Provision of
CHECK Penetration Test

For

IPO Remote Working Solution

Ref

IT-2015-080

Evolve Secure Solutions Limited

Prepared by:	[redacted]
Version:	**1.0**
Date:	**22nd October 2015**
Quality Assured by:	[redacted]
Released by:	[redacted]

TABLE OF CONTENTS

1 MANAGEMENT SUMMARY

Evolve Secure Solutions Limited (Evolve) is delighted to submit this proposal for a CHECK Penetration Test of the IPO Remote Working Solution.

This is an area in which we have a proven track record having delivered other IPO systems. Our wider IT Security work extends the breadth of the public sector, with similar and recent assignments including the Home Office and Criminal Justice Agencies, Department for Transport and its Executive Agencies, Department for Business, Innovation & Skills and the MoD.

Our capability in this field has been recognised at the highest level as we are approved by Crown Commercial Service for the provision of the full range of ICT Security Services. Our commitment to Information Security is signalled by achieving ISO27001 certification and that combined with our ListX status sets us apart from the majority of our competitors in this field.

In addition to our security accreditations, Evolve delivers all work through an independently audited ISO9001 Quality Management System (QMS) and has signalled its commitment to the Public Sector sustainability agenda through our achievement of ISO14001 certification and approved 'Carbon Neutral' status.

In responding to this requirement Evolve has elected to work closely with our colleagues at Cyberis who are our CHECK "Green Light" accredited partners. Evolve will act as the prime contractor, with Cyberis sub-contracted to perform and fulfil the technical obligations of the contract. This is the same team which has recently delivered three similar IPO ITHC. We regret that due to pre-existing customer commitments we are unable to meet the IPO stated delivery timescales. Our current availability is 10th to 18th September 2015, subject to confirmation at the time of order.

In all other respects we can provide a fully compliant solution to your requirements in that:

- Cyberis are a CHECK company with 'Green light' status;
- All our testers are a minimum of CHECK Team Members;
- All our testers hold a minimum clearance level of SC;
- We use experienced security consultants who have a wide-range of experience in delivering penetration tests for the public service.

In order to ensure availability and contingency, we propose a team approach comprising named CHECK Team Leaders, with support if required from other named CHECK Team Leaders and CHECK Team Members.

Assignment Management and CLAS overview would be provided by [redacted], Evolve's Director of Consultancy. He will ensure that the work is undertaken in accordance with the Evolve ISO9001 accredited QMS. [redacted] is a CESG Listed Adviser Scheme (CLAS) Lead SIRA who has extensive experience of Information Security in the UK Public Sector environment. He is a PRINCE2 practitioner, ITPC Government practitioner and Fellow of the Institute of Business Consultants.

Other key Evolve Support staff for this project are:

- [redacted] Contract & Account Manager
- Operations Manager
- Finance and Quality Manager
- CLAS Consultant
- CHECK Project Manager & Contingency Team Member

In accordance with Evolve's ListX and HMG Framework Accreditations, all Evolve consultants and support staff are cleared to a minimum of SC.

It is Evolve's policy to ensure continuity of key staff throughout the entire duration of a project and we confirm that once assigned our CHECK Team Leader(s) will deliver the work throughout the entire period, with support from the nominated staff detailed above as required.

Based on the information provided, we estimate that up to [redacted] man days may be required to complete the testing and report writing, together with reasonable contingency. We would only charge for the days actually required to be worked. Our day rate for this is £[redacted] + VAT to include all expenses for working at Concept House. Therefore our quote for the up to [redacted] days work is £13,500 + VAT.

1.1 Contact Information

We have provided contact information for [redacted], who is responsible for this submission and if successful would be responsible for all contractual matters and customer care, the consultants, their deliverables and the quality of support provided by Evolve.

Company Name	Evolve Secure Solutions Ltd (Evolve)
Address	A1/1001, Cody Technology Park, Farnborough. GU14 0LX
Telephone	[redacted]
Fax	[redacted]
Email	enquiries@evolvesecuresolutions.com
Company Registration	[redacted]
ISO14001:2004	[redacted]
ISO27001:2005	[redacted]
ISO9001:2000	[redacted]
Contact	[redacted]

2 UNDERSTANDING OF REQUIREMENTS

We have carefully evaluated the ITQ IT-2015-080 and following a clarification audioconference 21st October 2015, confirm our understanding that IPO requires a CHECK penetration test of infrastructure supporting the Remote Working Solution.

The ITHC is required as a check on the architecture and security controls implemented in the Remote Working Solution for the Intellectual Property Office. The tests must identify vulnerabilities in all layers of the system, from administrative accesses to configuration and integration layers and the underlying OS unless identified in the Out of Scope statement below.

The Remote Working Solution is implemented using Airwatch, RSA and VPN in a virtualised environment. The solution is mirrored across two sites, the Live site at Concept House in Newport and an HA backup solution at Companies House in Cardiff.

Logically the system is split across a DMZ, which hosts the Airwatch and RSA systems, and the LAN which holds the management console servers and other related systems, for example file shares, databases and, email servers and supporting LDAP and AD systems.

RSA systems are out of scope of testing, and only iOS devices are in scope for EUD review.

3 DELIVERING THE TESTING REQUIREMENT

3.1 Background

This section explains the methodology used when performing testing engagements, including information on activities prior to performing any work. All IT Health Check activity complies with the methodologies defined for the CHECK scheme. This has been enhanced by our own quality assurance procedures. There are a number of generic procedures that cover all testing scenarios. Specific techniques are described in the following sections.

We will take a manual, consultant-driven approach to your requirements, but one that also follows tried and tested procedures and techniques, meaning that the specific deliverables of the assignment will be delivered in a methodical, organised and timely manner. We will seek to work closely with your staff to ensure the most valuable outcomes, including elements of skills transfer inherent in collaborative working.

As part of any project, we will use some automated tools, typically to allow the consultant to quickly gain a broad understanding of the target environment before proceeding with the manual testing and auditing elements, as required by the project.

3.2 Pre-test Planning Meeting

The engagement will begin with a dialogue between the parties. All parties will exchange key information necessary for the smooth running and successful completion of the project. The agenda will typically include the following:

- Verification that a non-disclosure agreement has been signed to ensure confidentiality for individual specific projects;
- Confirmation of the exact system number at each location and the provision of network diagrams to confirm scope and sample sizes;
- Agreement of the timescale for the test programme, including start date, key milestones and estimated completion, with milestones where appropriate;
- Establish joining arrangements, vetting and access;
- Exchange of relevant contact details to allow both project teams to contact each other, as required;
- Agreement of a method of exchanging the draft and final reports.

Following this initial meeting we will produce a plan for the testing which will incorporate the key requirements and other inputs such as specific threat information, from the relevant project stakeholders.

3.3 Confirmation of Method

The proposed testing will take place 17th to 27th November and cover the following requirements:

1. External ITHC of all internet facing infrastructure

Assess the Airwatch and VPN solutions for any vulnerabilities from an external i.e. Internet-based threat actor, exploiting any found to demonstrate. Firewalls, Load Balancers, Airwatch and RSA servers are in scope as are SSL/TLS configurations and certificates.

2. Internal ITHC of all supporting infrastructure

Assess the Remote Working Solution for any vulnerabilities from an internal threat, exploiting any found to demonstrate. Firewalls, Load Balancers, Airwatch servers are in scope as are SSL/TLS configurations and certificates.

3. End-User Device Configuration Review

Review of device configuration of the Peripatetic devices against the HMG Cabinet Office EUD advice or industry best practice where EUD advice is non-existent. Included elements are AV installation, any HIDS configuration & user & system authentication. Certificates and encryption algorithms are in scope. Attempt to break into a device to gain access to user details and authentication data or sensitive data useful to a hacker. Attempt to spoof a known good device using a known backup as a source (e.g. a full iCloud backup). Review of device configurations against the Government EUD guidance and Vendor Leading Security Practice, including AV installation, any HIDS configuration & user & system authentication. Certificates and encryption algorithms are in scope.

4. Mobile Device Management Configurations

Review of the Management Console for configuration and installation vulnerabilities against Leading Security Practice as defined by the vendor, including network and authentication protocols and user & system authentication.

Out of scope are configurations appertaining to the Active Directory, MS Exchange and other Office services used independently of the Airwatch Solution, any Mobile GPOs or LDAP configurations are in scope.

5. Operating System Hardening and Build
   - Underlying OS of the AirWatch servers
   - AntiVirus and AntiMalware configurations
   - Vulnerability scan & patching status
   - VM Tool Configurations

6. Auditing
   Completeness of Audit Logs

The following works will be undertaken to meet the above objectives:
(a total of [redacted] days).

Phase 1. External Penetration Test ([redacted] days)

An external, black-box penetration test will be performed against the internet facing Infrastructure, in line with CHECK methodologies. There are 3 - 4 external facing IP addresses that comprise the solution.

Phase 2. Internal Penetration Test ([redacted] days)

An internal penetration test will be performed against the internal infrastructure, in line with CHECK methodologies. It is understood from the documentation that there are 7 Airwatch systems at each location, alongside a number of load-balancers.
The security testing will seek to identify the following:

- Vulnerabilities in systems within the DMZ network
- Exposure due to excessive access to the DMZ from IPO user network(s)
- Vulnerabilities in the supporting systems on the internal LAN

Where web or other applications are identified, for example the Airwatch management application, access control checks will be performed to ensure unauthorised access to the application is not possible. A full application test of the Airwatch is understood to be not in scope of this test.

Phase 3. End User Device Review ([redacted] days)

For the purpose of testing, IPO manages 2 different end user device types as follows:

- iPhone (iOS 8+)
- iPad (iOS 8+)

A review of the configuration of these end user devices will be performed and comparisons drawn to industry best practices and government guidelines.
In addition, we will perform tests to establish whether access to a device can be obtained to an unauthorised user, such that access to data on the device can be obtained, or unauthorised remote connectivity to internal IPO systems can be obtained.

Attempts to spoof a known good device will be undertaken, for example restore from iCloud backups.

It is understood that an authorised user's ability to manipulate the device to, for example install unauthorised applications, or code is not of concern at this stage.

Phase 4. Mobile Device Management Configuration ([redacted] day)

We will work with Airwatch MDM administrators to perform a review of the Airwatch Management Console for configuration and installation vulnerabilities against Leading Security Practice as defined by the vendor, including network and authentication protocols and user & system authentication.

Phase 5. Operating System Hardening Review ([redacted] days)

We will perform a review of the underlying operating system build of the Airwatch (Windows Server 2012 R2 (up to 10) and Loadbalancer VA V7.6.2 (up to 4)) against best practices, highlighting areas where security improvements can be made to reduce the exposure of these systems. In addition, specifically the following are to be audited:

- AntiVirus / AntiMalware configurations
- Patching status

Phase 6. Auditing Review ([redacted] day)

We will review the configuration of any implemented Airwatch logging mechanisms to establish areas where improvements can be made to ensure complete auditing of the remote access solution.

3.4 Pre-requisites

In order to conduct the ITHC, we will be dependent upon IPO to provide the following:

- Confirmation of the external facing IP addresses in scope
- Permission to connect testing laptops (up to 2) to the IPO networks, including source IP addresses for testing
- Target/IP address details for the infrastructure testing
- Access to each network segment for testing
- Supply minimum of 1 device of each type, as listed above, configured to use Airwatch
- User credentials, access codes and PINs, as appropriate, for mobile devices
- Confirmation of the servers in scope for build / hardening review
- Administrative credentials for each server included for build / hardening review
- Access to the MDM console to examine configuration
- Point of contact to work with whilst reviewing the MDM configuration
- Point of contact to discuss Airwatch logging, and access to logging configuration
- Completed ‘Authority For Security Testing’ (https://portal.cyberis.co.uk/loa)

3.5 Communication

Our consultants will provide frequent communication, including attendance of daily ‘wash up’ meetings. Where critical or high impact vulnerabilities are identified, they will be brought to the immediate attention of stakeholders. At the end of the ITHC, an informal report to IPO staff will be submitted.

3.6 Reports

Reports are normally issued within [redacted] working days of completion of the testing. Reports will be protectively marked to the same level as given for the test (currently stated as OFFICIAL-SENSITIVE).

Three bound copies and an electronic copy will be provided on CD, delivered by post (normally Royal Mail Special Delivery) within ten working days of testing being completed. An Excel spreadsheet of the vulnerabilities will also be supplied.

3.7 Restrictions

We acknowledge the restrictions set out in section 4.13 of the ITQ:

- Details of test results will not be transmitted across the Internet, unless suitable and approved encryption is used;
- All IP addresses noted in the report will be obfuscated in line with guidance provided by the IPO ITSO;
- The penetration test will exclude activity on the PSN, activity relating to other IPO service hosted at Concept House, Active Directory configuartions that are not part of the AirWatch Solution, the conducting of any tests with a high probability of impacting on the live operation of other services hosted at Concept house
- The ITHC is limited to devices in the specification in the ITQ. Other servers/devices are out of scope.

3.8 General Methodology and Approach

Cyberis follows a comprehensive testing methodology for all engagements, as reviewed and approved by CESG. Our comprehensive methodology, covering infrastructure and application security assessments as referenced in this bid will be used by all consultants engaged in the project.

During your engagement, we will assign a CHECK Team Leader who will be responsible for overseeing delivery of your work and keeping you up to date with progress reports. You will also be provided with an escalation point of contact in the event that any issues arise which cannot be addressed by your CHECK Team Leader.

The CHECK Team Leader will attend the pre-engagement planning meeting, and will be responsible for managing all aspects of the service delivery for IPO including co-ordinating Cyberis resources and providing a single point of contact for IPO staff.

The CHECK Team Leader will agree deliverables with IPO staff at the pre-engagement planning meeting and will ensure that these are produced within the agreed timescales.

3.9 Dependencies

In making this proposal we would be dependent on IPO to:

- Confirmation of the external facing IP addresses in scope
- Permission to connect testing laptops (up to 2) to the IPO networks, including source IP addresses for testing

- Target/IP address details for the infrastructure testing
- Access to each network segment for testing
- Supply minimum of 1 device of each type, as listed above, configured to use Airwatch
- User credentials, access codes and PINs, as appropriate, for mobile devices
- Confirmation of the servers in scope for build / hardening review
- Administrative credentials for each server included for build / hardening review
- Access to the MDM console to examine configuration
- Point of contact to work with whilst reviewing the MDM configuration
- Point of contact to discuss Airwatch logging, and access to logging configuration
- Completed 'Authority For Security Testing' (https://portal.cyberis.co.uk/loa)

3.10 Testing Tools Employed

Our consultants use a wide range of tools when carrying out testing services, depending on the technology they are testing. We ensure that our consultants are experienced and familiar with using all tools within a controlled environment before they are used on client engagements.

To ensure that we provide a comprehensive service, we use a variety of Open Source, commercial and proprietary tools. All our tools are sourced from a trusted supplier so that we can be sure that they are free from malicious code.

The source code of any exploit scripts from untrusted sources is examined prior to use and thoroughly tested within a controlled environment before being used. This will ensure that their function is understood and that they will not introduce any vulnerabilities to our clients' systems

So that we can provide extra value to our clients, we have developed a number of proprietary tools. In addition, our consultant can write scripts or develop tools as necessary if a particular test scenario requires.

If required we will provide IPO with a list of all tools to be used.

3.11 CHECK Team Leaders

The work will be undertaken by two of the following CHECK Team Leaders. The nominated CHECK Team Leaders will be confirmed at time of order and will be allocated to the work for the duration of the assignment.

3.12 [redacted] - CHECK Team Leader

Profile

[redacted] is an IT security professional with extensive managerial experience. He has a track record for innovation, having conceived and delivered new security products and service lines for established information security consultancies.

[redacted]'s experience encompasses in-depth infrastructure and application penetration testing, and [redacted] is a CREST Certified Tester for applications. He is also a recognised expert in the field of network forensic analysis, holding the CREST Certified Network Intrusion Analyst qualification. He was also a member of CESG's review panel for technical architectural solutions whilst working for GCHQ, offering technical project advice and assurance to multiple government and private organisations.

Before joining Cyberis, [redacted] was responsible for meeting demanding financial and delivery targets as the head of a service line for one of the UK's foremost consultancies. [redacted] continuously shares research and development across the security industry through various conferences, information exchanges and published tools.

Qualifications

- CHECK Team Leader (Infrastructure and Applications)
- CREST Certified Tester (Applications and Network Intrusion Analysis)
- HMG SC and DV clearance
- Non-Police Personnel Vetting
- First Honours Degree in BSc Software Engineering

Employment History

- March 2012 – Present: Director (Cyberis Ltd)
- June 2011 – March 2012: Security Consultant ([redacted])
- October 2008 – June 2011: Head of Network Forensics ([redacted])
- January 2008 – October 2008: Emerging Threats Team Lead ([redacted])
- October 2005 – January 2008: Lead Analyst and Incident Handler in GovCertUK ([redacted])

Areas of Expertise

- Computer forensics
- Network forensics
- Development of security tools and products
- Web application architecture, design, implementation and penetration testing
- Infrastructure penetration testing
- IDS architecture, deployment, analysis and rule development
- Open source information gathering
- Linux/Unix operating systems

Example Engagements

Incident Response and Forensic Investigation - Major High Street Retailer

[redacted] was assigned to investigate a reported compromise of credit card data from an Internet store of a major high street retailer. As many thousands of transactions

passed through the site each day, it was critical to minimise downtime to reduce the cost to the business. [redacted] led the investigation from the outset, including conducting complex acquisition of several servers and workstations out-of-hours at a customer data centre. An in-depth review of the web application code and decoding of several covert web 'back-doors' revealed a sophisticated theft of over 500,000 credit cards.

[redacted] has developed specialist acquisition techniques which have been proven in the field, dealing with high availability, scalable and redundant e-commerce systems that cannot simply be disconnected and detained. In addition to the numerous PCI related engagements delivered, [redacted] has carried out several investigations surrounding acquired workstations and laptops on behalf of UK government at SECRET level and above. Technical knowledge gained and regularly exercised during penetration testing allows [redacted] to understand the motivation and techniques used by attackers and nefarious individuals to uncover covert data, tools and other incriminating evidence from an engagement.

CHECK Test – Central Government Departments

As an active member of the CESG 'Virtual Team', [redacted] regularly worked on many of the UK's most critical networks and systems. This often involved a full IT Health Check of high classification systems, identifying vulnerabilities that may be exploited by an attacker, assessing the level of skill required to exploit, and the impact to UK national interests if an attacker were to actually compromise the systems. Many of the tests that [redacted] has carried out have identified risks that have implications government-wide.

Finance – European Online Banking Site

In 2011 [redacted] conducted a remote web application test of a European bank. Despite the client spending significant budget on the security of the public website, [redacted] was able to circumvent authentication to the website in a multitude of ways. As a result of testing, it was possible to demonstrate to the client how an attacker could easily transfer funds using techniques such as cross-site request forgery (CSRF), and gain access to administrative functions of the host across the Internet without any valid credentials

3.13 [redacted] – CHECK Team Leader

Profile

Over a decade working in the security consultancy industry, [redacted] has delivered information assurance consultancy engagements and compliance audits, together with numerous public and private sector infrastructure and application penetration tests. [redacted] is a CHECK Team Leader and CREST certified tester for both infrastructure and applications.

[redacted]'s wide experience includes engagements across Government, law enforcement, retail, financial, telecommunications and gambling sectors, and participation in a large range of projects including infrastructure and application penetration testing, information risk assessment, due-diligence compliance auditing, network forensic analysis and social engineering exercises.

Her strong communication skills and technical acumen allows her to engage at all levels, in order to deliver quality services to clients.

Qualifications

- CHECK Team Leader (Infrastructure and Applications)
- CREST Certified Tester (Infrastructure and Applications)
- HMG SC clearance
- Non-Police Personnel Vetting
- Imperial College, B. Eng. (Hons.) Computing

Employment History

- March 2012 – Present: Director (Cyberis Ltd)
- June 2011 – March 2012: Security Consultant ([redacted])
- March 2006 – July 2011: Head of Technical Consultancy ([redacted])
- January 2004 – March 2006: Security Consultant ([redacted])

Areas of Expertise

- Web application architecture, design, implementation and penetration testing
- Infrastructure design and penetration testing
- Information security risk assessment
- Information security consultancy
- Compliance auditing
- System build hardening and secure network device configuration
- Open source information gathering
- Linux/Unix operating systems

Example Engagements

Application Security Test for Government

A Government organisation required a web application to go live at very short notice. The penetration test revealed serious flaws, both in application design and business logic, potentially allowing malicious entities unauthorised access to highly personal information stored in the application's database. Deploying the application without these vulnerabilities being uncovered could have led to a serious data breach, leaving the client open to prosecution under the Data Protection Act, and the target of bad publicity. [redacted] recommended a complete redevelopment of the application, offering advice to the developers about secure coding practices from the start. As a result, the client was able to address the weaknesses in the application at the root cause level, reducing the on-going risk of compromise and support costs.

Technical Security Consultancy for Government Agencies

As part of the accreditation process for a client's restricted network, [redacted] coordinated the delivery of a multi-phase engagement, covering the client's networks and third parties in multiple locations across the country. In addition to enumerating individual vulnerabilities, the environment-wide testing revealed a number of serious underlying process failures that needed to be addressed to ensure that data within the network would be properly protected. The report from [redacted]'s team allowed the client to relate these findings constructively to the third parties involved in network and infrastructure management, and effect long-term changes in their internal security management processes to prevent recurrence of the issues identified.

User Access Review for Financial Organisation

A financial organisation was required to perform an internal due diligence audit, ensuring that all critical IT systems and applications conformed to the organisation's central policies with regards to user access, authorisation and accounting. Over the course of three months, [redacted] led a team of consultants conducting audit interviews with key systems administrators and business stakeholders, supplementing this with a hands-on technical investigation, to accurately establish the user access models present across the wide variety of technologies in use.

The result of the assessment was a documentation set identifying where current system management practices deviated from the organisation's internal policy requirements, including the identification of unnecessary access privileges, poor password management, areas where obsolete accounts had been left active and areas where system management did not conform to best practices.

[redacted]'s team also produced an access control framework report for each of the organisation's most critical applications, documenting exactly which employees had access to what, and what processes and procedures were in place to control access. The project was instrumental in allowing the client to focus their remediation effort on the most adversely affected systems in preparation to meet the requirements of their own group policies and an impending internal audit.

3.14 [redacted] – CHECK Team Leader

Profile

[redacted] is a CHECK Team Leader and security specialist with significant experience in technical security, penetration testing, application security testing, security infrastructure design and implementation and security best practices. He has a proven track record in the security and risk management field with practical experience of implementing security management frameworks (BS7799 / ISO27001).

He brings significant experience in design, configuration, maintenance and troubleshooting of layer 2 and layer 3 networks and VOIP solutions.

More recently, [redacted] has been responsible for running a team of consultants, managing workloads and maintaining budgetary control across a team of 20 consultants whilst ensuring that skills and personal development of team members is appropriate.

Qualifications

- CHECK Team Leader
- SC Cleared
- 1994 - BSc (Hons) Psychology - [redacted].
- 1991 - A Levels (Maths Physics Chemistry) - [redacted],
- 1989 - GCSE's (9), [redacted]

Employment

- May 2014 - Present – CHECK Team Leader - Cyberis Limited
- Feb 2011 - May 2014 - Managing Consultant - [redacted]
- Jan 2009 - Feb 2011 - Senior Consultant - [redacted]
- Nov 2007 - Jan 2009 - Consultant - [redacted]
- Feb 2004 – Oct 2007 - Security and Networks Analyst - [redacted]
- 2000 – 2004 - Network support technician - [redacted]
- 1998 - 2000 - Support Engineer - [redacted]
- 1994 - 1998 Research Assistant - [redacted]

Areas of Expertise

- Network penetration Testing
- Application security and penetration testing
- Networking and security infrastructure.
- Team Management

3.15 [redacted] – CHECK Team Leader

Profile

[redacted] is a CHECK Team Leader and CREST certified Information Security Consultant with over fourteen years' experience in IT, the past seven of which have been in dedicated information security roles. He has expert technical knowledge of web applications, networks, all major desktop and mobile operating systems and is skilled at both offensive and defensive security techniques.

He is used to working across all levels of an organisation and is highly adept at discussing technical content with both technical and non-technical audiences. [redacted] is an active member of the Information Security community, learning and working for constant improvement through knowledge sharing and personal research.

Qualifications

- 2013 CHECK Team Leader
- 2012 CREST Certified Tester (Applications - [redacted])
- SC Cleared
- 2007 Certified Information Systems Security Professional (CISSP)
- 2005 - Cisco Certified Network Associate (CCNA)
- 2003 - Red Hat Certified Engineer (RHCE) - [redacted]
- 2003 - Sun Microsystems Certified Solaris 8 Administrator

Employment History

- July 2014 – Present – CHECK Team Leader – Cyberis Limited
- December 2013 – Present – Director – [redacted]
- October 2011 – April 2014 – Principal Security Consultant – [redacted]
- October 2009 – October 2011 – Information Security Manager – [redacted]
- May 2007 – October 2009 – Security and Networks Manager – [redacted]
- May 2003 – May 2007 – Senior Systems Administrator/Deputy IS Manager – [redacted]
- March 2000 – May 2003 – Senior UNIX and Networks Engineer – [redacted]
- September 1999 – March 2000 – IT Manager – [redacted]
- March 1999 – September 1999 – UNIX and Windows Administrator – [redacted]

Areas of Expertise

OPERATING SYSTEMS: • Cisco IOS, CatOS and PixOS • Check Point SecurePlatform • Nokia IPSO up to 4.2 • GNU/Linux (Red Hat, Debian, Ubuntu + others) • Solaris 2.5.1/2.6/8/9/10 • Windows NT/XP/2000/2003/2008/Vista/7 • FreeBSD, OpenBSD, BSDi, HP-UX • Backtrack/Kali Linux • Mac OS X • Citrix XenServer • VMWare ESX/ESXi	**PROGRAMMING LANGUAGES:** • Ruby • Python • PHP • Shell Scripting • Perl • Java • C# .NET • C **COMPLIANCE:** • PCI DSS • ISO 27001
HARDWARE: • Experience across a broad range of hardware including Cisco, Nokia, HP, Dell and Sun	**SOFTWARE:** • Apache & ApacheSSL • Tomcat Java Servlet Engine • Much, much more

Example Engagements

- Successfully completed many security testing engagements for clients, responsible for scoping and proposal generation through to scheduling, delivery and post-testing wash-up;
- Wrote and delivered a workshop “Burp Suite Plugin Development for Java n00bs” at 44CON, London 2012;
- Spoken at PHP London on the state of PHP (in)security;
- Spoken at OWASP Birmingham on PHP Object Injection, Burp Suite and Splunk;
- Presented lightning talks at BruCON 2012 and 2013;
- Identified and developed an exploit module for the [redacted] for a security weakness in Splunk (Enterprise and Free);
- Developed a PCI DSS compliant information security policy from scratch and implemented solutions that have seen [redacted] through two successful PCI DSS assessments in 2009 and 2010.
- Introduced a cost-effective security solutions programme utilising intelligent deployment of both open source (FOSS) solutions and commercial applications.
- Conducted internal penetration testing which identified several critical vulnerabilities. Specified and implemented solutions for all test findings.
- Designed, planned and implemented a PCI DSS 1.2 compliant network and systems infrastructure. This involved a requirements gathering exercise, followed by detailed design and submission to our QSA for approval before planning, recruiting additional resource, purchasing and ultimately, implementation. Delivered hands on technical skills as well as managing a small team of contractors for this project.

3.16 Quality Management

The established procedure for dealing with work of this type is based upon Evolve's standard ISO9001 certificated processes, augmented by additional Account Management activity, to ensure complete supplier management and quality of Management Information, reporting and communication.

Cyberis has formally committed to Evolve's ISO9001 quality management procedures together with the Evolve stated company policies, standards and values. Evolve's role in any sub-contracted assignment is a proactive and visible one, in order to provide IPO with the assurance that all work is undertaken to our usual standards and in accordance with the Crown Commercial Service framework terms and conditions.

This process is defined within our Quality Management System (QMS) that includes procedures for the selection, management and quality assurance of sub-contractors. For completeness, we have included below the relevant sections from our QMS.

- Cyberis have been subject to a range of background checks including security vetting, capability to undertake the role and financial standing;
- Evolve have verified Cyberis technical and professional qualifications, track record and taken up appropriate public sector references;
- Cyberis has signed up to the Evolve quality system, with its required controls.

Evolve have assessed Cyberis in accordance with procurement and evaluation regimes established by organisations such as the Crown Commercial Service, including tendering, evaluation and identification.

Formal contracts are in place with Cyberis, defining all aspects of the relationship, including quality, performance, confidentially (based upon our ISO27001 certification), compliance with all health & safety legislation, standards, liability and intellectual property rights.

Only where we are satisfied that the sub-contractor and their consultants meet the client's requirements will they be recommended as part of any Evolve proposal. All sub contract work is subject to management by a full time senior member of the Evolve consultancy team through the application of defined and certificated 'Assignment Management' procedures. This role will be undertaken by [redacted], Evolve's Director of Consultancy. He will ensure that the work is delivered in accordance with the Evolve ISO9001 accredited QMS and the requirements of the CHECK scheme. [redacted] is a CESG Listed Adviser Scheme (CLAS) Lead SIRA who has extensive experience of Information Security in the public sector. He is a PRINCE2 practitioner, ITPC Government practitioner, Fellow of the Institute of Business Consultants and was a civil servant for 13 years.

4 CHARGES

4.1 Structure and profile of our proposed team

We propose a team approach undertaken by nominated CHECK Team Leaders.

Assignment Management and CLAS overview, provided by [redacted], Evolve's Director of Consultancy, together with Customer Care and Account Management Support will be provided free of charge.

4.2 Consultant fees

We propose a single day rate of [redacted] for all elements of this work.

This rate is inclusive of all framework, customer, quantity and other discounts from the commencement of the work.

Hard drives to be left on site at the conclusion of the testing (if necessary) are to be replaced at cost.

Travel and subsistence costs for working at Concept House are included.

All prices quoted are exclusive of VAT at the prevailing rate.

4.3 Commercial Offer

Based on the information provided, we estimate that up to [redacted] man days may be required to complete the testing and report writing, together with reasonable contingency and follow up. We would only invoice for the days actually worked.

Based upon these assumptions we estimate a total cost of up to [redacted] at [redacted] per day = £13,500 + VAT.

We can confirm that this proposal shall remain valid for 30 days from the date of close of tender.

4.4 Acceptance of IPO Terms and Conditions

Evolve confirms acceptance of the IPO Standard Terms and Conditions and that no other Terms and Conditions shall apply.

Evolve confirms acceptance of the IPO Intellectual Property Rights as outlined within Clause 27 of the above IPO Standard Terms and Conditions.

Evolve confirms acceptance of Section 9 of the ITQ regarding the Requirement to Publish Contractual Information.

5 CORPORATE CAPABILITY

5.1 Evolve Secure Solutions Ltd

Evolve is an independent business consultancy, focused on providing high quality consultancy solutions to the Public Sector. We are on a number of Crown Commercial Service and other frameworks, providing a range of services such as ICT Security, ICT Strategy, Performance Management, Business Continuity Planning and Financial Management. We have an established Information Assurance and Security Practice, which is managed by [redacted], our Director of Consulting, who is a CLAS consultant and ISO27001 Lead Auditor.

We are founder members of the CESG Listed Advisor Scheme (CLAS) for security consultants and all of our ISO27001 focused consultancy services were designed by a qualified ISO27001 Lead Auditor. Evolve holds its own certification to ISO27001. Our Quality Management system is ISO9001 certificated, and all our consultants receive full account management and technical support from our dedicated operational team.

In accordance with the Public Sector commitment to the environment and sustainability, Evolve is certificated to ISO14001 and is also an accredited 'Carbon Neutral' company. We are committed to continuing improvement of sustainability across all our corporate operations.

5.2 Cyberis

Cyberis is a CESG IT Health CHECK service company and is a CREST member.

All of their consultants are recognised experts in the security field, holding qualifications such as CHECK Team Leader, CREST Certified Infrastructure Tester and CREST Certified Application Tester. Our consultants have extensive experience working within multiple industry sectors and in similar projects, and are able to apply a wealth of historical knowledge to the project.

Cyberis prides itself on offering pragmatic and sensible solutions to risk management within business, taking business needs into account when prioritising remediation advice. We like to work closely with our clients to understand their business objectives, and their information assets, so that the advice we provide is relevant and contextualised.

5.3 References

We have provided the following references and case studies for our CHECK delivery partner Cyberis. Evolve references and track record can be provided upon request.

[redacted]

Cyberis has recently delivered a number of similar ITHC in respect of the [redacted] Protect Network under contract to Evolve.

[redacted]

E: [redacted]

[redacted]
Cyberis performed an application penetration test of an HMG system for [redacted] in September 2012.
[redacted]
E: [redacted]

[redacted] is a financial software development house. Cyberis has conducted a number of technical assurance engagements with [redacted] in recent months including extensive application and infrastructure level assessments.
[redacted]
E: [redacted]
M: [redacted]
F: [redacted]

[redacted]
Cyberis staff have performed work with the [redacted] in the past, in many areas, but particularly infrastructure security testing and incident response.
[redacted]
T: [redacted]
M: [redacted]
F: [redacted]
E: [redacted]

5.4 Case Studies

Within the last 12 months, Cyberis has delivered numerous engagements with HM Government, including:

- Four ITHC engagements conducted with [redacted], incorporating both infrastructure level assessments and application security testing;
- A multi-phase ITHC of a ministerial department network, including full internal and external infrastructure penetration tests, build reviews of servers and workstations, and password audit of the domain – providing a comprehensive assessment and level of assurance. Cyberis was commended for providing a 'first-class service with great helpful people';
- An extensive assessment of a sensitive internal production environment which incorporated infrastructure IT Health Checks, firewall configuration reviews, system and host build analysis and application security assessment. The organisation in question manages several large databases containing large quantities of personal data, and a review of this data protection against the requirements of GPG13 was also mandated;
- An extensive application security test against a platform providing statistical information to various Government agencies. The assessment revealed horizontal access control weaknesses that could compromise the confidentiality of the information. Following advice from Cyberis, our client was able to remediate these issues.

In the commercial arena, Cyberis has been recently involved in a number of relevant engagements, including:

- A full security assessment of public-facing transactional web applications, associated APIs and supporting infrastructure, identifying serious weaknesses in sensitive data handling and session management;
- An extensive and long term security consultancy engagement with a large organisation in the gambling sector which involved end-to-end security consultancy and technical assurance – covering everything from data mapping and migration plans, to the technical security of customer information, the security of associated web applications and payment details stored within back end processing systems;
- A full application security assessment for a financial software house which revealed a number of important access control issues within the application configuration. The weaknesses identified could have caused significant financial and reputational damage to the organisation concerned.