

Schedule 1: Call-Off Terms

Date	01/04/2015	Order Reference	ITC11695
-------------	------------	------------------------	----------

FROM:

Customer	Transport for London "Customer"
Customer's Address	55 Broadway, London, SW1H 0BD
Invoice Address	55 Broadway, London, SW1H 0BD
Principal Contact	Name: [REDACTED] Address: [REDACTED] Phone: [REDACTED] e-mail: [REDACTED]

TO:

Supplier	NCC Group Security Services Ltd "Supplier"
Supplier's Address	Manchester Technology Centre Oxford Road Manchester M1 7EF
Account Manager	Name: [REDACTED] Address: [REDACTED] Phone: [REDACTED] e-mail: [REDACTED] Fax: [REDACTED]

1. TERM**1.1 Commencement Date**

This Call-Off Agreement commences on: 01/04/2015

1.2 Expiry Date

This Call-Off Agreement shall expire on:

1.2.1 31/03/2017; or

1.2.2 the second (2) anniversary of the Commencement Date; whichever is the earlier, unless terminated earlier pursuant to Clause CO-9 of the Call-Off Agreement.

1.3 Services Requirements

1.3.1 This order is for the G-Cloud Services outlined below. It is mutually recognised that the volume of these services utilized by Customer may vary from time to time during the course of this Call-Off Agreement, subject always to the terms of the Call-Off Agreement.

1.3.2 G-Cloud Services

1.3.2.1 Lot1 IaaS Not Applicable

1.3.2.2 Lot 2 PaaS Not Applicable

1.3.2.3 Lot 3 SaaS Not Applicable

1.3.2.4 Lot 4 Specialist Cloud Services Provision of Web and Application Testing Services - To provide a range of security testing, monitoring and reporting services across all TfL's websites throughout the build, testing, deployment and live stages of a project. The provision of a managed security service.

Services/activities involved:

- Penetration testing / CHECK Testing / PSN-IT Health Check Services
<https://www.digitalmarketplace.service.gov.uk/service/5-q3-0353-003>
- Technical security assessment and IT security testing services , including
 - Social engineering
 - Remote access security testing
 - Wireless security testing
 - Mobile security testing<https://www.digitalmarketplace.service.gov.uk/service/5-q5-0353-235>
- Load testing
<https://www.digitalmarketplace.service.gov.uk/service/5-q4-0353-227>
- Performance testing
- Monitoring of service availability
- Capability to sub contract accessibility testing if necessary and manage end-to-end testing
- Compatibility testing

<https://www.digitalmarketplace.service.gov.uk/service/5-g4-0353-210>

The following services are covered within NCC Group Proposal filename: "**NCC Group Proposal to TfL Online – Managed Security Services – March 2015**" (Reference P50160): -

- Daily scanning
- Infrastructure penetration testing
- Application security testing
- Provision of a managed service for testing
- Access to a reporting portal to view
 - Reports
 - Vulnerabilities by website
 - Managed service membership and activity

2. PRINCIPAL LOCATIONS

2.1 Principal locations where the services are being performed

The majority of services will be performed remotely from NCC Group Testing laboratories, and/or at nominated TFL sites (TBC).

3. STANDARDS

3.1 Quality Standards

NCC Group is certified to the following quality standards: -

- Comply with ISO 9001
- Comply with ISO 27001

3.2 Technical Standards

For security testing services, we will employ Consultants with the following certifications where required: -

- CHECK Accredited (where required)
- CREST Accredited (where required)

4. ONBOARDING

4.1 On-boarding

Not applicable.

5. CUSTOMER RESPONSIBILITIES

5.1 Customer's Responsibilities

NCC Group will require the following from TfL Online in order to start on time, with the minimum of disruption:

- Any hosts to be strictly excluded from testing
- If applicable, disabling of any host based firewalls for the duration of the assessment or for the IP addresses assigned to NCC Group to be allowed through the firewall for the duration of the assessment
- Logical connectivity (without disruption from any other form of filtering) to each firewall interface that is being tested.
- The IP addresses of the all in-scope devices, to ensure that no mistakes are made through ambiguity.
- The URL to the target applications must be provided.
- Provision of 2 user accounts (with username and password) per consultant for each level
- One card reader and card, session token, RSA token or other device per consultant if this type of technology is present
- An up-to-date version of any client side application required to access the website on DVD or CD ROM if the application is not accessible via a standard web browser such as Firefox, Opera or Internet Explorer.
- Uninterrupted functionality of the application throughout the testing window
- The tested environment to be subject to a change freeze throughout the testing window
- Access to testing exclusive of other testing such as UAT, load balancing or other testing which could make the application behave in a way inconsistent with a normal deployment or otherwise hinder or prevent access to application functionality.
- Should any potential security vulnerability be discovered during any phase of the penetration test, NCC Group will work with the nominated technical contact to find a safe method of verifying the finding.
- No dangerous testing or exploitation of vulnerabilities will be conducted without the express authorisation and scheduling of the nominated technical contact.

5.2 Customer's equipment

Not applicable

6. PAYMENT

6.1 Payment profile and method of payment

Charges payable by the Customer (including any applicable discount but excluding VAT), payment profile and method of payment (e.g. Government Procurement Card (GPC) or BACS)

Pricing for the following services are covered within NCC Group Proposal filename: "NCC Group Proposal to TfL Online – Managed Security Services – March 2015" (Reference P50160): -

- Daily scanning

- Infrastructure penetration testing
- Application security testing
- Provision of a managed service for testing
- Access to a reporting portal to view
 - Reports
 - Vulnerabilities by website
 - Managed service membership and activity

Scanning Package



Pen Testing Package



The following services are also covered within the call-off agreement. Initial quantities for these services are not known at present, so as and when requirements are defined, we will issue individual Statements of Work utilising the pricing model defined within the G-Cloud Framework (subject always to the terms of the call-off agreement): -

- Penetration testing / CHECK Testing / PSN-IT Health Check Services
<https://www.digitalmarketplace.service.gov.uk/service/5-g3-0353-003>
- Technical security assessment and IT security testing services , including: -
 - Social engineering
 - Remote access security testing
 - Wireless security testing
 - Mobile security testing<https://www.digitalmarketplace.service.gov.uk/service/5-g5-0353-235>
- Load testing
<https://www.digitalmarketplace.service.gov.uk/service/5-g4-0353-227>
- Performance testing
- Monitoring of service availability
- Capability to sub contract accessibility testing if necessary and manage end-to-end testing
- Compatibility testing
<https://www.digitalmarketplace.service.gov.uk/service/5-g4-0353-210>

Preferred payment:

6.1.1 For vulnerability scanning services, invoice up front

6.1.2 For testing services, invoice monthly in arrears

6.2 Invoice format

The Supplier shall issue electronic invoices monthly in arrears.

The Customer shall pay the Supplier within thirty (30) calendar days of receipt of a valid invoice, submitted in accordance with this paragraph 6.2 the payment profile set out in paragraph 6.1 above and the provisions of this Call-Off Agreement.

7. DISPUTE RESOLUTION

7.1 Level of Representative to whom disputes should be escalated to:

██████████ NCC Group Finance Director for the Supplier

7.2 Mediation Provider

Centre for Effective Dispute Resolution.

8. LIABILITY**Subject to the provisions of CO-11 'Liability' of the Call-Off Agreement:**

The annual aggregate liability of either Party for all defaults resulting in direct loss of or damage to the property of the other Party under or in connection with this Call-Off Agreement shall in no event exceed £500,000.

The annual aggregate liability under this Call-Off Agreement of either Party for all defaults shall in no event exceed the greater of £500,000 and one hundred and twenty five per cent (125%) of the Charges payable by the Customer to the Supplier in the Year in which the liability arises or any anniversary thereof in which the liability arises

9. INSURANCE**9.1 Minimum Insurance Period**

Six (6) Years following the expiration or earlier termination of this Call-Off Agreement

9.2 To comply with its obligations under this Call-Off Agreement and as a minimum, where requested by the Customer in writing the Supplier shall ensure that:

- **professional indemnity insurance** is held by the Supplier and by any agent, Sub-Contractor or consultant involved in the supply of the G-Cloud Services and that such professional indemnity insurance has a minimum limit of indemnity of one million pounds sterling (£1,000,000) for each individual claim or such higher limit as the Customer may reasonably require (and as required by Law) from time to time;
- **employers' liability insurance** with a minimum limit of five million pounds sterling (£5,000,000) or such higher minimum limit as required by Law from time to time.

10. TERMINATION**10.1 Undisputed Sums Time Period**

At least ninety (90) Working Days of the date of the written notice specified in CO-9.2 of the Call-Off Contract.

10.2 Termination Without Cause

At least thirty (30) Working Days in accordance with Clause CO-9.2 of the Call-Off Contract.

11. AUDIT AND ACCESS

Twelve (12) Months after the expiry of the Call-Off Agreement Period or following termination of this Call-Off Agreement.

G-CLOUD SERVICES CALL-OFF TERMS

BY SIGNING AND RETURNING THIS ORDER FORM THE SUPPLIER AGREES to enter a legally binding contract with the Customer to provide the G-Cloud Services. The Parties hereby acknowledge and agree that they have read the Call-Off Terms and the Order Form and by signing below agree to be bound by the terms of this Call-off Agreement.

For and on behalf of the Supplier:

Name and Title		
Position		
Signature		
Date		

For and on behalf of the Customer:

Name and Title		
Position		
Signature		
Date		