SCHEDULE 2

REQUIREMENT

The CHECK Service shall be carried out in accordance with the following provisions

These requirements may be updated from time to time by CESG to reflect experience of operation of the CHECK Service. The Company is thus invited to provide comments and feedback to the CHECK Service Manager (see Schedule 16 for contact details).
In case of any conflict arising the CHECK Contract terms and conditions take precedence over the content of this Schedule 2

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other U.K. information legislation. Refer disclosure requests to the GCHQ Information Legislation Team on 01242 221491 ext 30306 or email infoleg@gchq

Crown © 2008

Schedule 2

I. ABOUT THE IT HEALTH CHECK SERVICE

1 The objective of the IT Health CHECK Service, also referred to as the CHECK Service or CHECK, is to enhance the IT health check services currently provided by private sector companies to enable the provision of health check services for HMG that are consistent with HMG Policy. The function of a CHECK Service health check is the detection of IT security weaknesses, through practical expert testing of a system by an independent Company, at the invitation of a Customer.

2 Roles of the various players are as follows:

2.1. The **Customer** will fund the health check;

2.1.1. The Customer is typically the owner of the system but could be a system procurer or provider.

2.1.2. A system to be tested may have one or more developers. A systems integrator may develop some bespoke code but otherwise integrate component products from other developers. Developers will usually be different from the Customer and will normally have completed their work prior to the health check. It is also possible that a developer will be asked to obtain an independent health check to confirm the security of their development.

2.2. The objectivity and repeatability of health check results is dependent on the expertise and knowledge of the Company's staff. In principle, CHECK can accommodate any areas of technical expertise to address the component technologies of a particular system.

2.3. Testing on these areas of expertise form the basis of the CESG-approved Team Member exams. Team Member exams test for a good grounding in all common technologies expected in modern Government ICT systems. Team Leader exams test for greater depth and expertise, and are offered in specific disciplines, for example web applications and infrastructure. Additional exams, which CESG reserve the right to introduce, will test an individual's knowledge of other areas, which will exist at the two levels.

2.3.1 'Green Light' status is achieved by at least one member of the team achieving Team Leader status. Should the company not have, or lose, Team Leaders, their status is recategorised to Red Light.

2.4. A CHECK Company will be contracted by the Customer to perform testing of the system. CESG is not a party to such contracts and has no responsibility to the Company or to any third party for securing any such contract.

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other U.K. information legislation. Refer disclosure requests to the GCHQ Information Legislation Team on 01242 221491 ext 30306 or email infoleg@gchq

Crown © 2008

2.5. The Customer will typically nominate a point of contact (such as a system manager) to liaise with the Company on arrangements for testing and other points of detail;

2.6. CESG as the National Technical Authority for Information Assurance is responsible for operating and managing the CHECK Service. In managing the Service CESG will be primarily concerned with:

2.6.1. assessing the Company, on an annual basis to confirm that they are able to meet the minimum standards for membership of the scheme;

2.6.2 maintaining definition of CHECK standards;

2.6.3 monitoring operation of the Company, to ensure that defined CHECK standards are consistently achieved;

2.6.4 managing and promoting the CHECK Service and publicising the approved status of the Company on a list of such companies.

3 Constructive dialogue between the Company and Customer is encouraged. An initial scoping meeting is particularly important as it allows the two parties to agree and adhere to terms of reference for the health check. The Company must also provide the Customer with a preliminary report, documenting the background, scope and context agreed at the initial scoping meeting. This allows the Customer to check the Company's understanding of the health check prior to testing.

4 The primary feature of a CHECK health check is the independent testing of the system. The Company's staff use their expertise and knowledge of the component technologies and products, together with their knowledge of tools and techniques, which would be available to an attacker in the public domain, to test for security weaknesses. The Company should suggest appropriate mitigation measures to address identified security weaknesses.

5 The Company will prepare and submit a report documenting the agreed terms of reference, health check findings and recommendations to the Customer (and copied to CESG).

6 The dependency of CHECK on the expertise and knowledge of the Company's staff is such that:

6.1. At least one member of the Company's staff should demonstrate that they meet the criteria to be assessed as a CHECK Team Leader through successful completion of CESG-approved Assault Course. All other

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other U.K. information legislation. Refer disclosure requests to the GCHQ Information Legislation Team on 01242 221491 ext 30306 or email infoleg@gchq

Crown © 2008

members of the team will be required to provide evidence of a baseline level of relevant experience, academic qualifications and to have passed a CESG-approved TEAM MEMBER exam in order to attain CHECK Team Member status.

6.2. The Company is required to supply CESG with evidence of appropriate expertise and continuing involvement in this area of work for all staff employed on CHECK work by issuing an up to date CV with CHECK membership renewal paperwork.

7. CHECK work performed by the Company will be subject to periodic audit by CESG and to this end the Company agrees to permit the authorised representatives of CESG full access to the Company's premises, systems and other materials on reasonable notice.

8. Should CESG have concerns about the service provided by the Company then:

8.1. The Company will be informed and their timely co-operation required to address the deficiencies in the service provided;

8.2. The Company may subsequently be subjected to closer monitoring to ensure that deficiencies have been addressed;

8.3. Should the concerns not be addressed to the satisfaction of CESG, the dispute resolution process may be invoked.

II. QUALITY REQUIREMENTS

Qualifications of Staff

9. All staff employed by the Company on CHECK work must first be agreed by CESG. The Company must nominate staff for inclusion in their team as part of the process of seeking Company approval. Additional staff may also be nominated at any point during the contract year. Staff must have been agreed by CESG as members of a Company's team before they are eligible to attend a CESG-approved Assault Course for the purpose of achieving CHECK Team Leader status.

10. To support nomination of staff for membership of a Company's team, the Company must also supply CESG with up-to-date records of staff experience and qualifications.

10.1. Evidence of appropriate staff expertise will be demonstrated by:

- academic IT qualifications,
- relevant IT work experience,
- formal training in IT system management,

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other U.K. information legislation. Refer disclosure requests to the GCHQ Information Legislation Team on 01242 221491 ext 30306 or email infoleg@gchq

Crown © 2008

- specific computer security training,
- on the job experience,
- vulnerabilities research.

11. Those staff agreed by CESG as being suitable to be members of a Company's team must hold a minimum of SC security clearance and have passed a CESG-approved exam (at TEAM MEMBER or TEAM LEADER level) before they can be employed on CHECK Service related tasks. Where they are not already cleared to SC or above, CESG will sponsor their clearance. Once the security clearance has been confirmed, CESG will notify the Company that the individual is fully approved as a member of their team. If an individual transfers to a new Company it is the responsibility of the importing Company to confirm that their SC is still current and shall be transferred to the new Company or, the new company shall request CESG to sponsor them and shall complete the appropriate SC application pack for the SC to be granted by GCHQ.

12. The test team must have sufficient experience to undertake the CHECK Service and comprise the necessary mix of expertise for the component technologies of the target system. All members of the team must have passed the relevant CESG-approved Assault Course(s). The CHECK TEAM LEADER must be present on site for the duration of the testing. Staff approved as having CHECK TEAM MEMBER status may assist in health checks provided that they are supervised by colleagues approved as having CHECK Team Leader status in the relevant discipline.

Test Reporting

13. A report must be produced for each health check. Failure to do this may result in termination of the CHECK membership Contract as described in Clause 7.

Audit

14. The Company:
    - should endeavour to notify CESG at least 5 working days before the commencement of each assignment to be undertaken under the CHECK Service;
    - must supply CESG with a copy of each report within 1 calendar month of it being issued to the Customer;
    - must comply with all requests to allow monitoring and observation of its CHECK work by CESG.

14.1. Failure to do this may result in termination of the CHECK membership Contract.

15. Unless otherwise agreed, all liaison with CESG in connection with the CHECK Service should be through either the CHECK Service Manager or CESG Contracts Manager as appropriate (see Schedule 16 for contact details).

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other U.K. information legislation. Refer disclosure requests to the GCHQ Information Legislation Team on 01242 221491 ext 30306 or email infoleg@gchq

Crown © 2008

16. To ensure a consistent standard of work CESG may audit the conduct of health checks by attending selected test sessions and by reviewing selected reports. A member of the CESG CHECK team may visit any Company as necessary to discuss methodology, current and future projects and respond to any queries the Company wishes to raise.

17. CESG reserves the right to solicit feedback from Customers receiving CHECK IT health checks.

Company Quality Standards

18. Because IT systems are business critical, Customers need confidence that their asset will be treated responsibly. It is of the utmost importance that the Company does not damage the system under test, either deliberately or accidentally. The Company must therefore ensure that:

    18.1. it performs no testing which might cause damage to the system (e.g. involving virus infection, release of malicious code, unchecked hacking scripts downloaded from the Internet or unacceptably high network loading);

    18.2. all testing is carried out with the full knowledge and authority of the Customer (or system owner, if different);

    18.3. the system manager is advised of the possible impact of testing, which might simulate one or more agreed threat scenarios, and advised to take appropriate precautions before any testing takes place. These might include system backups or isolation of critical elements;

    18.4. the system is left fully operative and functioning after testing (e.g. by relinquishing any test privileges back to the system manager).

19. CHECK assignments must be conducted impartially and deliver objective technical results and recommendations:

    19.1. Before entering into a contract to supply CHECK services, the Company must therefore declare any other commercial interest in the system or products used by the Customer (where, for example, the system to be tested had been supplied by its own, or a partner organisation). Equally, the Company must declare any interest (perhaps by nature of previous employment) which may apply to the staff they propose to use for the assignment.

    19.2. The Company may recommend use of certain products or services in order to eradicate vulnerabilities. Where the Company has a commercial interest in such products or services then this, and the existence of any alternatives of comparable capability of which an expert in the field would be expected to be

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other U.K. information legislation. Refer disclosure requests to the GCHQ Information Legislation Team on 01242 221491 ext 30306 or email infoleg@gchq

Crown © 2008

aware, must be acknowledged in the test report.

20. The Company must operate to a high standard and be able to demonstrate this to CESG's satisfaction as part of any quality reviews conducted on the Company. Where a Company is accredited as compliant with ISO 90001 or a comparable standard, this will add to the strength of its application for CHECK Service membership.

Claims made by Company

21. The Company must formally advise the Customer in writing whether or not the proposed work is provided in accordance with the CHECK Service. Any non-CHECK Service work must be separately identified. The Company must ensure that CESG are made aware of the performance of the work and given a contractual right of audit. The Company shall ensure that its contractual provisions with the Customer relating to CESG’s right of audit comply with the Human Rights Act 2000.

III. ASSURANCE REQUIREMENTS

Terms of Reference

22. The Company must agree with the Customer terms of reference for the health check. This must include identification of:

    22.1. the system itself;

    22.2. the threats (and threat agents) to be countered;

    22.3. the systems component technologies and products and configuration;

    22.4. the scope of testing.

23. The terms of reference should set out agreement about the supply to the Company of:

    23.1.1. any supporting system security procedures;

    23.1.2. any system security architecture documentation.

24. Note that:

    24.1. The focus and efficiency of testing can be enhanced by the supply of supporting system security procedures and system security architecture documentation (e.g. outlining a network topology) to the Company. The Company is therefore advised to acquire such information where available. This will not preclude the Company from investigating threat scenarios where

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other U.K. information legislation. Refer disclosure requests to the GCHQ Information Legislation Team on 01242 221491 ext 30306 or email infoleg@gchq

Crown © 2008

threat agents do not have direct access to such documentation/information;

24.2. The scope of testing should include those components where there is significant risk of system vulnerabilities being exercised. This will typically involve:

24.2.1. Components at risk from the specified threats;

24.2.2. Components considered by the Company to be particularly vulnerable (in respect of either their construction or supporting system security procedures);

24.2.3. Components in which the Customer has least confidence at the start of the health check (i.e. in respect of either their construction or supporting system security procedures. Note however that it may be appropriate to confirm the secure configuration of those components which are outside the primary scope of the health check, where the Customer is reliant on *general confidence* associated with the component, perhaps because it is an evaluated product.);

24.2.4. Components that are responsible for key critical Security enforcing functions (e.g. Firewalls, Domain Controllers/LDAP servers, System audit server).

24.2.5. Components that are responsible for access to significant levels (due to data volumes or sensitivity) of customer data.

24.3. Where the Customer or system manager wishes for certain critical system elements not to be physically tested (e.g. on account of operational risk), then other means of checking their effect on the security of the system should be sought, (e.g. through confirming release and patch numbers of the associated components and knowledge of relevant vulnerabilities).

25. If, at the scoping meeting stage, it is apparent to the Company that the system is incapable of countering the identified threats, the Customer should be advised forthwith.

Test Preparation

26. The Company shall ensure that it makes appropriate preparation for testing by formulating a test strategy, test plans and test scripts, and should refine and further develop the strategy, plans and scripts, as and where appropriate, during the course of testing. Test preparation is a matter for the Company. However, they shall also consider, and tailor for specific use, the following generic strategy, which has been proven on specific health checks undertaken by CESG.

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other U.K. information legislation. Refer disclosure requests to the GCHQ Information Legislation Team on 01242 221491 ext 30306 or email infoleg@gchq

Crown © 2008

26.1. Attack from External Threat Agents

26.1.1. Attempt to gain electronic access to a target node

26.1.2. Attempt to gain identity credentials for that node

26.1.3. Attempt to deny or disrupt service to that node (if appropriate and with the agreement of the customer)

26.2. Attack from Internal Threat Agents

26.2.1. Attempt to gain extra privileges for (assumed or gained) identity

26.2.2. Attempt to defeat auditing and detection mechanisms

26.2.3. Attempt to defeat other security mechanisms (e.g. access control)

26.3. Attack from Network Threat Agents

26.3.1. Attempt to move on to other network nodes (with appropriate permission)

26.3.2. Attempt to move on to other networks (with appropriate permission)

26.3.3. Attempt to prove access to key data owned by the customer.

Test Requirement

27. The Company must test for:

27.1. all obvious potential vulnerabilities within the scope of the terms of reference (this is expanded by the following guidelines, which are intended to give an illustrative, but not necessarily exhaustive, interpretation of the requirement); and

27.2. any other relevant vulnerabilities sources including those advised by CESG.

Test Guidelines

28. Where reasonably practical, testing shall address:

28.1. each threat identified in the terms of reference (including those which arise from the inadequate application of system security procedures),

28.2. each mode of attack associated with a given threat (e.g. at a first level of

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other U.K. information legislation. Refer disclosure requests to the GCHQ Information Legislation Team on 01242 221491 ext 30306 or email infoleg@gchq

Crown © 2008

categorisation, modes of attack might include monitoring communications, brute force, exploitation of bugs and loopholes),

28.3. each parameterisation of a given mode of attack (e.g. a representative selection of weak passwords),

28.4. each major system component (such as might be identified in the terms of reference) subject to a given threat.

29. Where practical, testing shall also confirm the secure configuration of system components. In confirming secure configuration, testing must address any potential configuration errors which carry the risk of introducing vulnerabilities.

30. Testing must also aim to identify vulnerabilities arising from inappropriate trust relationships; a trust relationship exists wherever a given node or network is connected to a node or network governed by a different security policy, different security management or different security procedures. A trust relationship is inappropriate where false assumptions have been made about the security of a connection or of a connected node or network.

31. When considering the level of testing which is reasonably practical, the following principles apply:

31.1. Where it is impossible to test for all potential vulnerabilities, priority shall be given to those where risks are considered to be greatest;

31.2. Testing must cover all aspects which might reasonably be expected from the terms of reference;

31.3. To maximise test coverage the following types of automatic test equipment shall be used where relevant:

31.3.1. password cracking tools;

31.3.2. network discovery tools;

31.3.3. service discovery tools (e.g. port scanners);

31.4. Confidence in the correct application of procedures may be obtained by sampling, but sampling should be representative of all procedures and personnel, and should never rely on single instances in a particular area of concern.

32. As a general principle, the most recently publicised public domain vulnerabilities should be viewed as representing a particularly significant risk.

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other U.K. information legislation. Refer disclosure requests to the GCHQ Information Legislation Team on 01242 221491 ext 30306 or email infoleg@gchq

Crown © 2008