SERVICE PROVISION GUIDELINES

REQUIREMENT

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

CONTENTS

These requirements may be updated from time to time by NCSC 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).

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

2.3. 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;

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

2.4.1. assessing the Company, on an annual basis being able to exceed the minimum standards for membership of the scheme;

2.4.2. maintaining definition of CHECK standards, and facilitating supply to the Company of recommended public domain vulnerability source information;

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

2.4.4. 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.

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 may suggest appropriate bugfixes 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 NCSC). Failure to do this may result in termination of the CHECK membership Contract as stated at Clause 7.

6 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. However, the following areas of technical expertise are together expected to be of relevance to the majority of HMG systems, and are accordingly recognised as being primary areas of specific expertise in CHECK:

- UNIX
- Windows NT
- network protocols
- use of network test tools
- firewalls.

6.1. Testing on these areas of expertise form the basis of the NCSC-approved Assault courses. Additional Assault courses, which NCSC reserve the right to introduce with agreed Assault Course providers, will test an individual's knowledge of other areas, such as Web vulnerabilities.

6.2. In order to be able to undertake IT health checks under the terms of CHECK, the Company must have achieved 'Green Light' status.

6.2.1. '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.

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

7.1. 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 a NCSC-approved Assault Course. All other members of the team will be required to provide evidence of a baseline level of relevant experience and academic qualifications to attain CHECK Team Member status. 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.

7.2. The Company is required to supply NCSC with evidence of appropriate expertise and continuing personal development for all staff employed on CHECK work by issuing an up to date CV with CHECK membership renewal paperwork.

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

9 Should NCSC have concerns about the service provided by the Company then:

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

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

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

II. QUALITY REQUIREMENTS

Qualifications of Staff

10 All staff employed by the Company on CHECK work must first be agreed by NCSC. 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 NCSC as members of a Company's team before they are eligible to attend an Assault Course and thereby attempt to achieve CHECK Team Leader status. The purpose of CHECK Team Member status is to provide training experience with a view to attaining CHECK Team Leader status in due course. It is the Company's responsibility to ensure that all CHECK Team Leaders and CHECK Team Members are kept up to date with latest developments. Please note schedule 1 for the requirements of CHECK Team Leader and CHECK Team Member.

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

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

- academic IT qualifications,
- relevant IT work experience,
- formal training in IT system management,
- specific computer security training,
- on the job experience,
- vulnerabilities research.

12 Those staff agreed by NCSC as being suitable to be members of a Company's team must hold a minimum of SC security clearance before they can be employed on CHECK Service related tasks. Where they are not already cleared to SC or above, NCSC will sponsor their clearance. Once the security clearance has been confirmed, NCSC 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, shall request NCSC to sponsor them and shall complete the appropriate SC application pack for the SC to be granted by NCSC.

13 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. The team must include at least one member that has passed the relevant 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

14 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

15 The Company:

- should endeavour to notify NCSC at least 5 working days before the commencement of each assignment to be undertaken under the CHECK Service;
- must supply NCSC 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 NCSC.

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

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

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

18 NCSC reserves the right to solicit feedback from Customers receiving CHECK health checks.

19 A newly approved Company will typically be subjected to closer monitoring than a reapproved Company.

Company Quality Standards

20 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:

20.1. 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);

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

20.3. 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;

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

21 CHECK assignments must be conducted impartially and deliver objective technical results and recommendations which have regard to Value For Money:

21.1. 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.

21.2. 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 aware, must be acknowledged in the test report.

22 The Company must operate to a high standard and be able to demonstrate this to NCSC'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

23 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 NCSC 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 NCSC's right of audit comply with the Human Rights Act 2000.

III. ASSURANCE REQUIREMENTS

Terms of Reference

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

24.1. the system itself;
24.2. the threats (and threat agents) to be countered;
24.3. the systems component technologies and products and configuration;
24.4. the scope of testing.

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

25.1.1. any supporting system security procedures;

25.1.2. any system security architecture documentation.

26 Note that:

26.1. 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 Customer is therefore advised to supply such information where available. This will not preclude the Company from investigating threat scenarios where threat agents do not have direct access to such documentation/information;

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

26.2.1. Components at risk from the specified threats;

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

26.2.3. 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.);

26.3. 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).

27 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

27.1. 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 NCSC.

27.2. Attack from External Threat Agents

27.2.1. Attempt to gain electronic access to a target node

27.2.2. Attempt to gain identity credentials for that node

27.2.3. Attempt to deny or disrupt service to that node

27.3. Attack from Internal Threat Agents

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

27.3.2. Attempt to defeat auditing and detection mechanisms

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

27.4. Attack from Network Threat Agents

27.4.1. Attempt to move on to other network nodes

27.4.2. Attempt to move on to other networks.

Test Requirement

28 The Company must test for:

28.1. 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

28.2. any other relevant vulnerabilities sources including those advised by NCSC.

Test Guidelines

29 Where reasonably practical, testing shall address:

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

29.2. each mode of attack associated with a given threat (e.g. at a first level of categorisation, modes of attack might include monitoring communications, brute force, exploitation of bugs and loopholes),

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

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

30 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.

31 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.

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

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

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

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

32.3.1. password cracking tools;
32.3.2. network discovery tools;
32.3.3. service discovery tools (e.g. port scanners);

32.4. 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.

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