it audits them and how the conclusions are reported. It is recognised to provide a reasonable level of assurance.

[6] GCHQ legal advisers confirmed that the audit work was covered as a piece of national security work and as such was exempt from public procurement regulations.

ii. a second phase to run a 'test' audit against the criteria identified above to ensure the Board were content and there was opportunity for any issues to be addressed;

iii. a final phase comprising the full audit report, given to the Board in January 2015.

The nature and scope of the audit

3.4 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; Personnel; Procurement; Evaluation Programme Planning; Cooperation and Support from elsewhere in Huawei and; Evaluation Reporting.

Headline audit findings

3.5 The HCSEC Annual Management Audit January 2015 comprised a rigorous evidence-based review of HCSEC processes and procedures. The audit report was produced by a team of four 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 a Senior Ernst and Young partner.

3.6 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 HCSEC control environment in place at the time of our work, effectively supports the independent operation of HCSEC, in all material aspects, based on the assessment criteria set out under "Audit Scope and Assessment Criteria[7]"'

3.7 The audit report usefully identified three control weaknesses within the HCSEC control environment for the Board to consider. These were presented to

[7] Page 3 of the HCSEC Annual Management Audit Jan 2015

the Board in its December meeting, based on the interim findings, with an Ernst & Young Executive Director in attendance to brief the Board. The Oversight Board discussed each of the three areas and agreed that each should formally be rated as ‘Low’ in terms of the overall risk to HCSEC’s independence. Nonetheless the Board emphasised that all three issues needed to be examined and they agreed an approach for each one.

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

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

3.9 Replicating the arrangements in place elsewhere in Government, GCHQ has developed a risk-managed approach whereby the HCSEC Management Board closely monitors all new entrants’ access and work.

3.10 New recruits are not allowed in the facility without DV cleared staff present. Additionally these individuals do not contribute directly to the production of security evaluation reports. Until their DV clearance is granted, they remain on probation with all of their work thoroughly peer reviewed by senior DV cleared staff. The new recruits also have clear objectives set and there is close management of their progress by DV cleared staff throughout probation period. Ongoing retention of their DV, which is refreshed on a bi-annual basis, is a condition of their continued employment at HCSEC.

3.11 Although Ernst and Young found four staff working who had not yet received their DV clearance, during their work in November 2014, this has now been reduced to two.

3.12 GCHQ is also responsible for ensuring that new staff receive a security briefing and sign the Official Secrets Act within a few weeks of joining. In addition, a new starter process is now in place, requiring all clearance paperwork to have been submitted for processing within a month of staff joining. Each case is then assigned to one of two dedicated GCHQ vetting officers whose primary task is to undertake the HCSEC clearances, in consultation with the HCSEC management team.

3.13 It is important to note that HCSEC staff who are awaiting DV are only employed if they are engaging fully with the clearance process (and therefore it is no fault of theirs if there is a delay). Where an employee is not engaging properly with the security clearance process they will not be able to work in HCSEC. Over the last year, two members of staff on probation have left the company in circumstances related to unsatisfactory engagement with the DV process. One of these was dismissed.

3.14 The Oversight Board recognises that despite mitigations, it is still not ideal for even a small number of staff to operate within HCSEC, for relatively short periods of time, while awaiting DV clearance. However the Board accepts that this is not the fault of the company and is the result of a wider backlog in the vetting system, which is the responsibility of the Government. The choice in these circumstances is between leaving HCSEC short-staffed, or putting in place specific mitigations to manage any risk. The Board is satisfied that in choosing the latter approach, HCSEC, in conjunction with GCHQ, is taking appropriate steps. The Board will continue to pay very close attention to this issue. However at present we do not consider it a serious risk.

Allocation of bonus payments by Huawei

3.15 A second issue was the payment of annual bonuses for staff within HCSEC which had previously been calculated by the Huawei UK senior management board, based on company criteria. HCSEC management were only notified of the bonuses after they had been issued by Huawei HR so HCSEC management were not able to review or approve the bonuses. In future, HCSEC management will review final bonus allocations to confirm that they appear in line with expectations. As this is an annual process, it will be followed for the first time during the year end appraisal process in 2015. Assuming this is the case, this issue can be considered closed.

Internal budgeting processes

3.16 The third issue is that the current HCSEC internal budgeting process does not document formal agreement and sign-off from HCSEC contributors. In response to this point, HCSEC management has updated the process documentation to define the requirement for email evidence to be retained to show approval at all key stages in the internal budgeting process. As above, this is an annual process which will be followed for the first time during the year end appraisal process in 2015. Again, assuming this is the case, this issue can be considered closed.

Issues identified that were out of scope of the audit

3.17 The audit also highlighted four potential issues in the governance surrounding HCSEC, which fell beyond the formal scope of the audit. They were; Use of HCSEC evaluation resources on non-UK product deployments; Communication of key evaluation decisions; Potential to use the Oversight Board as a point of escalation and; Formalising the understanding of 'senior management' in HCSEC. These four areas are described in more detail in in **Appendix C**, together with their respective mitigations agreed at the December Oversight Board. Whilst outside the scope of the audit they nonetheless proved useful insights into the potential areas where Government oversight of HCSEC could be improved.

Overall Oversight Board conclusions of the audit

3.18 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. Three issues of concern – rated collectively by the Board as of overall low risk – have been identified. Two of these have been dealt with and the other – delays in vetting procedures leading to individuals working for short periods of time without clearance – is being kept closely under review. Additionally the audit has led to useful improvements in the formal governance arrangements in the event of difficulties or unforeseen changes to the work of HCSEC.

~~~~~
~~~~~

SECTION IV: Conclusions

4.1 The Oversight Board has now completed its first full year of work. Its four meetings, and work out of Committee, have provided a useful enhancement of the governance arrangements for HCSEC.

4.2 The key conclusions from the Board's first year of work are:

- On GCHQ's advice, the Board accepts that the technical assurance provided by HCSEC was of sufficient scope and quality to meet its obligations under the 2010 arrangements between the UK Government and the company; and

- The management audit by Ernst & Young provides sufficient assurance that HCSEC has operated with sufficient independence from Huawei Headquarters and any other body in a manner consistent with its obligations under the same arrangements;

- A key focus for the Board in the next year will be monitoring the position on both recruitment and vetting, acknowledging that the recruitment market is challenging, and that solving the vetting backlog is not in the company's gift. Neither problem has, however, in the view of the Board, given rise to any operational failings; and

- Via the Oversight Board mechanism, the Government has once again emphasised to the company the importance of the part of the arrangement that requires HCSEC to report to the Oversight Board any change to its operation, or the emergence of any other factor that affects HCSEC's security posture.

4.3 Overall therefore, the Oversight Board concludes that in the year 2014-15 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 adds to Parliamentary – and through it – public knowledge of the operation of the arrangements.

~~~~~
~~~~~

Appendix A

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

1. Purpose

This Oversight Board will be established to implement recommendation two of the National Security Adviser's Review of the Huawei Cyber Security Evaluation Centre (HCSEC). The Oversight Board's primary purpose will be to oversee and ensure the independence, competence and therefore overall effectiveness of HCSEC and it will advise the National Security Adviser on this basis. It will work by consensus. However, if there is a disagreement relating to matters covered by the Oversight Board GCHQ, as chair, will have the right to make the final decision.

The Board is responsible for assessing HCSEC's performance relating to UK product deployments. It should not get involved in the day-to-day operations of HCSEC.

2. Scope of Work

2.1 In Scope

The Oversight Board will focus on:

- HCSEC's assessment of Huawei products that are deployed or are contracted to be deployed in the UK and are relevant to UK national security risk.
- The independence, competence and therefore overall effectiveness of HCSEC in relation to the discharge of its duties.

2.2 Out of Scope

- All products that are not relevant to UK national risk;
- All products, work or resources for non UK-based deployment,

including those deployed outside the UK by any global CSPs which are based in the UK;
- The commercial relationship between Huawei and CSPs; and
- HCSEC's foundational research (tools, techniques etc) which will be assessed and directed by GCHQ.

3. Objectives of the Oversight Board

3.1 Annual Objectives and Report to the National Security Adviser

To provide a report on the independence, competence and effectiveness of HCSEC to the National Security Adviser on an annual basis, explicitly detailing to what extent HCSEC has met its in-year objectives as set by the Board. This will draw upon the Annual Management Audit, the Technical Competence Review and will specifically assess the current status and the long term strategy for resourcing HCSEC.

All UK CSPs that have contracted to use HCSEC for assurance in the context of management of UK national risk for deployments shall be consulted.

In the event of a change to the operation of HCSEC, or the emergence of any other factor that affects HCSEC’s security posture, HCSEC will report this to the Oversight Board in a timely manner. GCHQ [or any other member of the Oversight Board] shall also be expected to inform the Oversight Board of any factor which appears to affect the security posture of HCSEC.

3.2 Commission Annual Management Audit

To assure the continued independence of HCSEC from Huawei HQ, the Oversight Board will commission a management audit to be performed by security cleared UK auditors; this will be funded by UK Government. The scope of the audit shall be as set out in the Huawei HQ Letter of Authorisation (Operational Independence) to HCSEC (as set out in Annex 3), or other agreed standards, as agreed by the Oversight Board. This will include the independence of budget execution and whether HCSEC were provided with the timely information, products and code to undertake their work.

The Oversight Board will ensure the scope of any such audit is appropriate and the auditor shall be agreed by the Chair and Deputy Chair.

The audit report mentioned in section 3.2 and 3.3 shall be treated as confidential information and subject to section 8.

3.3 Commission Technical Competence Review

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

3.4 Process to Appoint Senior Management Team

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

3.5 Timely Delivery

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

3.6 Escalation / Arbitrator for issues impacting HCSEC

In the event that an issue arises that may impact either the independence, effectiveness or the security posture of HCSEC, the oversight board should be informed in a timely manner, 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[8]. 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.

[8] 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.

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.

11. Annex – 3- Huawei HQ Letter of Authorisation (Operational Independence) to HCSEC

This Huawei HQ Letter of Authorisation to HCSEC has also been removed due to commercial sensitivities but is contained in the full version of the ToRs.

Appendix B

HCSEC Oversight Board membership for the period of the Oversight Board report 2014-15

Ciaran Martin, DG for Cyber Security at GCHQ (Chair)

Ryan Ding, Executive Director of the Board and President, Products and Solutions Huawei Technologies (Deputy Chair)

Huawei UK Executive Director

Managing Director HCSEC

GCHQ Technical Director

Director of the Office for Cyber Security and Information Assurance at the Cabinet Office

Deputy Director of the Office for Cyber Security and Information Assurance at the Cabinet Office

Deputy Director Cyber Security and Resilience, Digital Economy Unit, BIS

Director of the Office for security and Counter Terrorism, Home Office

Vodafone Group External Affairs Director

President, BT Security Enterprise, BT Global Services

Appendix C

HMG issues out of scope of the audit

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

1.1 HCSEC is a company resource that is required, by virtue of its arrangement with the UK Government, to fulfil various functions in order to provide assurance on the national risk to the UK from Huawei's involvement in critical networks. To ensure obligations to the UK Government can be satisfied, any other corporate use of the expertise in the Centre must first be agreed between Huawei and the Oversight Board. A small amount of work is therefore carried out from the Centre for non-UK customers. In the event of non-UK based work going forward, Huawei HQ will consult with HCSEC MD in order to avoid potential resource conflict with UK based activity.

1.2 The Oversight Board remains satisfied that HCSEC is fulfilling its obligations to the UK Government and that there has been no adverse impact on its UK facing outputs from its other work. The audit report did however query what would happen in the event that this was not the case. There is provision for this in the Oversight Board Terms of Reference which states that '*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*'.

2. Communication of key evaluation decisions

2.1 In a similar vein the audit also identified a potential lack of formal mechanisms for updating the Board about any significant reductions or limitations to planned evaluations, with 'significant' defined as 'where the lack of particular information or the lack of ability to perform a particular task would materially reduce the levels of assurance attained through the work of HCSEC'. That is not to say that such changes would not be made known to the Government; they would be of course notified to GCHQ as part of its ongoing direct engagement with HCSEC on its work programme. Indeed it could reasonably be expected to come to light to the Board in preparation of its annual report. However, to ensure there is no gap in time in the event of such a situation, the Board has agreed that in the event of any significant reduction, as defined above, GCHQ and HCSEC should formally commit jointly to providing the Oversight Board with an account of the situation for its consideration. Again, it is important to note that such a situation has not occurred and this is about a potential scenario.

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

3.1 The audit also looked at other areas where a greater degree of formality in the governance arrangements might be useful in the event of any serious tension in the relationship. As a result, the Oversight Board agreed to amend its Terms of Reference to enable explicitly the Board to act as a point of escalation and arbitrator of any such issues by convening and an extraordinary session. The ToRs at Appendix A reflect this amendment.

4. Formalising the understanding of 'senior management' in HCSEC

4.1 Finally, the auditors note that the term 'senior management' of HCSEC was used in a number of formal documents without any formal specification as to what that referred to. The Oversight Board agreed that HCSEC senior management should be understood as meaning the Centre's:

- Managing Director;
- Technical Director;
- Solutions and Programme Director.