IT HEALTH CHECK OF THE

IPO NETWORK INFRASTRUCTURE &

APPLICATIONS

STATEMENT OF WORK

Intellectual Property Office

London UK

UK Office:

Gotham Digital Science Ltd

161 Drury Lane

London WC2B 5PN

United Kingdom

New York USA

US Office:

Gotham Digital Science LLC

125 Maiden Lane – Third Floor

New York, NY 10038

United States

Contents

This Statement of Work (SOW) will confirm your engagement of Gotham Digital Science Ltd ("GDS") to perform Security Services ("Services") for Intellectual Property Office ("IPO" or "Client"), and is issued pursuant to GDS' Terms and Conditions, which are set out in Appendix A. Upon signature of this SOW the terms of GDS' Terms and Conditions shall be incorporated into and form part of this SOW.

Proposal Details

Client Name:	Intellectual Property Office
Project Name:	IT-2015-81
Proposal Date:	16 November 2015
Author:	[redacted] Gotham Digital Science, 161 Drury Lane, London. WC2B 5PN Email: [redacted] Office: [redacted] Mobile: [redacted] Fax: [redacted] Website: http://www.gdssecurity.com Public Key Fingerprint: [redacted] SendSafely Secure Link: [redacted]
Client Contact Details:	[redacted] Intellectual Property Office, Room GY33, Concept House, Newport, NP10 8QQ, Email: [redacted] Office: [redacted]
GDS Project Reference Number:	[redacted]
Estimated Start Date:	23 Nov 2015

Proposed Statement of Work for Intellectual Property Office

Section 1: Management Summary

Gotham Digital Science (GDS) has prepared this Statement of Work (SOW) following a request by Intellectual Property Office (IPO) for an IT Health Check of their network infrastructure and applications. Gotham Digital Science (GDS) is an international security services company founded in 2005 and specialising in Penetration Testing, Application and Network Infrastructure Security, and Information Security Risk Management.

IPO (an operating name of the Patent Office) is an Executive Agency of the department of Business, Innovation and Skills (BIS). It aims to stimulate innovation and enhance the international competitiveness of British industry and commerce. It offers customers an accessible, high quality, value for money system both nationally and internationally, for granting intellectual property rights.

This engagement will be conducted by CHECK Team Leaders, supported by CHECK Team Members, in line with the CESG CHECK scheme and is intended to assist with the IPO's PSN compliance and accreditation. The project will comprise two distinct strands:

1. An internal IT Health Check supporting IPO accreditation. This will be conducted using a white-box approach. A single report will present the findings of this stage of the test.
2. An external penetration test supporting both PSN compliance and IPO accreditation. This will be conducted using a black-box approach. A single report will present the findings of this stage of the test.

It is understood that all parts of the engagements, including all data and documentation, will be protectively marked Official Sensitive and shall be treated accordingly in all communications.

Section 2: Understanding of Requirements

This engagement will be conducted by the GDS CHECK team and will assess the internal network infrastructure and applications, as well as the externally Internet facing network, against current industry best practice and in line with CESG's CHECK testing guidelines.

- Internal IT Health Check – This testing will be conducted against the internal networks and applications on site at Concept House in Newport, Wales and will take a white-boxed approach. The aim of this test is to assure the security posture of the design, build and management of the IPO networks and applications (hosted on virtual servers) and should identify vulnerabilities which present a risk to this security posture.
- External Penetration Test – this will be a black-boxed test of the Internet facing elements of the IPO network infrastructure. All stages of this test shall be conducted in liaison with the IPO Head of Security/Accreditor who will mediate with the IPO DSO/ITSO for the duration of the test.

Section 3: Requirements

This engagement will be conducted in two distinct phases with a separate report being produced to present the findings in each phase.

- Internal IT Health Check - This stage of the test will aim to identify vulnerabilities and configuration weakness using a comprehensive approach including (but not limited to):
    - Unauthenticated Network vulnerability scan
        - A 30% sample of these networks will be assessed. To cover this significant number of hosts GDS would require a testing laptop to be scanning overnight as well as during business hours.
    - Firewall rulebase review.
        - Four firewall configuration files will be reviewed offsite at GDS's London Offices.
        - The rules should be provided in a flat text file; GDS can provide guidance on how to extract these files upon request.
        - The following devices will be assessed:

- Internal CheckPoint firewall.
- External CheckPoint firewall.
- One Cisco ASA (VPN termination point)
- One Cisco ASA (internet connection point)

  - VLAN bridging and a review of the DMZ architecture and vulnerability to DMZ 'hopping'
    - A 10% sample of VLANs (23) will be assessed)
  - Sample testing of three virtual machines. This will be a build review against industry best practice, including CIS hardening guidelines. A local administrative account will be required for each. The following devices will be assessed:
    - One vSphere host
    - One Windows 7 desktop
    - One Windows 7 laptop.
  - A build review of up to seven Windows and Linux servers (a total of seven servers). An administrative level account will be required for each device
  - SQL database secure configuration review to include patching, default configuration, default services, internal access controls and penetration test from the internal network on up to two SQL servers. An admin level account (sysadmin) will be required for each device
  - Web server secure configuration of IIS, Apache and Tomcat servers (three servers). A local administrator account will be required for each device
  - Review of local audit and logging configuration of the above devices
  - Review of local access controls of the above devices
  - Wi-Fi security assessment to include three SSIDs (1 guest & 1 corporate & 1 other)
- This stage of the test will provide a comprehensive unauthenticated infrastructure assessment of the external security posture of the IPO Internet facing network (five IP addresses) by evaluating the following:
  - Open ports and available services
  - Exposed web and application services
  - File Transfer services
  - Script injection and input validation
  - Exposure to the Internet and robustness of protective controls between the internal environment and the external DMZs.
  - Vulnerability assessment of Internet facing IP addresses
  - Mobile Worker Access (MDM entry point) – this will be a black-box assessment (unauthenticated) and will attempt a VPN breakout. No two-factor authentication solutions will be assessed.

GDS are to restrict testing to the list of devices provided by the IPO. All other servers and switches are specifically out of scope. Furthermore, GDS are explicitly forbidden from:

- Conducting any activities on the PSN.
- Conducting any activity relating to other services hosted at Concept House.
- Conducting of any tests (Denial of Service, etc.) with a high probability of impacting on the live operation of other services hosted at Concept House (unless expressly permitted by the IPO Accreditor).

Once all testing activities are completed, comprehensive reports of all identified security issues will be prepared as the primary project deliverable.

Detailed analysis of the test findings will be conducted to identify and formulate valid attack paths, often combining multiple vulnerabilities, to demonstrate the different avenues of attack and the current threat posture of the site.

The reports will include the necessary information for systems administrators and owners to implement the necessary changes to correct or mitigate all identified vulnerabilities. Security issues are typically rated on a scale from 1 to 4, based on the perceived threat in the context of the client's network environment.

Also included in the report are detailed walkthrough's of any proof-of-concept exploits that were carried out during the assessment, including screenshots illustrating each step.

An outline of our typical assessment report includes the following sections:

- Project Summary / Executive Summary
  - Report introduction
  - Project scope overview and timeline
  - Exposure profile
  - Remediation strategy
- Testing Overview
  - Testing performed
  - Test targets / subjects
  - Major findings by severity level
- Itemised Issue Listing
  - Detailed findings and recommendations for all identified issues
- Walk-Through of Selected Findings / Exploits
  - Proof-of-Concept exploits and vulnerability screenshots

The GDS Exposure Profile summarises all of the identified security issues by Exposure (Xp) Level. Security issues are grouped into each level based on GDS' understanding of the environment.

Exposure levels are ranked 1 through 4, with Xp1 comprising those issues that are perceived to pose the greatest security threat, relative to all identified exposures.

A suggested remediation timeframe and the general criteria used to classify items, in each exposure level, are also provided within the profile matrix.

The delivery of the reports will be completed no later than Friday 11th December. Both reports will be protectively marked OFFICIAL:SENSITIVE and will be communicated accordingly. In addition to the final reports, GDS will deliver a vulnerability summary spreadsheet for each test which will include the following details:

- Task Reference
- Issue Number
- Affected Host(s)
- Severity
- Impact
- Threat
- Summary of Finding
- Recommendation

Full details of the GDS testing methodologies for both the internal and external elements of this engagement are available upon request.

If GDS are invited to proceed with this engagement it would be the intent to commence the internal phase of the test on 23rd November 2015 which would complete within [redacted] business days, including [redacted] business days onsite testing and [redacted] further days to conduct the firewall reviews (if they can be conducted remotely), all analysis and final reporting. The external element would commence on 4th December 2015 and would complete within [redacted] business days. It is understood that all testing would be conducted within normal business hours.

GDS is a member of CREST, the Council of Registered Ethical Security Testers, as well as a UK Government CHECK scheme "Green Light" company. GDS regularly performs testing of extremely sensitive production applications and networks for commercial sector clients and provides security assurance services to Her Majesty's Government across UK Critical National Infrastructure, including a number of engagements for IPO in recent years. GDS is also a member of the CBEST scheme, allowing GDS to deliver intelligence-led penetration testing for financial services organisations regulated by the Bank of England, as well as the Cyber Essentials scheme, allowing GDS to assess and certify organisations to the UK Government's Cyber Essentials standard. This indicates the experience and capability of GDS to deliver a fully comprehensive and professional assessment of the security posture of IPO in line with both CHECK and PSN requirements.

Section 4: Charges

Description	Unit	Cost
Internal IT Health Check including: 30% sample VA (24/7 scanning) Firewall review VLAN Hopping (23 VLANs) Build reviews (10 devices) SQL database review (2 sql dbs) Web server config review (3 servers) WiFi PT (3 ssids)	[redacted] Days (total) [redacted] Days [redacted] Days [redacted] Days [redacted] Days [redacted] Day [redacted] Day [redacted] Day	[redacted]
External Penetration Test including	[redacted] Days	[redacted]
Analysis and reporting	[redacted] Days	[redacted]
Estimated Expenses		[redacted]

The fee for the project will be based on [redacted] days of information security review and testing services at a cost of **£22,900 excluding VAT.**

- Testing will be carried out on a "best efforts" time boxed approach.
- VAT will be applied at the applicable rate at the time of invoicing.
- All testing will be conducted by a CHECK Team Leader but may be supported by a CHECK Team member if required to meet the deadlines of the test. It is expected that the following personnel will be conducting the testing:
    - Onsite IT Health Check – [redacted] (CTL)
    - Onsite IT Health Check – [redacted] (CTM)
    - Onsite IT Health Check – [redacted] (CTL)
    - External Penetration Test – [redacted] (CTL)

  It is understood by GDS that any changes to this CHECK team must be agreed with IPO before the test commences.
- GDS expect the following expenses to be charged during this engagement:
    - Accommodation – £990 (9 nights @ £110.00 (incl. VAT) per night B&B) – dependent upon late availability
    - Car Hire – £130 (estimate)
    - Fuel - £100 (estimate)
    - Standard class return rail fare from London to Newport - £200
    - Food - £270 (9 days @ £30 per day)
    - Bridge Toll - £6.40
- GDS will issue invoices at the completion of each phase, and payment of each invoice will be due within 30 days of the invoice date.

It is anticipated that testing activities will be performed at Intellectual Property Office, Concept House, Newport, NP10 8QQ and remotely at GDS' London offices.

Section 5: Other information

GDS Exposure Levels

The following table illustrates and summarises the different Exposure Levels.

Exposure (*Xp*) Level	Description
	***Xp*[1]** Remotely exploitable issue, which can directly be used to compromise the server, access sensitive application functionality, or obtain confidential data. This includes impersonation of application accounts and unauthorised administrative host/application access. Typically, the exposure is easily identified and successful exploitation is trivial.
	***Xp*[2]** Exploitable issue which could result in server compromise, access to sensitive application functionality, or disclosure of confidential data. Successful exploitation may require either user-level access to system/application or exploits may not be publicly available.
	***Xp*[3]** Issue is typically leveraged in conjunction with one or more security issues to compromise the server, application, data, or application accounts. This level is also used to classify failures in error handling, auditing, or logging.
	***Xp*[4]** Results from general information leakage about the application, network, server, user accounts, or is inconsistent with security best practices and guidelines.

Rules of Engagement

GDS and the Intellectual Property Office agree to comply with the following rules of engagement:

- A Client Point-of-Contact (CPOC) will serve as the main point of contact for all aspects of testing. GDS will communicate primarily with the CPOC. In addition, Intellectual Property Office should communicate primarily with the identified GDS Project Lead.
- The CPOC will ensure that all necessary information required for the engagement is provided to GDS prior to or during the kick off meeting. For example, such information could include, but is not limited to, design documentation, target IP addresses, valid test accounts, and appropriate project team contact information. Please note that failure to provide or make available any of the pre-requisites listed could affect the amount of effort required to complete the assessment. Such circumstances may lead to additional charges to cover additional time required to complete the testing.
- CPOC to inform business owners of systems to be tested, and to ensure their permission has been granted, before the engagement commences.
- All activities conducted during this engagement will take place during dates to be agreed between Intellectual Property Office and GDS. Lead time for projects will be a minimum of 14 days unless otherwise agreed by both parties in writing.
- All sensitive project data between GDS and CPOC will be encrypted and marked OFFICIAL:SENSITIVE and handled accordingly.
- All test plans, methodologies, raw data, results and project reports associated with the engagement will not be disclosed to any 3rd parties without the prior written consent of both GDS and the Intellectual Property Office.
- High-risk issues that pose an immediate security threat to the hosts or applications under review will be communicated to the CPOC immediately by GDS.
- The CPOC will ensure that all the Intellectual Property Office stakeholders are informed with regard to any production testing occurring, understand all risks associated with such testing, and have provided explicit permission for the testing to be performed by GDS in writing.
- The CPOC will ensure, if appropriate, that application stakeholders, SOC / CERT, and incident response teams are advised of any Security Assessment of systems that is taking place.
- The CPOC will ensure that a Intellectual Property Office technical point-of-contact is made available during the testing window who is responsible for issues/incidents with systems or the network, and accounts for the applications to be tested – in addition to general assistance with the environment. GDS will assist with troubleshooting issues with the test environment at the discretion of the CPOC, however this time is fully billable and may impact the final assessment report.
- The CPOC will ensure assessors are clearly informed, prior to assessment, of all critical systems, systems with known issues that may result in service availability issues, and systems that should be assessed at special times so as to minimise the business impact if a problem does occur.
- The CPOC will, at the discretion of the Intellectual Property Office teams, carry out a full back-up of the most critical systems, to protect against the unlikely event of an unintended system failure or disruption.

Cancellation & Delays

By signing this SOW Intellectual Property Office agrees to the following:

- If all or part of the test is to be cancelled or postponed once booked and confirmed, GDS requires at least 7 working days prior notice. Failure to do so will entitle GDS to invoice for the full amount of effort utilised and any cancellation charges incurred relating to travel/accommodation booked.
- After the project start date and/or commencement any project delays occurring due to Intellectual Property Office environments, test accounts, personnel or other required project resources not being available or useable will result in GDS billing project days as per normal.
- During the test, all work executed at the request of the Intellectual Property Office project team for GDS to perform on the testing environment or application/solution debugging, or readiness testing, will count as services performed under this SOW and be billed as per normal.

Other Matters

IN WITNESS WHEREOF, the parties hereto, each acting with proper authority, have executed this Statement of Work as of the date first written above.

Intellectual Property Office		**Gotham Digital Science Ltd**	
By:		By:	
Name:		Name:	[redacted]
Title:		Title:	[redacted]
Date:		Date:	13 November 2015

Terms and Conditions

THIS SERVICES AGREEMENT is between Gotham Digital Science Ltd ("GDS") and Intellectual Property Office ("Client").

Services and Fees

GDS agrees to provide Client with the Services described in the above Statement of Work. Client agrees to pay GDS the fees and expenses calculated and payable in accordance with the terms of the Statement of Work.

Confidentiality

GDS understands that during the course of its work for Client, GDS will obtain confidential information from Client, and GDS agrees to maintain the confidentiality of such information (including all portions or copies thereof) in accordance with the obligation of confidence set out in the Confidentiality Agreement between GDS and the Client dated 3 January 2014. Client agrees to keep all information concerning GDS' business, procedures and methods in performing the Services confidential.

Intellectual Property

Upon payment of all sums due to GDS under this Agreement, GDS hereby grants Client a non-exclusive, worldwide licence to use the reports specified in the SOW (the "Reports"). The Reports are prepared on the basis that they are only to be used by Client and without limiting the foregoing, the content of the Reports are not to be relied upon by any third party.

Unless otherwise agreed to by the parties in writing, GDS and its licensors expressly reserve all copyright, intellectual property rights and any other rights of whatever nature in or to any of the software, testing programs, methodologies and all other materials used and/or provided to Client by GDS in the course of the Services.

Limitation of Liability

The total aggregate liability of GDS and its subcontractors to the Client under or in connection with this Agreement whether in contract, tort (including negligence) or otherwise shall be limited to the greater of the fees actually paid to GDS in respect of such Services or £[redacted]. In no event will either party hereto be liable to the other party, for any consequential, incidental, indirect, punitive or special damages or for loss of profits, loss of data, loss of business, loss of goodwill or loss of any benefit howsoever arising whether or not such loss or damage is foreseeable, foreseen or known. Nothing in this Agreement shall exclude or in any way limit GDS' liability for fraud, or for death or personal injury caused by its negligence, or any other liability to the extent such liability may not be excluded or limited as a matter of law.

Termination

This Agreement shall terminate upon completion of the Services, or upon thirty days written notice by either party. Notwithstanding the foregoing, either party may terminate this Agreement immediately upon written notice if the other party breaches any of its material obligations hereunder and such breach is not cured within 15 days following receipt of written notice thereof. Client shall pay for work in-progress, completed Services and expenses incurred by Client up to and including the effective date of termination.

Use of Names

Neither party shall use publicly the other party's name, trademark, service mark or logo without the prior written consent of such other party.

Warranties

GDS shall perform the Services with reasonable skill and care and in accordance with the standards applicable in the industry for similar services. Save as otherwise set out in this clause GDS expressly disclaims all representations warranties, conditions, terms and obligations implied by statute, common law, trade usage or otherwise warranties of any kind for its Services, whether express or implied, including, but not limited to any condition of satisfactory quality or fitness for a particular purpose.

Without limiting the foregoing, GDS makes no warranty that (i) the Services will meet the Client's requirements, (ii) the Services will be uninterrupted, timely, secure, or error-free, (iii) the results that may be obtained from the Services will be accurate or reliable, and (iv) any errors in any software or otherwise will be corrected.

Testing

Client hereby consents to GDS performing the Services at the agreed times and in the manner reasonably determined by GDS. Client shall obtain all necessary consents and authorisations of any third parties that own or control any systems accessed by GDS in the course of the Services and/or that may be affected by the Services. GDS is entitled to presume that written consents from any third parties have been obtained by Client unless otherwise informed by Client.

Client acknowledges that the Services may result in disruptions of and/or damage to the Client's or third party's information systems and the information and data contained therein. Client shall indemnify and keep GDS indemnified from and against all liabilities, losses, damages, costs and expenses (including, without limitation, legal fees) suffered or incurred by GDS related to or arising out of any claim pending or threatened, of any kind (whether based in contract, tort or otherwise) by third parties related to or arising out of the Services.

Miscellaneous

This Agreement shall be governed by the law of England and Wales and the courts of England and Wales will have exclusive jurisdiction over all disputes arising from or in connection with this Agreement.

The parties acknowledge and agree that GDS is solely an independent contractor, is not an employee of Client and neither party has authority to bind the other as its agent.

Client shall bring any claim relating to the Services or this Agreement no later than two years after the completion of the Services or the earlier termination of this Agreement.

Estimated project dates set forth in the Statement of Work are not intended to represent project deadlines. The failure of GDS to complete any project phase by the estimated dates included in the Statement of Work is not a breach of this agreement.

No provision in this Agreement shall be enforceable by a person who is not a party to this Agreement. This Agreement and the SOW contain all the terms agreed between the parties regarding its subject

matter and supersede any prior agreement, understanding or arrangement between the parties, whether oral or in writing.

Each of the parties acknowledges and agrees that in entering into this Agreement it has not relied on, and shall have no remedy in respect of, any statement, representation, warranty or understanding other than the statements, representations, warranties and understandings expressly set out in this Agreement and its only remedies in connection with any statements, representations, warranties and understandings expressly set out in this Agreement shall be for breach of contract as provided in this Agreement.

GDS adheres to the Human Rights Act specifically Article 14 (Prohibition of discrimination) and Article 8 (right to respect for private and family life). This extends out to not only our employees, but to our clients in which we perform work. In addition, the UK Data Protection Act 1998 expressly requires that personal data shall only be obtained and processed fairly and lawfully. This requires that a minimum level of protection is used.

Changes in Scope

Any changes to the scope of the Services and the fees associated with such change must be agreed to in writing in advance by both parties (a "Change Order").

Any other information - that you wish to add further to that already requested, that you feel may further demonstrate your ability.