HM Government

Huawei Cyber Security Evaluation Centre:

Review by the National Security Adviser

December 2013

Executive Summary

1. The Intelligence and Security Committee (ISC) reported in June 2013 on Foreign Investment in Critical National Infrastructure. The report questioned in particular the ability of the Huawei Cyber Security Evaluation Centre (HCSEC) to operate with sufficient independence from Huawei headquarters. The report recommended that the staff in HCSEC should be GCHQ employees; or that, as an absolute minimum, oversight arrangements should be strengthened, and the Government should be more directly involved in the selection of HCSEC staff.

2. The Government welcomed the ISC report. It responded in July, with a commitment that the National Security Adviser would undertake a review of HCSEC and report to the Prime Minister. A summary of this review is set out below. In essence, the review concluded that HCSEC staff should remain part of Huawei, primarily for reasons of full access to equipment, code, and design teams. But after discussions with the Chairman of the ISC, the review also concluded that oversight arrangements should be enhanced, and GCHQ should have a leading and directing role in senior-level HCSEC appointments, in consultation with Huawei.

3. In more detail, the global reality is that virtually every telecommunications network worldwide incorporates foreign technology. Huawei equipment, for example, is now used in 140 countries and Huawei is a valued investor and employer in the UK. The Government has managed any potential security concerns through: increased engagement with the company; expert assistance to its customers, the Communication Service Providers (CSPs); and since 2010, the establishment of HCSEC. This is, moreover, part of a wider set of measures, designed with the CSPs, to minimise risk and opportunities for interference with equipment.

4. HCSEC‘s basic task is to analyse Huawei equipment to identify potential vulnerabilities. Its broader objective is to inform the design of more secure networks. This represents a relatively new approach but one that some other countries are interested in replicating.

5. The review focused on the operational independence of HCSEC, including the employment of its staff; its planning and budgetary oversight; how it did its work; and the security around the facility. The review involved visits to HCSEC, interviews with the main stakeholders, and examination of the documentary evidence.

6. The review judged that HCSEC was operating effectively and achieving its objectives, and that existing arrangements, although some of them informal, gave it sufficient independence. It noted that, after some initial teething problems, Huawei’s cooperation with HCSEC appeared exemplary, with equipment and software supplied without delay and full access provided to Huawei design teams. It also noted that those vulnerabilities identified since HCSEC’s establishment could be explained as genuine design weaknesses or errors in coding practice.

7. The review also judged that, although the fact of HCSEC staff being employed by Huawei appeared to create conflicts of interest, it was, in reality, the best way of ensuring continued complete access to Huawei products, codes and engineers, without which HCSEC could not do its job. In particular, were HCSEC staff not to be Huawei employees, access arrangements would be complicated by Huawei’s non-disclosure agreements with its hundreds of third party suppliers. Also, there would be a possibility of commercial risk or even liabilities for the taxpayer were GCHQ, in effect, to impose themselves between Huawei and the UK telecommunications market.

8. The review’s first conclusion, however, was that GCHQ’s involvement in the future appointment of senior staff to HCSEC should be strengthened. At

present, GCHQ have a power of veto over appointments through the security vetting process. The review recommends that, in future, GCHQ should lead and direct senior HCSEC appointments (in consultation with Huawei), in particular through chairing the selection panel.

9. The review also concluded that oversight arrangements and current informal agreements between HCSEC and Huawei should be formalised, to ensure the permanent embedding of the open and cooperative relationship existing between HCSEC and Huawei, and to strengthen still further HCSEC's operational independence. The particular recommendations include:

    - The creation of an Oversight Board. This should be chaired by a senior member of GCHQ with Huawei as Deputy Chair. Membership should be small and include representatives of Whitehall departments, including a senior member of the National Security Secretariat in the Cabinet Office, and CSPs. The Board should not get involved in the day-to-day operations of HCSEC. Instead, its purpose should be periodically to assess HCSEC's performance and verify its continuing independence from Huawei headquarters. The Board might appropriately meet quarterly.

    - An annual objective-setting exercise for HCSEC, led by GCHQ in consultation with Huawei, and overseen by the Board.

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

- The formalisation of currently informal arrangements governing the timely provision by Huawei of equipment and code to HCSEC, and the cooperation of Huawei engineers. And,

- The creation of a longer-term strategy for HCSEC covering both predicted future workloads and human resource planning.

10. The Terms of Reference of the review were confined to the role, resourcing, management, independence, and overall contribution of HCSEC. Nevertheless, it became clear in the course of the work programme that there were some broader and longer term issues and concerns. Two in particular were worth highlighting. The first was an apparent shortage of individuals in the UK employment market with the necessary technical expertise and skills to fill all the available posts in HCSEC, GCHQ and the relevant parts of Whitehall. The review noted that there were already good education initiatives in place through the National Cyber Security Programme, but recommended further and broader efforts to deepen the pool of individuals with the requisite cyber security skills.

11. The second concerned the fast moving nature of the telecommunications industry. HCSEC is a model for Government collaboration with the private sector. But the industry is evolving rapidly and becoming more diverse and complex. The review therefore recommends that officials assess the security implications arising from the changing industry landscape and propose options for Ministerial consideration.

Kim Darroch