华为网络安全评估中心（hcsec）监督委员会

2019年年度报告

2019年3月向英国国家安全顾问提交的报告

华为网络安全评估中心监督委员会年度报告

第一部分：总结

1. 这是华为网络安全评估中心（HCSEC）监督委员会的第五份年度报告。HCSEC是牛津郡班伯里的一家工厂，隶属于华为技术（英国）有限公司（华为英国），其母公司华为技术有限公司是一家总部位于中国的公司，现在是全球最大的电信供应商之一。

2. HCSEC已经运行了八年。它于2010年11月根据华为与女王陛下政府（HMG）之间的一系列安排开放，旨在减轻华为参与英国（英国）部分重要国家基础设施所带来的任何风险。HCSEC为英国电信市场中使用的一系列产品提供安全评估。通过HCSEC，英国政府可以深入了解华为的英国战略和产品系列。英国国家网络安全中心（NCSC和以前的政府通信总部（GCHQ））作为国家信息保障技术机构和政府网络安全运营机构，领导政府与HCSEC和华为打交道。关于技术安全问题。

3. HCSEC监督委员会成立于2014年，由NCSC首席执行官Ciaran Martin担任主席，并担任GCHQ董事会执行委员，负责网络安全。监督委员会继续包括华为高级主管作为副主席，以及来自政府和英国电信部门的高级代表。监督委员会的结构没有发生重大变化，但成员资格在2018年发生了变化。主要是由于HMG和华为职位的员工轮换。

4. 监督委员会现已完成其第五个全年工作。在这样做的过程中，它涵盖了HCSEC在一年中的几个工作领域。这项工作的全部细节载于本报告第二部分。在本摘要中，主要亮点是：

   i. HCSEC的新安全楼宇已经完工 – 先前报告的HCSEC新楼宇的购置经历了一些商业延误，但现已成功完成，新设施全面运作；

   ii. NCSC技术能力评估发现，HCSEC的能力在2018年有所改善，员工素质并未降低，这意味着与整体缓解策略相关的技术工作可以大规模，高质量地进行；

   iii. 对HCSEC独立于华为总部运营的能力的第五次独立审计已经完成，再次 – 没有高优先级或中等优先级的调查结果。审计报告确定了一项低评级的调查结果，涉及在商定的服务水平协议内提供信息和设备。安永认为没有重大问题，监督委员会对HCSEC的运作符合HMG与公司2010年的安排表示满意；

   iv. **华为工程流程中发现了更多重大技术问题，导致英国电信网络出现新风险；**

   v. 华为在去年报告的问题的修复方面没有取得任何重大进展，因此不适合改变去年的保证水平或对潜在的未来保证水平作出评论。

5. 监督委员会第五年工作的主要结论是：

谢谢观看！

i. 2018年，HCSEC履行了向NCSC和英国运营商提供软件工程和网络安全保障文物的义务，作为管理华为参与英国关键网络对英国国家安全风险的战略的一部分；

ii. 然而，正如2018年报道的那样，HCSEC的工作继续确定华为软件开发方法中的问题，为英国运营商带来了显着增加的风险，这需要持续的管理和缓解；

iii. 在2018年以前的报告中提出的问题没有取得重大进展；

iv. 监督委员会继续只能提供有限的保证，即可以在目前英国部署的华为设备中管理长期安全风险；

v. 监督委员会建议，在英国部署的背景下，很难对未来产品进行适当的风险管理，直到华为软件工程和网络安全流程的根本缺陷得到纠正为止；

vi. 目前，监督委员会还没有看到任何让华盛顿成功完成其转型计划要素的能力，而该计划已提出解决这些潜在缺陷的方法。理事会将要求持续证明HCSEC和NCSC验证的更好的软件工程和网络安全质量；

vii. **总体而言，监督委员会只能提供有限的保证，即华为参与英国关键网络对英国国家安全的所有风险可以在长期内得到充分缓解。**

此页有意留为空白

第二部分：技术和运营报告

这是华为网络安全评估中心（HCSEC）监督委员会的第五份年度报告。该报告可能包含一些更广泛的华为公司战略和非英国利益的参考。值得注意的是，监督委员会在这些问题上没有直接的位置，只有它们可以影响与HCSEC英国业务保证直接相关的结论。英国政府对这些非英国安排的兴趣仅限于确保HCSEC有足够的能力履行其对英国的商定义务。无论是英国政府还是整个董事会，在这个过程中都没有任何其他地方。

介绍

1. 这是华为网络安全评估中心（HCSEC）监督委员会的第五份年度报告。HCSEC是牛津郡班伯里的一家工厂，隶属于华为技术（英国）有限公司（华为英国），其母公司是一家总部位于中国的公司，华为技术有限公司，现在是全球最大的电信提供商之一。

2. HCSEC已经运行了八年。它于2010年11月根据华为与HMG之间的一系列安排开放，旨在减轻华为参与英国部分重要国家基础设施所带来的任何风险。HCSEC为英国市场上使用的一系列产品提供安全评估。通过HCSEC，英国政府可以深入了解华为的英国战略和产品系列。英国国家网络安全中心（NCSC，以前是GCHQ）作为国家信息保障技术机构和政府网络安全运营机构，领导政府与HCSEC和华为进行更广泛的技术安全事务处理。

3.　HCSEC监督委员会成立于2014年，由NCSC首席执行官Ciaran Martin担任主席，并担任GCHQ董事会执行委员，负责网络安全。监督委员会继续包括华为高级主管作为副主席，以及来自政府和英国电信部门的高级代表。监督委员会的结构没有发生重大变化，但成员资格在2017 – 18年度发生了变化。这主要是由于HMG和华为职位的员工轮换。

4.　第五份年度报告已得到监督委员会成员的一致同意。与去年的报告一样，理事会同意不需要机密附件，因此本报告中的内容代表了全面的分析和评估。

5.　报告载列如下：

I.　第一节规定了监督委员会的职权范围和成员资格；
II.　第二节描述了HCSEC的人员配置，技能，招聘和住宿；
III.　第三节涉及HCSEC技术保障，优先排序和研发；
IV.　第四节总结了2018年独立审计的结果；
V.　第五节汇总了一些结论。

第一部分：HCSEC监督委员会：职权范围和成员资格

1.1 HCSEC监督委员会于2014年初成立。它每季度召开一次会议，由NCSC首席执行官Ciaran Martin和GCHQ总干事董事会执行成员担任主席。Martin先生直接向GCHQ的董事Jeremy Fleming报告，并负责该机构的网络安全工作。

1.2 监督委员会的职责是监督和确保HCSEC的独立性，能力和整体有效性，作为整体缓解战略的一部分，以管理华为在英国的存在并在此基础上为国家安全顾问提供建议. .然后，国家安全顾问将向部长，议会和最终公众保证风险是否得到妥善管理。

1.3 监督委员会的范围仅涉及与英国国家安全风险相关的产品。它的职责是双重的，涵盖：

- 首先，HCSEC对华为部署或签约将在英国部署的产品的评估与英国国家安全风险相关，该风险由NCSC自行决定;和
- 第二，HCSEC在履行职责方面的独立性，能力和整体效力。

1.4 理事会有一份商定的职权范围，其副本见附录A.今年的职权范围没有变化，监督委员会的职权范围和目标保持不变。监督委员会负责向国家安全顾问提供年度报告，国家安全顾问将向国家安全委员会和议会情报和安全委员会（ISC）提供副本。

董事会的目标是HCSEC

1.5 监督委员会对HCSEC的四个高级目标与之前报告的目标保持一致，并且：

- 为年度HCSEC评估计划中定义的一系列英国客户部署提供安全评估；
- 通过确保对政府和英国客户安全问题的公开性，透明度和响应能力，继续向英国政府提供保证；
- 通过提高评估产出质量或开发定制的安全相关工具，技术或流程，证明技术能力的提高；
- 为HCSEC支持华为研发，继续发展和提升华为的软件工程和网络安全能力。

HCSEC监督委员会：2018年4月至2019年2月

1.6 本报告涵盖2018年1月至2018年12月期间的技术工作。上一份报告涵盖了2018年3月的监督委员会会议。在自2018年年度报告发布以来的五次会议中，监督委员会：

- 提供华为英国的定期公司更新；
- 讨论了未来的技术趋势以及它们如何影响监督委员会的工作；
- 提供有关HCSEC招聘，人员配置和住宿计划的定期更新；
- 收到NCSC技术总监和技术团队（一些与英国运营商）在深圳和上海对华为总部进行技术访问的详细报告，以讨论技术问题；
- 进一步证实了去年出现的重大软件工程和网络安全问题的根本原因；
- 进一步证实了华为提出的重大软件工程和网络安全问题的补救措施，并判断它们不足；
- 委托第五次HCSEC管理层审核中心的独立性。

第二部分：HCSEC人员配备

2.1　本节介绍了HCSEC的人员配备和技能，包括招聘和保留。

人员和技能

2.2　NCSC领导HMG与HCSEC以及公司更广泛地处理技术安全问题。NCSC代表HMG赞助HCSEC员工的安全许可。一般要求是所有工作人员必须具有开发审查（DV）安全许可，这与政府频繁，不受控制地访问机密信息所需的级别相同，并且对于情报部门的成员是强制性的。HCSEC的新招募人员在试用期间受到护送管理，等待其DV清除期（通常为六个月）完成。

2.3　HCSEC的人员配备增加与2018年的预期一致。截至本日历年年底，员工人数为38人（以“接受报价”为就业点）。

2.4　HCSEC继续招募技术网络安全专家来管理自然减员和继任仍然至关重要。HCSEC领导层持续的个人参与推动了这一持续的良好进展，并代表了大量的工作。

2.5　今年再次，由于清关要求，大量潜在的新兵被筛选出来。此外，一名通过初步筛选并被HCSEC聘用的候选人随后未通过DV检查，并被从中心移除。通过在试用期内提供的监督和监督，对与此人相关的小风险进行了充分的管理。

住所

2.6　上一份报告谈到成功寻找新的住宿条件，以应对所需的扩建，以及完成延迟。该

由于与建筑物配置和搬迁后勤相关的原因，该报告中提到的延误得以实现。但是，这一过程今年已成功结束。所有HCSEC工作人员都转移到新设施，并且在2018年11月之前安装了IT和代表性客户网络。所产生的延迟绝不是华为总部不采取行动或干扰的结果。

2.7　新设施旨在安全地应对HCSEC承担的敏感工作，同时确保满足华为知识产权保护标准。HMG安全团队对该建筑进行了足够安全的评估，并且还获得了华为总部团队对其适用于保存所有华为源代码的认可。

2.8　新的住宿将支持并发参考网络的部署，使产品和解决方案评估能够按计划进行。它还有助于增加开发活动，以支持需要评估的大量产品。

2.9　应该指出的是，HCSEC的2018年预算是2017年预算的160%，尽管其中一部分与移动成本和其他一次性费用有关。

2.10　总体而言，2018年期间在住宿，人员配备和技能方面取得了良好进展。监督委员会的季度监测表明，工作人员及其技能的数量没有引起关注。新住宿的延误是不幸的，但此举已成功完成，对HCSEC的工作没有重大影响。

~~~~~
~~~~~

第III（a）节：HCSEC技术保证

3.1 2018年是政府积极管理华为在英国电信网络中的第15个年头，这是政府在英国和监督委员会第五年的华为延长风险管理计划的第八个年头。在之前的四份报告中，监督委员会包括了当年华为产品评估结果的一些基本技术细节。这对于理事会向国家安全顾问提供明确和全面的保证是必要的。本报告涵盖监督委员会2018年3月至2019年2月期间的活动，但报告2018年1月至2018年12月期间的技术工作，更新了先前报告中提出的技术立场，并在必要时进一步阐述，以解释监督的结论。董事会已达成技术保证和HCSEC有效性，以及其对如何在未来减轻风险的意见。监督委员会认为有必要提供本报告中包含的技术细节，以履行其报告职能。特别是，监督委员会认为，提供这一细节对于解释和证实其与前几年相比降低保证水平的决定是必要的，并且还有助于那些目前没有在监督委员会中有代表的经营者了解他们可能面临的风险。在他们的网络中。本节包括NCSC向监督委员会提交的报告，分为两部分。第一部分概述了HCSEC所做的工作以及从中获得的高级结果，以及有关技术保证和HCSEC有效性的结论。第二部分提供详细的技术信息，旨在帮助读者理解为什么达到这里的结论。

HCSEC评估流程

3.2 HCSEC在2018年的评估计划延续了近年来的产品和解决方案评估。2018年，完成了39项产品评估，完成了3项解决方案评估，另一项计划于2019年初完成。总体而言，这大致符合年初商定的计划。评估涵盖了五家英国运营商的产品和架构。这个节奏是

尽管纳入了大量非评估工作，以支持监督委员会的行动和搬迁到新房地，但仍保持不变。

3.3　　NCSC的目标是要求HCSEC至少每两年对英国的所有相关产品进行产品评估，平均而言，这些产品得到满足。HCSEC的产品评估管道仍然配置为实现这一目标。监督委员会相信，HCSEC老年人的持续关注将确保有足够的技术熟练的员工继续满足非公务员合约的目标。HCSEC员工必须能够获得安全许可并具备必要的技能，这意味着可用人才库很少。由于有足够的空间和基础设施来同时维护多个代表性网络，消除了大部分拆除并为评估工作留出了时间，因此HCSEC迁移到新办公楼将有助于为评估渠道提供服务。

3.4　　评估过程将继续发现点漏洞和更具战略性的架构和流程问题，详见本节后面部分。华为继续进行整治工作;HCSEC向英国运营商，NCSC和华为研发部门提供的反馈意见继续保持高质量，HCSEC技术人员继续协助华为研发团队进行整治。

HCSEC计划建立和优先排序

3.5　　先前监督委员会报告中详述的基于风险的优先排序方案在2018年期间继续适用。

程序构建过程与前几年大致相同。英国运营商，NCSC和HCSEC合作确定了HCSEC的优先事项。这对于平衡有时相互竞争的约束和要求以实现英国的最佳整体利益是必要的，例如，由于商业压力，不允许任何特定的运营商不公平地支配工作计划。最终计划由NCSC技术总监或NCSC电信技术总监代表监督委员会签署，并在年内由HCSEC进行审查。如果HCSEC认为有必要修改该计划，那么涉及NCSC和相关部门的轻触过程

运营商用于管理和批准任何修改。除了为评估渠道提供服务外，HCSEC还做了大量工作，支持监督委员会在上一份报告中征收的目标，以支持华为研发部门加强华为软件工程和网络安全能力的工作，从而开始纠正已发现的潜在问题在此报告和之前的报告中。

3.6 尽管华为参与英国电信行业的规模和范围意味着HCSEC需要管理的工作量很大，但在设备的高级优先级方面几乎没有变化。目前，HCSEC很好地管理该管道，始终满足NCSC和英国运营商的期望。HCSEC的工作成果直接向运营商报告，他们希望将其纳入企业风险管理流程。

HCSEC技术工作和高级别调查结果概述

3.7 HCSEC和NCSC在2018年进行了大量技术工作，NCSC已经对职权范围第3.3段设想的监督委员会进行了审计。该部分的后半部分提供了该工作的详细信息，但为方便起见，此处提供了高级结论和结论。

- 华为提供了四种产品来测试二进制等价。HCSEC对其进行验证的工作仍在进行中，但已经暴露了底层构建过程中的更广泛的缺陷，需要在大规模展示二元等价之前对其进行纠正。NCSC已告知监督委员会，优先应该是纠正这些潜在的缺陷，作为华为转型计划的一部分。除非并且直到完成，否则不可能确信HCSEC检查的源代码正是用于构建在英国网络中运行的二进制文件的源代码。
- 由于各种与构建相关的问题，很难确信类似的华为设备的不同部署大致相当安全。例如，很难确信在一个版本中发现的漏洞是通过持续的正常操作在另一个版本中得到修复的。

工程过程。这样做的能力以及特定源代码集恰好用于构建特定二进制文件的端到端保证通常会被视为现代软件工程过程的副作用。

- 自2010年以来，由英国社区推动的华为配置管理改进尚未普遍应用于产品和平台开发组或跨配置项类型（源代码，构建工具，构建脚本等）。如果没有良好的配置管理，华为提供的产品就不会有端到端的完整性，对华为理解任何给定构建内容的能力或对所识别问题进行真正根本原因分析的能力缺乏信心. .
- 华为继续使用旧的，即将脱离第三方提供的知名且广泛使用的实时操作系统的主流支持版本。华为已经分别从供应商处购买了一份高级长期支持协议，以便在未来以商业上可行的方式解决漏洞，但单一内存空间，单用户环境安全模型带来的潜在网络安全风险仍然存在。NCSC认为目前没有可靠的计划来降低英国使用这种实时操作系统的风险。华为自己的等效操作系统与其他组件的许多华为开发流程相同，而NCSC目前没有足够的证据来判断该组件的软件工程质量和网络安全影响。此外，它采用了更现代的内存和安全模型，因此与运行在操作系统上的现有产品的集成带来了风险。这意味着迁移到这个实时操作系统可能不会长期改善这种情况，同时给英国运营商带来整合风险。华为，HCSEC，英国运营商和NCSC之间的工作仍在继续，以制定切实可行的计划，以减少英国网络因使用这种旧的第三方实时操作系统而产生的长期风险。但是，NCSC仍然关注自发现这个问题以来没有提出可靠计划的时间。

- 对华为更广泛的软件组件生命周期管理的分析揭示了导致重大网络安全和可用性风险的缺陷。这是一个重要发现，本节第二部分提供了更多细节。如果这是一个问题，现有代码库的修复以及允许系统发生的有缺陷的流程将需要进行重大整改。
- HCSEC进行了软件工程和网络安全趋势分析，比较了LTE eNodeB软件的后续主要版本。后来的版本旨在整合华为的所有改进，因此平均而言应该比以前的版本客观上更好。虽然有所改进，但产品的一般软件工程和网络安全质量仍然显示出大量主要缺陷。因此，NCSC仍然担心华为的软件工程和网络安全能力以及相关流程未能充分改进。
- 监督委员会要求华为提供计划，以修复LTE eNodeB产品开发和持续工程中的软件工程和网络安全问题，并由NCSC在英国运营商的支持下进行审核。提出的计划对NCSC和英国运营商来说是不可接受的。目前，NCSC并不相信华为能够解决其面临的重大问题。
- 针对其工程流程中发现的缺陷，华为向监督委员会提出了通过五年内20亿美元的投资改变其软件工程流程的意图。然而，这项拟议的投资虽然受到欢迎，但目前仅仅是针对尚未指明的活动的拟议初步预算。虽然对华为全球转型计划的正式监督不属于监督委员会活动的范围，但董事会希望看到转型计划的细节及其对英国网络中使用的产品的影响的证据，然后才能确信它将会推动更改。除非并且直到提供和审查详细计划，否则不可能对华为所解决的问题提供任何程度的信心。

- HCSEC继续发现华为产品的严重漏洞。向英国运营商报告了数百个漏洞和问题，以便在2018年为其风险管理和补救提供信息。在先前版本的产品中发现的一些漏洞仍然存在。

结论：HCSEC能力

3.8 NCSC继续认为，英国缓解战略（包括HCSEC执行技术工作和监督委员会提供保证作为两个组成部分）是管理华为参与英国电信部门风险的最佳方式。本报告中发现的问题的发现表明该模型正常工作。华为目前继续参与此流程。

3.9 HCSEC在2018年的工作继续为基础工具开发能力，以便为英国运营商和NCSC提供理解和技术安全文物。到2018年，HCSEC继续在华为产品中发现问题，展示了他们持续发现华为产品缺陷的能力。此外，2018年HCSEC在分析华为研发索赔方面做出了巨大努力，并且在一个异常复杂且控制不良的开发和构建过程中有效地逆转了工程根本原因问题。这需要卓越的技术技能和洞察力。

3.10 HCSEC继续拥有世界级的安全研究人员，他们正在创建新的工具和技术，以便英国社区了解华为独特的软件工程和网络安全流程在复杂的电信领域中对软件工程和网络安全的影响。

3.11 在核心网络安全工作方面，向英国运营商报告的漏洞和问题数量已增加到数百个。鉴于2018年进行的产品评估数量增加（2017年为39个，超过27个），这个数字与前几年基本一致。在以前的评估中报告的一些严重漏洞在新版本中仍然存在。

3.12 漏洞的特征在几年之间没有显着变化，许多漏洞影响很大（相当于高基数CVSS评分）

和相关的操作上下文），包括公共可访问协议中的无保护　　堆栈溢出，导致拒绝服务的协议健壮性错误，逻辑错误，加密弱点，默认凭据和许多其他基本漏洞类型。尽管华为强制要求在研发中应用其安全编码标准，广泛使用商业静态分析工具，并且华为坚持认为风险代码已被重构，但目标软件工程和网络安全质量几乎没有任何改进。HCSEC和英国运营商。

3.13　华为设备带来的英国电信基础设施的重大风险将继续需要由英国运营商管理，并且需要所有相关方的重大工作，以减少现有设备的风险。NCSC和英国运营商将继续与华为合作，为英国的设备制定可靠和可持续的补救计划。华为已同意英国设备的修复与华为可能做的任何其他工作无关，并且将及时发生。作为正常业务的一部分，监督委员会将判断HCSEC在此方面的有效性。目前尚不清楚，如本报告所述，可以为英国新设备制定类似的计划。

3.14　这些风险并非由于HCSEC的人员配置和能力问题，这些问题仍然是世界级的。监督委员会将期待HCSEC对华为选择对其开发过程所做的任何变更提供独立的观点，并确定所部署的最终产品的任何软件工程和网络安全提升的效果。

3.15　NCSC认为，HCSEC在技术安全领域仍然具备相关能力，可以向运营商，NCSC和监督委员会提供有关华为产品在英国电信基础设施中使用的产品和解决方案风险的建议。NCSC向监督委员会提交的报告是，HCSEC继续提供独特的世界级网络安全专业知识，以协助政府持续的风险管理计划，围绕华为设备与英国运营商的使用。

结论：对英国国家安全风险的影响

3.16　上述HCSEC的工作揭示了华为软件工程和网络安全能力的严重和系统性缺陷。因此，NCSC继续向监督委员会提出建议，因为NCSC尚未看到可靠的补救计划，因此仅对目前在英国部署的设备进行安全风险管理提供有限的技术保证是恰当的。即使这种有限的保证也只有在很大程度上归功于HCSEC的工作，才能在英国很好地理解华为设备的缺陷。鉴于这种知识，在极端情况下，NCSC可以指导华为对目前在英国的设备进行补救。这不应该被视为最大限度地减少这样做的难度或建议这是一种可持续的方法。在某些情况下，修复还需要更换硬件（由于CPU和内存限制），这可能是也可能不是自然运营商资产管理和升级周期的一部分。

3.17　鉴于良好的软件工程和网络安全实践的不足以及华为通过其宣布的转型计划目前未知的研发流程，很可能是对英国新产品或新的主要软件版本的安全风险管理目前在英国的产品将更加困难。根据HCSEC已经开展的工作，NCSC认为很可能在HCSEC尚未检查的产品中存在新的软件工程和网络安全问题。

3.18　糟糕的软件工程和网络安全流程会导致安全和质量问题，包括漏洞。HCSEC中相对较小的团队发现的漏洞的数量和严重性，以及架构和构建问题，都是一个特别令人担忧的问题。如果攻击者了解这些漏洞并充分利用它们，则它们可能会影响网络的运行，在某些情况下会导致其停止正常运行。其他影响可能包括能够访问用户流量或重新配置网络元素。但是，大多数英国运营商采用的架构控制限制了攻击者无法明确地与任何网络元素进行通信的能力

暴露给公众，在采取其他措施的情况下，更容易利用漏洞。这些架构控制以及英国运营商对网络的运营和安全管理在未来几年仍将是至关重要的，以管理由所识别的工程缺陷造成的剩余风险。这些调查结果涉及基本的工程能力和网络安全卫生，这些因素会产生一系列能够被各种行为者利用的漏洞。NCSC不相信所发现的缺陷是中国国家干预的结果。

第III（b）节：支持技术证据二元对等和软件一致性

3.19 一直是缓解策略的一部分，以确保HCSEC检查的源代码正是编译到英国网络设备中执行的二进制文件的源代码。如果没有一个流程来证明HCSEC检查的源代码和构建环境能够独特地生成在英国网络中部署的二进制文件，则无法在使用中的产品的安全性和完整性方面提供端到端的保证。面对华为极其复杂的构建过程，二元等价被认为是获得这种保证的临时步骤。值得注意的是，源到二进制链接的保证绝不会保证工程质量或安全性。之前的监督委员会报告了实现二进制等价的新流程的详细进展，即能够从HCSEC的源代码构建产品到华为研发生成的通用可用性（GA）版本的二进制等效（不一定相同）在中国。在之前的报告中，记录了单一产品 - 宽带头端 – 已经成功创建了可重复的构建，并且预计会立即部署此版本。遗憾的是，由于版本特定的依赖关系在今天的英国部署中无法满足，因此没有英国运营商能够部署此版本。

3.20 上一份报告中的预期是，来自LTE，EPC和光传输产品线的其余三种试验产品将在2018年上半年成为商用，可重复的GA版本。而华为研发的二进制文件已经通过在华为标记为GA的过程中，HCSEC的单独验证工作尚未完成。EPC产品的验证工作刚刚开始于2018年底，光传输产品已重新安排在2019年开始。与所有HCSEC计划的变更一样，这些变更与NCSC代表监督委员会达成一致。

3.21 HCSEC的任务是了解华为在创建可重复构建方面面临的问题。所有情况下的问题都在于华为的底层构建过程，它没有提供端到端的完整性，没有良好的配置管理，

没有跨版本的软件组件的生命周期管理，使用已弃用和不支持的工具链（其中一些是非确定性的）和构建环境中的不良卫生，其中许多都不能由HCSEC轻松重新创建。鉴于底层构建过程中的基本问题以及驱动它的客户管理和工程过程，目前还不清楚在继续二元等价程序方面是否有任何实用性。HCSEC和NCSC已经同意，作为更广泛的软件工程和网络安全转型的一部分，将更好地从头开始重新设计构建过程。NCSC仍然认为所有在英国部署的产品都具有可重复的构建，并且HCSEC将能够定期显示安装在英国网络中的二进制文件与可以使用HCSEC持有的源代码构建的二进制文件之间的等效性，因为通常有一个管理良好的软件工程流程。最近对四种试验产品的研究表明，鉴于华为目前的构建过程，目前这在任何有用的规模上都是不切实际的。NCSC已告知监督委员会，除非并且直到构建过程发生根本性变化，否则只能对目前在英国部署的设备提供有限保证。

3.22 英国运营商社区仍然担心华为提供的类似版本软件的一致性。在某些情况下，构建版本在运营商预期的最终配置中进行测试 – 由运营商提供 – 在华为发布之前。虽然这提高了预期配置的可靠性，但它可能会掩盖本报告中详述的严重问题，这些问题会在配置受到干扰或漏洞利用时影响网络性能，从而对网络造成安全性或可用性影响。运营商之间的真实一致性要求对本报告中的问题进行补救。

配置管理

3.23 正如2018年报告中所详述的那样，监督委员会和非公务员制度委员会要求华为研发部门完成二进制等值计划所需的更多的液压工作，HCSEC将转向其提供验证的角色。随着这项工作的进展，研发团队产生了越来越多的意外文物。HCSEC被要求进行分析，以揭示导致遇到问题的潜在系统性问题。他们发现了以下缺陷：

- 在构建过程中使用的虚拟机的配置管理很差。具体来说，虚拟机在构建开始时并不干净，许多虚拟机包含（有时是不相关的）源代码，以前构建的伪像和其他碎片。
- 构建环境的配置管理（包括工具链）很差，有时甚至不存在。工具在构建环境中或在不需要它们的环境中多次安装。许多工具明显不受支持并且具有不期望的属性，例如基于环境变量值的非确定性编译或优化。
- 源代码的配置管理很差。这体现在两个广泛的领域。首先，开发团队之间不一致地应用配置管理。产品代码的管理方式与平台代码不同，两者的管理方式与第三方组件不同。其次，与整个产品体系结构的集成非常差，具有多个副本和组件版本，显然相同版本化的组件包含显着差异，组件之间的循环依赖性以及在整个产品增量之间的版本中的一些组件回归。

3.24 NCSC（当时的CESG）首先要求华为在2010年进行适当的配置管理，并且该公司此后一直在投资该流程，之前的监督委员会报告详细介绍了华为在该领域的工作。然而，由于在中间期间进行的各种技术工作，已经发现了人工制品，这表明该推出在整个公司中并不一致，并且配置项目在工作期间尚未合理化。2016年，HCSEC撰写了一份报告，概述了许多这些问题，以回应NCSC的要求，但这些发现在当时被华为拒绝。从HCSEC和NCSC在监督委员会主持下完成的后续工作中，现在很明显，2016年报告中确定的问题在公司的产品线中仍然是系统性的。由于存在这些问题，NCSC已经向监督委员会提出建议，目前华为提供的产品没有端到端的完整性，对华为理解这些产品的能力缺乏信心。

任何给定构建的内容或其对已识别问题执行真正根本原因分析的能力。

第三方组件支持问题

3.25　各方已投入大量精力，充分了解上一份报告中提出的有关支持特定第三方软件组件的问题。这个问题涉及广泛使用的第三方实时操作系统的主流支持版本的各种旧版本和即将推出的版本，华为已选择继续使用其生命周期结束时间明显更长的产品。继续使用依赖旧软件组件（包括但不限于操作系统）的产品会给运营商带来风险。此外，所讨论的操作系统基于单个内存空间，单用户模型（在设计时普遍存在），这进一步增加了风险，因为在此操作系统下运行的任何进程中的单个漏洞足以允许泄密在同一操作系统实例中运行的任何组件。华为已经从供应商那里购买了一份单独的高级长期支持协议，以便在未来以商业上可行的方式解决漏洞，但单一内存空间，单用户环境安全模型带来的潜在网络安全风险仍然存在。行业良好做法是使组件保持最新并根据供应商版本升级版本。监督委员会和英国运营商明确表示，长期依赖英国的这一操作系统是不可接受的，必须建立升级路径。在撰写本文时，NCSC尚未看到华为提出的缓解此问题的可靠计划，以及通过适用于现代运营商级电信系统的安全模型的可支持操作系统的升级途径。在制定可靠的计划之前，运营商将继续做出非凡的工作来缓解持续的风险。

更广泛的组件和生命周期管理问题

3.26　在华为上海工厂举行的2018年6月监督委员会会议上，会议结束时增加了技术跟进日，以便更好地了解更广泛的组件和生命周期管理策略，包括上面详述的操作系统问题。

3.27 第一项工作是围绕华为打算从基于开源Linux内核的实时操作系统的主线支持中撤出操作系统。在上海进行审查之后，NCSC得出的结论是，它没有足够的证据对华为自己的实时操作系统的长期持续工程有信心。将现有应用程序代码移植到更现代的操作系统内存和安全模型存在集成风险。这会产生跨操作员风险，需要特别注意修复，特别是在某些情况下可能需要新硬件。需要做的工作是权衡过时的操作系统的已知风险与改变不同操作系统的风险以及所有需要的风险。对于运营商而言，这是一个极其困难的位稍后将介绍更多细节。

3.28 第二项工作是确定更广泛的组件和生命周期管理是否显示类似的问题。由于监督委员会会议在上海举行，因此有可能让工程师在现场开发系统上执行操作以显示实时证据。华为提出了预期的流程和一些高级证据，表明它正在被遵循。然后，NCSC选择了一个常用的组件，即OpenSSL库，并在华为开发数据库上执行了特定的查询。这表明允许在产品中使用的OpenSSL版本数量难以管理，包括不在主要开发列车上的版本，这些版本具有已知漏洞且不受支持。向监督委员会报告的结论是，华为的基本工程流程无法正确管理组件使用或生命周期维护问题，导致产品一般不受支持。

3.29 监督委员会在9月的会议上明确表示这是不可接受的，并重申了过去12个月华为从根本上改变其软件工程和网络安全流程的需求。

LTE eNodeB的改进测试

3.30　在华为在上海的工厂举行的2018年6月监督委员会会议上，HCSEC的任务是对两个版本的LTE eNodeB之间的软件工程和网络安全质量变化进行分析。根据华为的计划实施，正在执行的改进过程通常是在后续版本完成代码时嵌入的。向NCSC递交此报告是为了给华为提供改进计划的时间，但由于在确定潜在根本原因或改变开发过程的举措方面缺乏进展，NCSC在9月份的董事会会议上提出要求。

3.31　期望软件的后期版本完美无缺是不切实际的，但NCSC希望看到广泛而持续的改进。该审查显示，两个版本之间的代码重复已大大减少，并且一个开源组件的副本数量显着减少。遗憾的是，该产品的一般软件工程和网络安全质量仍然存在大量主要缺陷：

- 自2013年起，广泛不遵守基本的，安全的编码实践，包括华为自己的内部标准，使得漏洞更有可能发生。版本的范围在版本之间有所减少，但仍然令人担忧；
- 广泛使用不正确的安全内存操作功能，大大增加了内存安全漏洞的可能性。版本的范围在版本之间有所减少，但仍然令人担忧；
- 在执行包括边界计算在内的算术运算时，大量滥用有符号/无符号键入和转换为不同的变量大小，显着增加整数溢出和下溢漏洞的可能性以及相关的缓冲区大小漏洞；
- 软件组件导入管理不善，使支持性和生命周期安全性变得非常困难；
- 静态分析工具不恰当地抑制警告，可能隐藏漏洞；

- 广泛使用固有的不安全和禁止的内存操作功能，进一步增加了内存安全漏洞的可能性。版本的范围在版本之间有所减少，但仍然令人担忧；
- 无法管理的构建过程，包括过时的工具链。

3.32 从广泛的报告中抽取的两个具体例子说明了所发现问题的规模。

3.33 该报告分析了常用且维护良好的开源组件OpenSSL的使用情况。OpenSSL通常对安全至关重要，并处理来自网络的不受信任的数据，因此组件保持最新非常重要。在该软件的第一个版本中，有4个不同OpenSSL版本的70个完整副本，范围从0.9.8到1.0.2k（包括来自供应商SDK的一个），包含14个版本的部分副本，范围从0.9.7d到1.0 .2k，编号为304的部分副本。在代码库中也发现了10个版本的碎片，范围从0.9.6到1.0.2k，这些碎片通常是为了导入某些特定功能而被复制的小型文件集。还有大量的文件，这些文件再次分布在代码库中，这些文件已经在OpenSSL库中开始生效，并且已被华为修改过。

3.34 在更高版本中，只有6个副本的2个不同的OpenSSL版本，其中5个是1.0.2k，一个来自供应商SDK。剩下17个部分副本的3个版本，范围从0.9.7d到1.0.2k。来自10个不同版本的OpenSSL的片段保留在代码库中，华为也修改了OpenSSL派生文件。更令人担忧的是，后一版本似乎包含易受10个公开披露的OpenSSL漏洞攻击的代码，其中一些漏洞可追溯到2006年。这表明由于糟糕的配置管理，产品架构和组件生命周期管理导致的可维护性和安全性不足。

3.35 该报告还分析了该产品对华为自身安全编码指南的部分遵守情况，即安全内存处理功能。eNodeB中面向公众的处理板之一上的二进制图像被分析用于直接调用memcpy（） - 类似，strcpy（） - 和sprintf（） - 类似于安全和不安全变体的函数。该板处理与不可信接口的通信

并且期望以强大和防御的方式编码。在这种情况下尤其如此，因为缺少操作系统缓解。

3.36 综上所述：

- 有超过5000个直接调用17个不同的安全memcpy（）函数和超过600个直接调用12个不同的不安全memcpy（）函数。大约11%的memcpy（）函数的直接调用是针对不安全的变体。
- 有超过1400个直接调用22个不同的安全strcpy（）函数和超过400个直接调用9个不同的不安全strcpy（）函数。大约22%的strcpy（）函数的直接调用是针对不安全的变体。
- 有超过2000次直接调用17个不同的安全sprintf（）函数和近200个直接调用12个不同的不安全sprintf（）函数。大约9%的sprintf（）函数的直接调用是针对不安全的变体。

3.37 这些数字不包括任何间接调用，例如通过函数指针等。值得注意的是，这些不安全的函数存在于二进制文件中，因此存在实际风险。

3.38 对相关源代码的分析令人担忧地确定了一些形式为“#define SAFE_LIBRARY_memcpy（dest，destMax，src，count）memcpy（dest，src，count）”的预处理器指令，它有效地将安全功能重新定义为不安全的函数。删除为删除源代码中的不安全函数所做的工作的任何好处。还存在强制不安全使用潜在安全功能的指令，例如“#define ANOTHER_MEMCPY（dest，src，size）memcpy_s（（dest），（size），（src），（size））”形式。

3.39 这种重新定义使开发人员更难以做出良好的安全选择，并且任何代码审计员的工作都异常艰难。这些只是示例，但表明华为自己的内部安全编码指南并未在本产品中经常使用，在某些情况下，开发人员可能会积极地隐藏错误的编码实践而不是修复它。

3.40　总体分析表明，华为软件工程和网络安全发展仍存在重大问题。

LTE改进计划

3.41　在2018年9月的监督委员会会议上，董事会成员越来越担心华为在纠正HCSEC和NCSC发现的基本问题方面缺乏进展。特别是，在过去的12个月中，在制定可靠的计划以减轻英国不受支持的软件的重要安装基础方面缺乏进展已变得至关重要。为了集中精力，监督委员会要求制定一项计划来修复单一产品，最终选择成为LTE eNodeB。华为一直到2018年10月19日 – 随后延长到10月26日 – 为eNodeB的整治提供可靠的计划。目的是确保华为，HCSEC，英国运营商和NCSC之间能够进行讨论，并在12月监督委员会会议之前进行改进，以便讨论该计划。

3.42　提交的文件大部分是对eNodeB功能的安全性分析，主要来自NIST SP800-187。已经确认了HCSEC和NCSC发现的问题以及一些描述基本修复的尝试，但该文件主要描述了华为目前的流程及其预期结果，而不是实际发现的产品和根本原因。报告的一小部分涉及对华为发展过程进行变更的计划。遗憾的是，交付的计划没有解决所遇到的问题的规模，也没有从根本上解决潜在的软件工程能力问题。在与NCSC和英国运营商的会议上，华为还有四周时间提出计划。华为在那次会议上的发言表明，没有取得实质性进展。在撰写本文时，NCSC没有看到华为在英国使用eNodeB或任何其他华为产品进行补救的可靠计划。

华为转型

3.43　在会议讨论LTE eNodeB改进计划后，NCSC再次代表监督委员会致函华为，寻求一个可靠的计划，对已部署在英国的产品进行战术整治，并寻求更广泛的转型计划。这些问题在未来不太可能发生。NCSC明确表示，如果没有这样的计划，对华为的技术或华为长期安全使用运营商的能力可能没有长期信心。

3.44　华为接受了对其软件工程和网络安全流程的批评，并承诺在五年内投资20亿美元用于整个公司的转型，这将包含并缓解监督委员会提出的问题。显然，任何此类投资必须得到包含可衡量成果的计划的支持。虽然对华为全球转型计划的正式监督不属于监督委员会活动的范围，并且预计不会报告与英国网络安全风险无关的更广泛事项，但董事会希望看到华为转型的充分细节。其软件工程和网络安全流程使其能够评估其有效控制和减轻其识别风险的程度。在理事会重新评估其保证水平之前，需要持续证明其对英国正在使用的产品的影响，特别是考虑到威胁环境和所涉及的技术日益复杂。与此同时，NCSC将告知监督委员会，它可以继续仅对英国目前部署的设备的安全性提供有限保证。NCSC和英国运营商将继续与华为合作，为英国的设备制定可信和可持续的补救计划，不受任何更广泛的华为转型的影响。在极端情况下，NCSC可以指导华为如何在华为正常开发和支持流程之外修复英国基础设施中的特定产品，从而将英国的风险降低到更合理的水平。这不是一个可持续的响应，只有良好的实践软件工程和网络安全开发过程才能提供未来的保证基础。

3.45　重要的是，NCSC目前无法预测转型期间和之后华为未来产品的技术结构和特征。此外，鉴于华为的开发过程不一致

在产品组中，NCSC不能假设英国使用的产品组合的结果转化为其他产品。英国在英国电信领域使用华为设备的缓解策略（其中HCSEC和监督委员会是其中一部分）预计将以行业良好实践软件工程和网络安全开发和支持流程为基础。华为目前不符合这一基本预期。由于HCSEC的运营，英国运营商和NCSC对目前部署的华为设备产生的风险有详尽的了解。没有相同详细程度的重要新设备和基于现有知识的假设无法重复使用（由于不一致的开发实践），并且会使风险管理更加困难。

3.46　鉴于问题的严重性，需要在多个版本和多个产品上提供重要且持续的改进证据，以开始建立对华为软件工程和网络安全质量和开发流程的信心。单一的“良好”构建将不会对现实世界中产品的长期安全性和可持续性产生信心。华为关于其转型计划的公开声明表明，这需要五年时间。NCSC的技术总监认为这与最佳案例估计基本一致。监督委员会承认，在未来的年度报告中报告与英国网络安全风险有关的事项的进展时，它将继续考虑华为的任何陈述，即特定事项对商业敏感和/或与英国网络安全风险无关。它将继续适当考虑任何此类陈述，前提是它能够按照附录A中的职权范围的要求，适当履行其报告英国网络安全风险的义务。

~~~~~
~~~~~

第四部分：理事会的工作：保证独立性

4.1　　除了监督HCSEC提供的技术保证外，本节重点介绍监督委员会的一般性工作。管理委员会连续第五年委托并审议了HSCEC对华为总部所需的运营独立性的审计。在委员会看来，这是最有效的方式，即获得保证，这些安排的设计方式与支持英国国家安全有关。审计审查的主要问题是，HCSEC是否具有华为总部所要求的运营独立性，以履行2010年英国政府与公司达成的安排所规定的义务。独立审计并未寻求对质量作出评论任何技术工作 – 来自HCSEC或华为总部 – 并且详细的技术发现与HCSEC的独立运作无关。本节介绍了审计过程，以及主要调查结果的摘要。

任命安永会计师事务所为审计师

42　　安永会计师事务所（E&Y）在2014年进行了首次HCSEC审计，经过严格的程序，GCHQ邀请三家审计机构考虑进行管理审计，并就适当的审计标准和流程寻求建议。紧随其后。E&Y在2015年进行了第二次审计，2016年，在NCSC的鼓动下，他们被保留为随后三年提供审计服务，即2019年11月.E&Y的年度管理审计是根据国际保证业务标准进行的。　（ISAE）3000。

4.3　　监督委员会同意采用三阶段审计方法，这与前几年大致相同：

i. 评估控制环境的初始阶段，并就审核的范围和关键问题达成一致。这一阶段于2018年11月完成；
ii. 第二阶段对现有控制系统的设计和运行进行排练审核，以支持HCSEC的独立运作。这一阶段于2018年11月完成；

iii. 最终审计阶段包括2018年12月的全年结束审计，报告于2019年1月提交。

审计的性质和范围

4.4 审计评估了流程和控制的充分性和运作，旨在使HCSEC的员工和管理层能够独立于华为其他地方的不当影响而运营。范围的主要领域是：财务和预算；人力资源；采购；评估计划规划；华为其他地方的合作与支持；和评估报告。对于列出的所有审核区域，E＆Y考虑到HCSEC的运营必须在华为与HCSEC商定的年度预算范围内进行。

4.5 监督委员会同意对审计范围进行一些排除。具体而言，他们同意审计不会：

- 关于支持对英国关键国家基础设施中部署的华为产品进行测试所采用的整体治理模式的适当性的说法；
- 评估HCSEC的技术能力，个人员工的能力或技术测试的表现质量；
- 评估对HCSEC的物理访问或对其IT基础架构的逻辑访问。它也不会考虑现有基础设施或灾难恢复或业务连续性规划的弹性。

标题审计结果

4.6 HCSEC年度管理审计2019年1月对HCSEC流程和程序进行了严格的循证审查。审计报告由安永会计师事务所清理工作人员组成；实地工作由经验丰富的经理进行，由高级经理领导。内部审计主题知识合作伙伴作为质量审核人，最终报告的第二次审核由安永会计师事务所合作伙伴执行。

4.7 总之，安永认为对HCSEC的独立运作没有重大担忧。审计报告的主要结论是：

“除了下面的发现[一项评定为’低’的发现]之外，根据对照描述和商定的测试程序，评估的对照被认为是有效的。在某些情况下，有人指出，有机会进一步加强控制制度或提高审计过程的效率，下文已将这些建议视为“咨询”建议，而不是确定的控制缺陷“

控制弱点

4.8　总之，确定的控制薄弱领域以及商定的答复涉及以下领域：

i.　RFI在SLA期间返回

向华为提供的信息请求并不总是在规定的SLA期限内返回，硬件为12周，软件源代码为30天。这在上次审计中作为咨询建议报告，但一直持续到今年。

虽然HCSEC计划中有一些“松弛”以适应延迟交付，但应更新HCSEC RFI以包括“要求日期”，并且应该升级任何违反交付的行为。

咨询通知

4.9　审计还确定了两份咨询通知。

i.　审查评估计划的进展情况

4.10 今年没有继续对评估计划的进展情况进行正式定期审查。审查发现，定期举行的SMT会议可以提出评估进展中的任何问题，但是前几年已经完成的每周评估进展报告尚未完成。

4.11 应恢复定期报告评估状态。这提供了HCSEC工作的记录，并清楚地突出了任何延迟及其原因。

ii. 可审计信息的严谨性

4.12 基于样本的测试确定了一些记录未得到适当维护的情况 – 尽管在每种情况下都确定相关控制仍在有效运行。审核确定了在未记录所有正确批准的情况下处理的采购订单，并且在有效合同到位时，HCSEC供应商列表中的某些供应商被错误地标记为非活动状态。

4.13 应严格遵守HCSEC当前的流程。

上一年度问题和现状

4.14 附录B概述了2018年出版的上一年度报告中的问题和意见。

总体监督委员会的审计结论

4.15 总体而言，HCSEC监督委员会总结了审计报告的结论，该报告向全球知名公司提供了重要的外部保证，即HCSEC从华为总部的运营独立安排运行稳健有效，并且与2010年政府与公司之间的安排。已经确定了三个问题 – 一个低评级发现和两个咨询问题。鉴于审计范围，这与本报告中的更广泛调查结果完全一致。

~~~~~
~~~~~

第五部分：结论

5.1 监督委员会现已在此期间完成工作。其五次会议及其在委员会之外的工作为HCSEC的治理安排提供了有益的改进。

5.2 监督委员会的结论是，在2018年，HCSEC履行了向NCSC和英国运营商提供软件工程和网络安全保障文物的义务，作为管理英国国家安全风险战略的一部分，华为参与英国的关键网络。

5.3 然而，正如2018年报道的那样，HCSEC的工作继续确定华为软件开发方法中的重大问题，为英国运营商带来了显着增加的风险，这需要持续的管理和缓解。由于HCSEC工作提供的广泛漏洞和软件工程以及网络安全质量信息，运营商需要考虑所需的缓解措施。

5.4 2018年报告中提出的问题没有取得实质性进展，今年的报告也揭示了进一步的问题。监督委员会继续只能提供有限的保证，即可以在目前在英国部署的华为设备中管理长期安全风险。监督委员会特别注意到NCSC的以下建议：

i. 华为提供的产品没有端到端的完整性，对华为理解任何特定构建内容的能力以及对已发现问题进行真正根本原因分析的能力的信心有限。这引起了对长期漏洞管理的重大关注；

ii. 华为的软件组件管理存在缺陷，导致更高的漏洞率和无法支持的软件风险；

iii. 尽管对eNodeB后续主要版本的审查显示代码重复方面有所改进，OpenSSL组件的副本数量也大幅减少，但该产品的一般软件工程和网络安全质量仍然存在大量主要缺陷. .

5.5 监督委员会建议，在英国部署的情况下，很难对未来的产品进行适当的风险管理，直到华为的软件工程和网络安全流程得到纠正。监督委员会目前还没有看到任何让华盛顿能够通过其转型计划实现变革的信心，并且需要持续证明HCSEC和NCSC验证的更好的软件工程和网络安全质量。

5.6 华为的转型计划原则上可以成功，将华为的软件工程和网络安全流程推向当前的行业良好实践。华为自己的公开估计，这种转变需要三到五年。监督委员会将要求非公务员制度委员会评估多个产品的多个版本持续变化的证据，以便对成功充满信心 – 单一产品的单一版本具有更好的客观工程质量和安全性，并不能保证成功和可持续的变革。公司，甚至是那个单独的产品组。

5.7 持续变革的证据尤为重要，因为华为过去类似的措辞强硬的承诺没有带来任何明显的改善。监督委员会特别注意到华为2012年网络安全白皮书中首次做出的承诺（可从中获取）https://www-file.huawei.com/-/media/corporate/pdf/cyber-security/cyber-security-white-paper-2012-en.pdf并随后重复。因此，需要提供重要且持续的证据，以使监督委员会相信华为的转型计划将带来所需的变更。

5.8 应该明确的是，监督委员会的有限保证声明并不是对今天英国网络安全性的评论，这是个别运营商，Ofcom，DCMS和NCSC的问题。这是保证

HCSEC是否可以继续提供安全相关的文物，以告知英国利益相关者作为减缓战略的一部分。我们针对华为在英国的存在的缓解策略所规定的监督可以说是世界上最严格，最严格的。因此，该报告并未表明英国网络比去年更加脆弱。事实上，HCSEC为英国运营商提供的重要技术见解使他们能够制定更有效的缓解措施。监督委员会的报告只表明华为的开发和支持流程目前不利于长期安全风险管理，目前，监督委员会对华为解决这一问题的能力没有任何信心。

5.9 监督委员会的这些结论并未预示DCMS目前正在代表政府对英国的电信供应安排进行审查，目的是确保有一个有效的政策框架来部署安全和有弹性的5G和全光纤网络。DCMS表示，审查将在制定政策时仔细考虑监督委员会关于技术保证的调查结果和结论以及其他证据。但审查将基于一系列不同的证据，监督委员会的结论只是其中的一部分。

5.10 最后，还应该指出的是，监督委员会希望强调，它没有任何职责来指导或影响英国运营商的采购决策。在Ofcom，DCMS和NCSC的支持下，他们必须单独管理自己网络中的风险。

5.11 监督委员会希望本报告继续增加议会
– 通过它，公众 – 了解安排的运作及其运作的透明度。

~~~~~
~~~~~

附录A：华为网络安全评估中心监督委员会的职权范围

1. 目的

将成立该监督委员会，以实施国家安全顾问对华为网络安全评估中心（HCSEC）的审查建议二。监督委员会的主要目的是监督和确保HCSEC的独立性，能力和整体有效性，并将在此基础上向国家安全顾问提供建议。它将以协商一致方式运作。但是，如果对监督委员会所涵盖的事项存在分歧，作为主席的GCHQ将有权做出最终决定。

董事会负责评估HCSEC与英国产品部署相关的绩效。它不应该参与HCSEC的日常运作。

2. 工作范围

2.1范围

监督委员会将重点关注：

- HCSEC对部署或签约部署在英国并与英国国家安全风险相关的华为产品的评估。
- HCSEC在履行职责方面的独立性，能力和整体效力。

2.2超出范围

- 所有与英国国家风险无关的产品；
- 非英国部署的所有产品，工作或资源，包括位于英国境外的任何全球CSP在英国境外部署的产品，工作或资源；
- 华为与CSP之间的商业关系；和
- HCSEC的基础研究（工具，技术等）将被评估

并由GCHQ执导。

3. 监督委员会的目标

3.1 年度目标和向国家安全顾问报告

每年向国家安全顾问提供有关HCSEC的独立性，能力和有效性的报告，明确详细说明HCSEC在多大程度上实现了董事会制定的年度目标。这将利用年度管理审计，技术能力审查，并将具体评估HCSEC资源的现状和长期战略。

所有已签约使用HCSEC进行英国国家部署风险管理的英国CSP均应参考。

如果HCSEC的运营发生变化，或者出现影响HCSEC安全状况的任何其他因素，HCSEC将及时向监督委员会报告。GCHQ［或监督委员会的任何其他成员］也应该通知监督委员会任何似乎影响HCSEC安全态势的因素。

3.2 委员会年度管理审计

为了确保HCSEC从华为总部继续独立，监督委员会将委托由安全审查的英国审计师进行管理审计;这将由英国政府资助。审计范围应按照监督委员会同意的华为总部授权（操作独立）授予HCSEC（见附件3）或其他商定标准的规定。这将包括预算执行的独立性以及是否向HCSEC提供及时的信息，产品和代码以开展工作。

监督委员会将确保任何此类审计的范围是适当的，审计员应由主席和副主席商定。

第3.2和3.3节中提到的审计报告应视为机密信息，并受第9节的约束。

3.3 委员会技术能力审查

确保HCSEC履行的职能适用于GCHQ和CSP规定的更广泛的风险管理战略。监督委员会将委托GCHQ对HCSEC员工的技术能力，HCSEC所采取的流程的适当性和完整性以及华为产品质量和安全对英国国家安全风险的战略影响进行审计。作为年度规划过程的一部分，GCHQ将向HCSEC提供他们希望在一年内制定的技术能力的任何增强建议。

3.4 指定高级管理团队的流程

监督委员会将同意GCHQ领导和指导HCSEC高级职员的任命。但是，监督委员会不会直接参与，但会收到GCHQ任何发展的最新情况。

3.5 及时交货

监督委员会将同意华为总部向HCSEC提供的代码，产品和信息的现有安排的正式化，以确保评估的完成不会被不必要地延迟。

3.6 影响HCSEC的问题的升级/仲裁员

如果出现可能影响HCSEC独立性，有效性，资源配置或安全状况的问题，董事会成员应及时通知监督委员会。在这种情况下，理事会可以召开特别会议。

4. 监督委员会成员资格

董事会最初将由以下成员组成。会员资格将每年进行审核。国家安全顾问将任命理事会主席。然后通过主席的邀请成为会员。

- GCHQ – 主席（Ciaran Martin，NCSC首席执行官）
- 华为总部 – 副主席（Ryan Ding，董事会执行董事）
- 华为英国董事总经理
- 华为英国通讯总监
- HCSEC常务董事
- 内阁办公室主任，网络安全，国家安全秘书处
- NCSC技术总监
- 白厅部门代表:(副主任，DCMS电信安全负责人，内政部安全与反恐办公室网络政策中心负责人)
- 现任CSP代表：BT CEO Security;沃达丰集团安全总监

每次最多可有4名CSP代表。CSP被任命为代表行业对董事会顾问能力的观点[1]。在实际或感知的商业利益冲突或商业利益前景的情况下，相关的CSP将被要求从相关的董事会讨论中回避。不参加监督委员会的国别战略计划将定期收到秘书处的最新情况和信息，他们可以通过秘书处提出意见和要求。秘书处将确保不会将CSP之间被视为商业敏感的信息分发给成员CSP。非会员CSP可能会被邀请临时参加。

5. 会议频率和主题

预计监督委员会每年将召开三次会议，如果需要，会更频繁地举行会议。

[1] “咨询能力”一词用于与个人行业专家有关的CSP成员，而不是代表其公司。他们仍然是监督委员会的正式成员。

- 第一次会议 – 将根据CSP合同确认的HCSEC要求，将HCSEC的高级　　目标设定为与监督委员会的范围相关。
- 会议二 – 年中将评估HCSEC实现目标的进展情况。
- 会议三 – 年底将评估目标的实现情况，并审查年度管理审计和技术能力审查的结果，以制定国家安全顾问的年度报告。

6. 报告

监督委员会将向国家安全顾问提供年度报告，讨论第3.1段所述的主题。国家安全顾问将向国家安全委员会提供本报告的副本，并向议会情报和安全委员会主席提供关键要点摘要。所有报告将根据其内容的敏感性进行分类，并由国家安全顾问自行决定。

7. 对监督委员会职权范围（TOR）的修改

理事会的意图是仅在绝对必要时修改这些职权范围。必要时，应使用以下程序修改职权范围：

- 对职权范围的任何修改都需要有关监督委员会议程的特定主题，并且必须在面对面会议上进行讨论；
- 拟议的修改和案文应至少在会议召开前7个工作日分发给OB成员；
- 拟议的修正案应在监督委员会会议上讨论，并可在所有成员达成共识后予以修正；

- 修正案的最终文本应由所有监督委员会成员以书面形式正式确认。

经最终协议后，更新的职权范围将分发给所有监督委员会成员。

8. 秘书处

GCHQ将提供秘书处职能。

9. 不披露义务

在不妨碍第6款的情况下，向监督委员会成员或第三方（共同为“接收方”）提供的与监督委员会运作有关的所有信息均应视为机密信息，不得复制，分发或披露。未经信息所有者事先书面同意的任何方式。除了违反保密义务之外，此义务不适用于披露时属于公有领域的任何信息。在向该方披露之前，它也不适用于接收方所拥有的任何信息，而且没有保密义务。它也不适用于接收方以非保密方式从另一个人那里收到的任何信息，这些信息并非接收方的知情和信仰，但有义务不向该方披露该信息。也不妨碍任何接收方遵守法院命令或其他法律要求披露信息。

附录B.

2017-2018审计中提出的问题和现状

2018 – 2019年审计审查了针对2017 – 2018年报告中强调的以下两个问题和两个建议的进展情况。

i. 请求并保留评估计划签字

内部非公务员合约制进程得到进一步加强，以确保评估计划得到适当的正式签署。2018年审计署确认，NCSC正式批准HCSEC计划。

ii. 预算设定和持续财务审查

更新了HCSEC内部流程以解决此问题。2018年的审计确认了HCSEC预算制定过程之后，记录和保留了每个SMT成员的正式签字。

iii. RFI在SLA期间返回

这一发现仍未得到解决，今年也有类似的发现。

iv. 在审计期间，对支出与预算的监测并未得到很好的维持

更新了HCSEC内部流程以解决此问题。2018年的审计确认已经进行了经常预算监测，并提供了每月审查的现有证据。

HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD

ANNUAL REPORT

2019

A report to the National Security Adviser of the United Kingdom

March 2019

Embargoed - Not for publication or broadcast until 0930 GMT Thursday 28 March

HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD ANNUAL REPORT

Part I: Summary

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

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

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

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

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

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

    iii. **The fifth independent audit of HCSEC's ability to operate independently of Huawei HQ has been completed**, with – again – no high or medium priority findings. The audit report identified one low-rated finding, relating to delivery of information and equipment within agreed Service Level Agreements. Ernst & Young concluded that there were no major concerns and the Oversight Board is satisfied that HCSEC is operating in line with the 2010 arrangements between HMG and the company;

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

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

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

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

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

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

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

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

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

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

This page is intentionally left blank

HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD 2018 ANNUAL REPORT

Part II: Technical and Operational Report

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

Introduction

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

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

3. The HCSEC Oversight Board, established in 2014, is chaired by Ciaran Martin, the Chief Executive Officer of the NCSC, and an executive member of GCHQ's Board with responsibility for cyber security. The Oversight Board continues to include a senior executive from Huawei as Deputy Chair, as well as senior representatives from across Government and the UK telecommunications sector. The structure of the Oversight Board has not changed significantly, but membership has changed in the year 2017-18. Mainly, this is due to staff rotations in both HMG and Huawei positions.

4. This fifth annual report has been agreed unanimously by the Oversight Board's members. As with last year's report, the Board has agreed that there is no need for a confidential annex, so the content in this report represents the full analysis and assessment.

5. The report is set out as follows:

I. Section I sets out the Oversight Board terms of reference and membership;
II. Section II describes HCSEC staffing, skills, recruitment and accommodation;
III. Section III covers HCSEC technical assurance, prioritisation and research and development;
IV. Section IV summarises the findings of the 2018 independent audit;
V. Section V brings together some conclusions.

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

1.1 The HCSEC Oversight Board was established in early 2014. It meets quarterly under the chairmanship of Ciaran Martin, the Chief Executive of the NCSC and an executive member of GCHQ's Board at Director General level. Mr Martin reports directly to GCHQ's Director, Jeremy Fleming, and is responsible for the agency's work on cyber security.

1.2 The role of the Oversight Board is to oversee and ensure the independence, competence and overall effectiveness of HCSEC as part of the overall mitigation strategy in place to manage the risks presented by Huawei's presence in the UK and to advise the National Security Adviser on that basis. The National Security Adviser will then provide assurance to Ministers, Parliament and ultimately the general public as to whether the risks are being well managed.

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

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

1.4 The Board has an agreed Terms of Reference, a copy of which is attached at **Appendix A**. There have been no changes to the terms of reference this year and the remit and objectives of the Oversight Board remain unchanged. The Oversight Board is responsible for providing an annual report to the National Security Adviser, who will provide copies to the National Security Council and the Intelligence and Security Committee of Parliament (ISC).

The Board's objectives for HCSEC

1.5 The Oversight Board's four high-level objectives for HCSEC remained consistent with those reported previously and are:

- To provide security evaluation coverage over a range of UK customer deployments as defined in an annual HCSEC evaluation programme;
- To continue to provide assurance to the UK Government by ensuring openness, transparency and responsiveness to Government and UK customer security concerns;
- To demonstrate an increase in technical capability, either through improved quality of evaluations output or by development of bespoke security related tools, techniques or processes;
- For HCSEC to support Huawei Research and Development to continue to develop and enhance Huawei's software engineering and cyber security competence.

The HCSEC Oversight Board: Business April 2018-February 2019

1.6 This report covers the technical work undertaken from January 2018 until December 2018. The Oversight Board meeting in March 2018 was covered in the previous report. In its five meetings since the publication of the 2018 Annual Report, the Oversight Board has:

- Provided regular corporate updates on Huawei UK;
- Discussed future technology trends and how they may affect the work of the Oversight Board;
- Been supplied with regular updates on HCSEC recruitment, staffing and accommodation plans;
- Received a detailed report on technical visits to Huawei HQ in Shenzhen and Shanghai by the NCSC Technical Director and technical team, some with UK operators, to discuss technical issues;
- Taken further evidence around the root causes of the significant software engineering and cyber security problems that came to light last year;
- Taken further evidence on Huawei's proposed remediation for the significant software engineering and cyber security problems, and judged them to be inadequate;
- Commissioned a fifth HCSEC management audit of the independence of the Centre.

~~~~~
~~~~~

SECTION II: HCSEC Staffing

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

Staffing and skills

2.2 The NCSC leads for HMG in dealing with HCSEC and the company more generally on technical security matters. The NCSC, on behalf of HMG, sponsors the security clearances of HCSEC's staff. The general requirement is that all staff must have Developed Vetting (DV) security clearance, which is the same level required in Government to have frequent, uncontrolled access to classified information and is mandatory for members of the intelligence services. New recruits to HCSEC are managed under escort during probation pending completion of their DV clearance period, which is typically six months.

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

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

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

Accommodation

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

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

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

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

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

~~~~~
~~~~~

Section III(a): HCSEC Technical Assurance

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

HCSEC Evaluation Process

3.2 HCSEC's assessment programme in 2018 continued the product and solution evaluation split of recent years. In 2018, 39 product evaluations were completed, and 3 solution evaluations were completed, with another scheduled to finish in early 2019. Overall, this is broadly as per the programme agreed at the start of the year. The evaluations covered products and architectures for five UK operators. This tempo was maintained despite the inclusion of significant amounts of non-evaluation work in support of Oversight Board actions and the move to new premises.

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

3.4 The evaluation process continues to uncover both point vulnerabilities and more strategic architectural and process issues, as detailed later in this section. Huawei continues with their remediation work; the feedback provided by HCSEC to UK operators, NCSC and Huawei R&D continues to be of high quality and the HCSEC technical staff continue to assist the Huawei R&D teams in their remediation efforts.

HCSEC Programme Build and Prioritisation

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

The programme build process remains broadly the same as in previous years. The UK operators, NCSC and HCSEC set priorities for HCSEC collaboratively. This is necessary to balance the sometimes competing constraints and requirements to achieve the best overall benefit for the UK, for example not allowing any particular operator to unfairly dominate the programme of work due to commercial pressures. The final programme is signed off by the NCSC Technical Director or NCSC Technical Director for Telecommunications on behalf of the Oversight Board and kept under review during the year by HCSEC. Where HCSEC believes modifications to the programme are necessary, a light-touch process involving the NCSC and the relevant operators is used to manage and approve any modifications. As well as servicing the evaluation pipeline, HCSEC has done significant work in support of the Oversight Board's objective levied in the previous report to support Huawei R&D in its efforts to enhance Huawei's software engineering and cyber security competence and so begin to remedy the underlying issues identified in this and previous reports.

3.6 Little has changed in terms of high-level prioritisation of equipment, although the scale and scope of Huawei's involvement in the UK telecoms sector means there is a significant pipeline of work for HCSEC to manage. At present, HCSEC manages that pipeline well, consistently meeting the expectations of NCSC and UK operators. The results of HCSEC's work is reported directly to the operators and they are expected to feed them into their corporate risk management processes.

Overview of HCSEC Technical Work and High-Level Findings

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

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

engineering process. The ability to do so, and the end-to-end assurance that a particular source code set is precisely that used to build a particular binary would normally be satisfied as a side effect of a modern software engineering process.

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

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

- HCSEC has continued to find serious vulnerabilities in the Huawei products examined. Several hundred vulnerabilities and issues were reported to UK operators to inform their risk management and remediation in 2018. Some vulnerabilities identified in previous versions of products continue to exist.

Conclusion: HCSEC Competence

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

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

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

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

3.12 The character of vulnerabilities has not changed significantly between years, with many vulnerabilities being of high impact (equivalently, a high base CVSS score and a relevant operational context), including unprotected stack overflows in publicly accessible protocols, protocol robustness errors leading to denial of service, logic errors, cryptographic weaknesses, default credentials and many other basic vulnerability types. Despite Huawei mandating application of its secure coding standards across R&D, extensive use of commercial static analysis tools and Huawei's insistence that risky code has been refactored, there has been little improvement in the objective software engineering and cyber security quality of the code delivered for assessment by HCSEC and onward to UK operators.

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

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

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

Conclusion: Implications for the UK National Security Risk

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

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

3.18 Poor software engineering and cyber security processes lead to security and quality issues, including vulnerabilities. The number and severity of vulnerabilities discovered, along with architectural and build issues, by the relatively small team in HCSEC is a particular concern. If an attacker has knowledge of these vulnerabilities and sufficient access to exploit them, they may be able to affect the operation of the network, in some cases causing it to cease operating correctly. Other impacts could include being able to access user traffic or reconfiguration of the network elements. However, the architectural controls in place in most UK operators limit the ability of attackers to engender communication with any network elements not explicitly exposed to the public which, with other measures in place, makes exploitation of vulnerabilities harder. These architectural controls and the operational and security management of the networks by UK operators will remain critically important in the coming years to manage the residual risks caused by the engineering defects identified. These findings are about basic engineering competence and cyber security hygiene that give rise to vulnerabilities that are capable of being exploited by a range of actors. NCSC does not believe that the defects identified are a result of Chinese state interference.

Section III(b): Supporting Technical Evidence

Binary Equivalence and Software Consistency

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

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

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

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

Configuration Management

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

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

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

Third-Party Component Support Issue

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

Wider Component and Lifecycle Management Issue

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

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

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

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

Improvement Testing on LTE eNodeB

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

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

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

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

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

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

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

3.35 The report also analysed the adherence of the product to part of Huawei's own secure coding guidelines, namely safe memory handling functions. The binary image on one of the public-facing processing boards in the eNodeB was analysed for the use of direct invocation of memcpy()-like, strcpy()-like and sprintf()-like functions in their safe and unsafe variants. This board handles communication with untrusted interfaces and it would be expected to be coded in a robust and defensive manner. This is especially true in this case because of the lack of operating system mitigations.

3.36 In summary:

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

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

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

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

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

LTE Improvement Plan

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

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

Huawei Transformation

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

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

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

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

~~~~~
~~~~~

SECTION IV: The work of the Board: Assurance of independence

4.1 This section focuses on the more general work of the Oversight Board beyond its oversight of the technical assurance provided by HCSEC. For the fifth year running, the Board commissioned and considered an audit of HSCEC's required operational independence from Huawei HQ. This was the most effective way, in the Board's view, of gaining assurance that the arrangements were working in the way they were designed to work in support of UK national security. The principal question for examination by the audit was whether HCSEC had the required operational independence from Huawei HQ to fulfil its obligations under the set of arrangements reached between the UK Government and the company in 2010. The independent audit does not seek to comment on the quality of any technical work – from either HCSEC or Huawei HQ – and detailed technical findings are not relevant to the independence of operation of HCSEC. This section provides an account of the process by which the audit took place, and a summary of the key findings.

Appointing Ernst & Young as auditors

4.2 Ernst & Young LLP (E&Y) were appointed to carry out the first HCSEC audit in 2014, following a rigorous process during which GCHQ invited three audit houses to consider undertaking the management audit and sought their recommendation as to the appropriate audit standard and process to be followed. E&Y undertook the second audit in 2015 and in 2016, at the NCSC's instigation, they were retained to provide audit services for the subsequent three years, that is until November 2019. E&Y's Annual Management Audit was conducted in accordance with the International Standard on Assurance Engagements (ISAE) 3000.

4.3 The Oversight Board agreed a three-stage approach to the audit, which broadly followed that of previous years:

i. An initial phase to assess the control environment and agree the scope and key issues for review. This phase was completed by November 2018;

ii. A second phase to run a rehearsal audit of the design and operation of the controls in place to support the independent operation of HCSEC. This phase was completed during November 2018;

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

The nature and scope of the audit

4.4 The audit assessed the adequacy and the operation of processes and controls designed to enable the staff and management of HCSEC to operate independently of undue influence from elsewhere in Huawei. The principal areas in scope were: Finance and Budgeting; HR; Procurement; Evaluation Programme Planning; Cooperation and Support from elsewhere in Huawei; and Evaluation Reporting. For all the review areas listed, E&Y took into account that the operation of HCSEC must be conducted within the annual budget agreed between Huawei and HCSEC.

4.5 The Oversight Board agreed some exclusions to the scope of the audit. Specifically, they agreed that the audit would not:

- Opine as to the appropriateness of the overall governance model adopted to support the testing of Huawei products being deployed in the UK Critical National Infrastructure;
- Assess the technical capability of HCSEC, the competency of individual staff or the quality of the performance of technical testing;
- Assess physical access to HCSEC or logical access to its IT infrastructure. Nor would it look at the resilience of the infrastructure in place or at Disaster Recovery or Business Continuity planning.

Headline audit findings

4.6 The HCSEC Annual Management Audit January 2019 comprised a rigorous evidence-based review of HCSEC processes and procedures. The audit report was produced by a team of DV cleared staff from Ernst & Young; the fieldwork was conducted by an experienced Manager and led by a Senior Manager. A Partner with Internal Audit subject matter knowledge acted as quality reviewer, and a second review of the final report was performed by an Ernst & Young Associate Partner.

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

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

Control Weakness

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

i. RFIs returned outside SLA period

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

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

Advisory Notices

4.9 Two advisory notices were also identified by the audit.

i. Review of progress against evaluation plan

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

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

ii. Rigour of auditable information

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

4.13 HCSEC's current processes should be rigorously followed.

Prior year issues and current status

4.14 **Appendix B** provides a summary of the issues and observations from the previous year's report, published in 2018.

Overall Oversight Board conclusions of the audit

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

~~~~~
~~~~~

SECTION V: Conclusions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

~~~~~
~~~~~

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

1. Purpose

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

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

2. Scope of Work

2.1 In Scope

The Oversight Board will focus on:

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

2.2 Out of Scope

- All products that are not relevant to UK national risk;
- All products, work or resources for non-UK-based deployment, including those deployed outside the UK by any global CSPs which are based in the UK;
- The commercial relationship between Huawei and CSPs; and
- HCSEC's foundational research (tools, techniques etc.) which will be assessed

and directed by GCHQ.

3. Objectives of the Oversight Board

3.1 Annual Objectives and Report to the National Security Adviser

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

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

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

3.2 Commission Annual Management Audit

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

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

The audit report mentioned in section 3.2 and 3.3 shall be treated as confidential information and subject to section 9.

3.3 Commission Technical Competence Review

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

3.4 Process to Appoint Senior Management Team

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

3.5 Timely Delivery

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

3.6 Escalation / Arbitrator for issues impacting HCSEC

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

4. Oversight Board Membership

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

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

There will be up to 4 CSP representatives at any one time. CSPs are appointed to represent the industry view on an advisory capacity to the board[1]. In the case of an actual or perceived commercial conflict of interest or prospect of commercial advantage the relevant CSP will be expected to recuse themselves from the relevant board discussion. CSPs that do not sit on the Oversight Board will receive regular updates and information from the Secretariat and they can feed in comments and requirements through the Secretariat. The Secretariat will ensure that no information which would be deemed commercially sensitive between CSPs is circulated to the member CSPs. Non-member CSPs may be invited to attend on an ad hoc basis.

5. Meeting Frequency and Topics

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

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

- Meeting One – will be to set the high level objectives of HCSEC as relevant to the scope of the Oversight Board, based on CSP contractually confirmed requirements to HCSEC.

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

- Meeting Three – end of year will be to assess the delivery of objectives, and to review the findings of the Annual Management Audit and the Technical Competence Review to develop the annual report for the National Security Adviser.

6. Reporting

The Oversight Board will provide an annual report to the National Security Adviser addressing the topics set out at paragraph 3.1. The National Security Adviser will provide copies of this report to the National Security Council and a summary of key points to the Chairman of the Intelligence and Security Committee of Parliament. All reports will be classified according to the sensitivity of their contents and will be distributed at the discretion of the National Security Adviser.

7. Modification to the Oversight Board Terms of Reference (TORs)

The Board's intent is that these Terms of Reference are modified only when absolutely necessary. The following process shall be used to amend the Terms of Reference when necessary:

- Any modification to the Terms of Reference requires a specific topic on the Oversight Board Agenda and must be discussed at a face-to-face meeting;

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

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

- The final text of the amendment shall be formally confirmed in writing by all Oversight Board members.

Upon final agreement, updated Terms of Reference will be distributed to all Oversight Board members.

8. Secretariat

GCHQ will provide the secretariat function.

9. Non-Disclosure Obligation

Without prejudice to paragraph 6, all information provided to any Oversight Board Member or third party (together a “receiving party”) in connection with the operation of the Oversight Board shall be treated as confidential information which shall not be copied, distributed or disclosed in any way without the prior written consent of the owner of the information. This obligation shall not apply to any information which was in the public domain at the time of disclosure otherwise than by the breach of a duty of confidentiality. Neither shall it apply to any information which was in the possession of a receiving party without obligation of confidentiality prior to its disclosure to that party. Nor shall it apply to any information which a receiving party received on a non-confidential basis from another person who is not, to the knowledge and belief of the receiving party, subject to any duty not to disclose that information to that party. Nor shall it prevent any receiving party from complying with an order of Court or other legal requirement to disclose information.