Service Agreement for

Enterprise Network Security Assessment

Presented by Insight Public Sector, Inc.

Insight Public Sector, Inc. Contact:
Insight Public Sector, Inc. Contact Name
Insight Public Sector, Inc. Contact Title
Insight Public Sector, Inc. Contact Email
Insight Public Sector, Inc. Contact Phone

Customer Name Contact:
Customer Contact Name
Customer Contact Title
Customer Contact Email
Customer Contact Phone

Services to be delivered Remotely to address:
Service Delivery Street Address
Service Delivery City, State, Zip
STANDARD TERMS AND CONDITIONS

Insight Public Sector, Inc. shall perform in accordance with this Service Agreement effective on the date agreed upon by and between Insight Public Sector, Inc. ("Provider") whose principal office is located at 6820 South Harl Avenue, Tempe, Arizona 85283 and CUSTOMER NAME, with its principal office located at CUSTOMER BUSINESS ADDRESS ("Customer").

When mutually signed (executed), this Service Agreement becomes contractually binding on Provider and Customerin accordance with DIR-TSO-4173. In the event of a conflict of terms between this Section D and Contract No. DIR-TSO-4173, the latter terms will take precedence.

Any information, whether protected by patent or copyright, including, but not limited to, programs, files, specifications, plans, business information, technical information, or other data either written or otherwise (hereinafter "Information"), which has been furnished or disclosed by Customer to Provider (or Provider delivery partners), or by Provider to Customer, its employees, or agents shall remain property of the originating party and shall be considered proprietary Information by the receiving party, its employees, or agents. Information shall not be reproduced, published, or disclosed to any third party (except as noted Provider delivery partners) without prior consent of the originating party. All copies of any and all Information furnished or disclosed (except for 'Deliverables' listed by this Service Agreement) shall be returned to the originating party immediately upon written notice.

Indemnification shall be handled in accordance with DIR-TSO-4173 and Appendix A, Standard Terms and Conditions, Item 10.A

Liability shall be handled in accordance with DIR-TSO-4173 and Appendix A, Standard Terms and Conditions, Item 10.K

Termination shall be in accordance with DIR-TSO-4173 and Appendix A, Standard Terms and Conditions, item 11.B

DEFINITIONS

Deliverable: For the purposes of this Service Agreement, the term ‘deliverable’ refers to one specific work product that is the outcome of the engagement. Collectively, deliverables are the product for which the price of this Service Agreement is exchanged. Services or activities (work) will be performed as a part of this Service Agreement in order to produce the deliverables (work product).

Documentation: The terms ‘document’ and ‘documentation’ as they relate to this Service Agreement are intended to mean any notes, charts, graphs, diagrams, report outputs, network addresses, passwords, configuration logs, or any other discretionary information deemed by Provider to be relevant to this effort. Documentation is not intended to be, or considered to be, complete, comprehensive, or exhaustive as it relates to the overall customer network or information systems environment. Any documentation provided as a part of the execution of this Service Agreement will be limited to systems, items, or topics specifically referenced in this Service Agreement.

Knowledge Transfer: The term ‘knowledge transfer’, as it relates to this Service Agreement, is intended to mean conversational discussions about various technical aspects of this effort. Knowledge transfer is not intended to be, expected to be, or considered to be complete, comprehensive, or exhaustive as it relates to the overall customer network or information systems environment. Additionally, knowledge transfer is not intended to replace the need for formal instruction or vendor-supplied training in the operation of any systems installed or configured as part of this Service Agreement.

Training: Unless otherwise specifically stated in this Service Agreement, Provider supplied training is not intended to convey any formal certification or credential and is provided on a ‘best effort’ basis as a courtesy to the customer.

IN SCOPE: The work described in the Activities section of this document, and effort toward the fulfillment and delivery of items described in the Deliverables section of this document are considered to be ‘IN SCOPE’ as they relate to this effort. The contents of the Assumptions sections of this document provide specific clarification of the scope.

OUT OF SCOPE: Any items, components, materials, efforts, objectives, tasks, or services not described in either the Activities or Deliverables section of this document are considered ‘OUT OF SCOPE’ as they relate to this effort. OUT OF SCOPE work will not be performed without written authorization by the customer via the project change control process described herein.

Testing, Validation, Verification: The terms ‘testing’, ‘validation’ and ‘verification’ refer to the process of comparing measurements and observations of specific information systems to customer provided expectations or criteria. The customer is responsible to confirm that tests, validation, or verification is successful.
1 INTRODUCTION OF SERVICE

Recognizing the heavy reliance business environments have on information technology, a network security assessment is a vital component of maintaining a healthy, safe and secure network. Provider’s Enterprise Network Security Assessment is a foundational component to the Customer’s ongoing risk management program.

Provider delivers the most fundamental evaluation of the security state and associated risk posture of the network. The assessment’s prime purpose is to test Customer’s systems and networks for common security weaknesses, assess their risk posture, and verify the adequacy of these systems to protect from data breaches using the same methods as the criminal hackers.

1.1 Assessment Focal Points

1.1.1 Vulnerability Assessment and Penetration Testing
Vulnerabilities in external and internal infrastructure hosts are identified, quantified, and prioritized. Identified weakness are validated through controlled attacks on the system or network.

The external assessment will be conducted in a black box mode while the internal assessment will be conducted using credentialed (white box) scans. Our assessment methodology is based on a combination of NIST standard and open source framework OSSTMM methodology.

The assessment targets externally available hosts and firewalls and internal networked hosts including firewalls, switches, routers, servers, workstations, etc.

We will be conducting penetration test on the external facing firewalls and hosts to validate the vulnerabilities identified. Activities include:

- Conduct network discovery to confirm active and responding hosts.
- Probe for open ports and identify listening services.
- Scan open ports for known vulnerabilities.
- Conduct penetration testing attacks on external assets to exploit vulnerabilities identified in the prior activities.
- Analyze data to assess risk and document results according to prioritized risk model.
- Recommend possible remediation activities for risks identified.

Activities for internally facing-hosts will include:

- Network discovery and scanning of all internal subnets for active hosts.
- Probe for open ports and identify listening services.
- Scan open ports for known vulnerabilities using approved vulnerability scanner.
- Analyze data to assess risk and document results according to prioritized risk model.
- Recommend possible remediation activities for risks identified.

1.1.2 Web Application Security Testing.
Publicly facing websites hosted internally by the customer are assessed for weaknesses.

Web application security testing is the process of testing, analyzing and reporting on the security level and/or posture of a Web application. It is a systematic process that starts from identifying and scoping the entire application, followed by planning multiple tests.

The Web application undergoes a rigorous testing process that includes a series of fabricated malicious attacks to see how well the Web application performs/responds. The overall security testing process is
generally followed by a format report that includes the identified vulnerabilities, possible threats and recommendations for overcoming the security shortfalls. Some of the processes within the testing process include:

- Brute force attack testing
- Password quality rules
- Session cookies
- User authorization processes
- SQL injection

1.1.3 Active Directory Security Assessment.

The existing Microsoft Active Directory environment is assessed for weaknesses and includes:

- User and Computer Object Audit
- Security Policy Assessment
- Share Permission
- User Permissions
- User Behavior Analysis.
- Login Failures by Computer.
- Login History by Computer.

1.2 Completion of Assessment

Once Assessments are completed, the data collected is analyzed by Provider’s security engineers and the necessary reports compiled on the state of the systems and network. The assessment results, documented vulnerabilities, and prioritized remediation recommendations are presented and shared with Customer’s stakeholders in a secure manner at the end of the engagement.

1.3 Assessment Methodology

The assessment methodology, depending on the Customer’s needs, follows the standards Ethical Hacking methodology including four phases.

1.3.1 Reconnaissance Phase

In this phase, Provider gathers external network structure information. This phase identifies the client’s resources that may facilitate an attack vector or foothold in the client’s network. Assessment elements identified include:

- Organization information such as defined by ARIN.
- External resource name information. An example is attempting to perform DNS zone transfers, detailing Internet facing servers and the like.
- Examining the client’s web pages for clues such as other web pages, other network domains…etc.
1.3.2 Network and Resource Mapping
Provider will take the information gathered in the reconnaissance phase and use that to map the client's network. This phase takes information gathered (IP address, services) and gathers additional information such as what version of the operating system (Windows 7, Vista...etc.) and version of any given device (Microsoft IIS version 6, Apache...etc.). Elements of the mapping activity include:

- Network Server and Appliances – Firewalls, DNS servers, web servers, VPNs, and other devices are identified.
- Port Scanning – This determines which TCP/UDP ports are open and what may be used as a vector into the client's network.
- Banner Grabbing – This task attempts to capture information from common services (i.e. using telnet to grab the banner information on a target's website)
- Wireless Mapping – This element detects SSIDs, encryption keys, and wireless end stations. Also, rogue access points, and "war driving" are covered in this process.

1.3.3 Vulnerability Scanning
The identified appliances / services will be used to attempt to exploit weaknesses in the client's infrastructure. Building upon what was mapped, Provider attempts to exploit identified vulnerabilities. Examples include:

- SNMP Scanning – Captures both the physical and logic construct of the device.
- Operating System Scanning – Identifies the target's operating system in order to tailor applicable and specific attacks for that platform.
  1. Windows XP
  2. Windows 7
  3. Linux Red Hat
  4. Apple OS X
  6. Window's Active Directory - The Windows AD environment is a key component of this assessment since it controls the entire enterprise’s communications and authentication infrastructure. The key elements are:
    - DHCP
    - DNS
    - Tree / Forrest evaluation
    - Business Unit structure
    - Others
• Application Scanning – Examines the running services found on that device including:
  1. Windows Internet Information Services (web server).
  2. Apache web server.
  3. PHP scripting.
  4. P’s OpenView management application.
  5. Broken SSL vulnerabilities.

• Host Evaluation – This service looks at the device and compares it to established standards using such scoring tools as:
  1. CIS.
  2. NSA Hardening Guides.
  3. SCAP (OVAL Interpreter).
  4. NIST Configuration References.

• Network Device Scanning – This step examines hardware appliances on a client’s network. Such devices are:
  5. LinkProof Load Balancers.
  6. Cisco ASA or Checkpoint (Nokia) firewalls.
  8. Web Sense or Cisco ESA/WSA content security appliances.

1.3.4 Reporting
With the data gathered in the previous phases, a report is created that details the following:

• Executive Summary – high-level overview of the process.
• Network resources that were discovered, what services they offered, platform (OS), vulnerabilities discovered and exploited.
• Remediation – Based on the vulnerabilities, suggest what actions are to be taken to either mitigate or reduce the risk posed by the vulnerabilities discovered.
• Other – This task performs additional actions that the client expressed. An example would be a numerical weighted average noting a score of how the client did. Using the NSA’s IEM protocol, a value between one (least vulnerable) and ten (most vulnerable).

1.4 Assessment Tools
A variety of tools may be deployed through the various assessment phases. The customer’s needs, business operating requirements, and security constraints combine with Provider’s expertise and assessment objective drive the selection of tools. Upon disclosure, other tools may be used to gather information.

Reconnaissance Phase

WHOIS – Gathers organizational data such as:
Company Name, Mailing address, Technical and administrative contact information, Domain expiration of the domain, and Name servers.

Xprobe – Scans any given device (like NMAP, but offers other information.

DNSenum – Gather DNS information where DNS zone transfers are prohibited.

Maltego – Name, telephone, website spidering, etc.

DNSwalk – Additional name information.
NSLOOKUP – Gathers network resource information such as: Name to IP address mapping (A record); Mail IP address mapping (MX record); Name alias (CNAME record).

NMAP – Gathers in depth information for a given resource. Examples are:
- Resources appearing on detected subnet.
- Network topology.
- Operating system the device uses.
- Services the device supports (web, SNMP, SMB, DNS...etc.).
- System banners, Malware detection.

**Network and Resource Mapping**

NMAP – (See preceding section).

SNMPWalk – Details what SNMP services the device offers: Version of the operating system; Physical device construct (NICs, disk drives, displays connected); Monitor / Management (SNMP get vs. SNMP put).

Firewalk – Similar to SNMPWalk but yields additional information.

Cisco-auditing-tool – examines Cisco devices and details what services they perform.

Cisco-router-config – attempts to capture device configuration data.

Ftester – Examines IPS, Firewall rule set discovery.

SMTP-User-name – Gathers email addressing and other information.

**Vulnerability Scanning**

NexPose – Commercial Vulnerability assessment tool.

Metasploit – Network attack framework.

Nessus – Device Mapping and service exploiter.

OpenVAS – Like Nessus in nature, but gathers additional information and offers other attack tools.

Cisco Global Exploiter – Attacks Cisco routers and switches.

PING – Can execute “ping of death” attacks.

Perl – Perl is a programmable language but supports custom scripts that can be used for attacking or using covert channels into an “owned” device.

Fast Track – An attack platform that supports reporting and an attack log.

IWAR – Telephony (PBX) information.

LANMAP2 – Discovers NETBIOS information including: NetBios names, Fileshare information, Printing information.

HPING3 – Gathers host service information similar to NMAP but yields additional information.

SIPSCAN – Gathers Voice over IP (VOIP) information.

IKE-SCAN – Gathers VPN server data.

SSLDUMP – Gathers SSL data such as certificates, encryption...etc.

SQLScan – Captures SQL information (MS SQL, Oracle).

MYSQL – Captures SQL information (like SQLScan but yields additional information).

VOIPer – An attack platform that attempts VOIP and SIP exploits.

W3AF – An attack framework for auditing a website and web servers. Offers several modes for compliance or ad hoc testing.

DarkmySQL – SQL attack tool.

Burp Suite – An attack tool suite.

Nikto – Web vulnerability analysis tool.

SQLMap – Similar to DarkmySQL but offers other attack features.

SQLninja – Similar to DarkmySQL and SQLMap, but offers additional functionality.

Social Engineering Tool Kit (SET) – Tests “behind the keyboard” attacks such as link clicking and password harvesting tools.

WebScarab – Web site testing tool suite.
ZAP Proxy – Website analysis tool.

Paros Proxy – Website analysis tool.
2 SCOPE OF WORK

The following sections define the scope of this work effort. Only the items detailed here will be considered in scope to this project. Any other tasks, activities, services, or work products which may be requested by Customer throughout this engagement will be considered out of scope and may require additional costs or fees, changes of project schedule, or a project change order.

2.1 Activities

Provider has identified the following activities which will be performed as a part of this engagement:

1) Specify assessment environment (including internal and external assets and associated networking infrastructure, web applications) through collaborative chartering session.
2) Configure and ship internal assessment tool host.
3) Conduct external vulnerability assessment and penetration testing.
   a) Confirm active and responding hosts through network discovery.
   b) Identify open ports and listening services.
   c) Scan open ports for known vulnerabilities.
   d) Conduct penetration testing attacks to exploit vulnerabilities on confirmed external assets.
4) Conduct web application security testing.
   a) Identify and scope web applications for security test.
   b) Conduct security testing on identified web applications.
5) Conduct internal vulnerability assessment and penetration testing.
   a) Confirm active hosts through network discovery and scanning of all internal subnets.
   b) Identify open ports and listening services.
   c) Scan open ports for known vulnerabilities.
   d) Conduct penetration testing attacks to exploit vulnerabilities on confirmed external assets.
6) Conduct Active Directory security assessment.
7) Analyze and assess vulnerabilities.
8) Develop remediation strategies for prioritized vulnerabilities.
9) Document assessment results according to prioritized risk model.
10) Purge customer-specific data from assessment systems.
11) Present assessment results and recommended remediation strategies.

2.2 Deliverables

The following items will be delivered to Customer and shall constitute the work product of this engagement.

1) Collaborative planning session
2) Executive Summary
3) Detailed Security Report on External and Internal Threats with the following data;
   a) Overview of the process.
   b) High Level findings.
   c) Organizational INFOSEC Posture
   d) Findings by severity (high, medium, low).
   e) Severity by System.
f) Detailed system vulnerability analysis.
g) Remediation Roadmap.
h) Detailed (Raw) tool output.
i) Assessor’s notes.
j) CVE, OSVDB, OVAL, and other vulnerability references.
k) Relevant Best Practice Documentation

4) Active Directory Assessment Reports
   a) Security Risk Report. This executive-level report includes a proprietary Security Risk Score along with summary charts, graphs and an explanation of the risks found in the security scans.
   b) Security Policy Assessment Report. A detailed review of the security policies that are in place on both a domain wide and local machine basis.
   c) Shared Permission Report. Comprehensive lists of all network “shares” by computer, detailing which users and groups have access to which devices and files, and what level of access they have.
   d) User Permissions Report. Organizes permissions by user, showing all shared computers and files to which they have access.

5) Internal Vulnerabilities Report. Highlights deviation from industry standards compared to outbound port and protocol accessibility, lists available wireless networks as part of a wireless security survey, and provides information on Internet content accessibility.

6) Vulnerabilities Full Detail Report. A comprehensive output including security holes, warnings, and informational items that can help you make better network security decisions, plus a full Scan which checks all 65,535 ports and reports which are open. This is an essential item for many standard security compliance reports.

7) Proposed Remediation Plan

8) Presentation of Documented Assessment and Recommendations

2.3 Assumptions

Provider has identified the following assumptions which are relevant to the scope of this work effort:

1) Vulnerability assessment and penetration testing is limited to 30 public IP addresses and 500 internal network hosts.
2) Web application security testing is limited to no more than 15 websites.
3) Customer will provide temporary domain administrator account for internal vulnerability and Active Directory assessments.
4) Customer will physically receive and add to their network a Provider-owned laptop to be used as the source for internal assessments.
5) Internal assessments will only be initiated from a single location; site-to-site connectivity for multi-site environments is assumed to be present and accessible.
6) All work related to this engagement will be performed remotely during normal business hours (Monday through Friday 8 a.m. – 6 p.m. customer local time) and occasionally outside normal business hours between 7pm – midnight.
7) All documentation will be provided in Microsoft Word™, Microsoft Excel™, Microsoft Visio™, or Adobe PDF™ electronic file formats at Provider discretion or in any format otherwise agreed to by Provider and Customer.
8) Customer will provide reasonable access (including remote access) to all facilities and equipment as needed to perform the engagement and accomplish the stated objectives.
9) Customer is to provide complete and accurate documentation of Customer systems and policies as requested throughout the engagement, so long as such requests comply with Customer’s stated security policies.

10) Customer is fully responsible to maintain any and all needed backups of company information, data, and system states throughout the entire engagement. Provider will make every effort to avoid the possibility of data loss, but Provider is not responsible for any data loss that may occur during this engagement.

11) Customer will advise of all relevant security and operational policies impacting Provider’s access to the environment and requisition of such access.

12) Provider will request information or systems access in a reasonably timely fashion, so as not to cause project delays or missed deadlines.

13) Provider will request information or systems access in a way that complies with stated Customer security and operational policies.

14) Provider will provide a project timeline (upon request) and reasonable justification for any missed deadlines or project delays.

15) Provider will provide responses to any reasonable inquiries regarding project status and progress (upon request) throughout the engagement.

2.4 Risks:

Provider has identified the following risks associated with the scope of this work effort:

1) Failures and delays in providing network configurations, diagrams, credentials, or site information could alter the timeline of the project.

2) The only change within the environment involves the implementation of a host system for the assessment tools; to mitigate the risk of data loss associated with any production change, Provider recommends Customer maintain necessary data and system state backups throughout the engagement.

3) Discovery data is accurate at the time of data collection; any changes to the overall environment after survey completion can negatively impact assessment accuracy.

4) Application of assessment results from this scope toward any security requirements not defined within this scope will fail to qualify as an assessment for those security requirements.

2.5 Scope Exclusions

Provider has identified the following items which will be specifically excluded from the scope of this engagement:

1) Compliance with specific security requirements from Customer or any 3rd party (including vendors, government, and industry organizations) is specialized and not a standard for this scope of work.

2) Vulnerability assessment and penetration testing will not be performed for more than 30 public IP addresses nor more than 500 internal network hosts.

3) Web application security testing will not be performed for more than 15 websites.

4) Assessments on internal infrastructure will only be launched from a single physical location; other sites not accessible through site-to-site connectivity from source location will be excluded from assessment of internal components.

5) Provider will provide no configuration services for server, network, or end-user infrastructure.
3 SCHEDULE

Provider will work with Customer upon execution of this Service Agreement to determine a project start date based on mutual availability of resources and scheduling constraints.

4 PRICE

The services and deliverables outlined in this Service Agreement will be provided for a fixed price detailed below. If additional out of scope activities are required during the engagement, authorization for those activities and associated costs will be managed through a separate Service Agreement or through the project change control process. The fixed price will not be exceeded without formal change approval.

4.1 Pricing Detail

<table>
<thead>
<tr>
<th>Service</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Network Security Assessment (less than 500 hosts)</td>
<td></td>
</tr>
</tbody>
</table>

4.2 Billing Terms

The total amount for this engagement will be billed in full upon project completion, and in accordance with DIR-TSO-4173 and Appendix A, Standard Terms and Conditions, Item 8, Pricing, Purchase Orders, Invoices, and Payments.

4.3 Project Completion

This project will be considered complete when all expected deliverables have been received by Customer, as acknowledged and agreed to by the parties through a Project Completion form, in accordance with the procedures set forth in this paragraph. At the completion of the project, Provider will provide the Customer with a Project Completion form. Customer will have 7 calendar days from the date of receipt of the Project Completion form either (i) to accept it by signing and returning it to Provider, or (ii) to articulate its objections in writing to Provider If Customer does not timely provide Provider with written acceptance or objection(s) within such 7 calendar day period, Customer will be deemed to have accepted the project and all associated deliverables without any further action by either party.
5 ACCEPTANCE

I, the undersigned, have read and agree to the terms of this Service Agreement titled ‘“Service Agreement for Enterprise Network Security Assessment’. I am an authorized representative of my organization, and I agree that once mutually signed all pages of this Service Agreement will have full force and effect for execution by all parties. Customer authorizes Provider to perform the services detailed herein, and agrees to the fee schedule also defined herein. Provider agrees to perform the activities and provide the deliverables defined herein. Upon completion of services and Customer acceptance, Customer authorizes Provider to invoice for services performed under this Service Agreement. Customer agrees to pay Provider by the due date set forth in the Provider invoice (including all applicable taxes).

[CUSTOMER NAME]  

Insight Public Sector, Inc.

Authorized Signature  

Authorized Signature

(Above name printed)  

(Above name printed)

Title (printed)  

Title (printed)

Date  

Date

Please initial one option to indicate Purchase Order requirement:

- Purchase Order #
- Hard copy Purchase Order attached
- Initial

At the discretion of Provider, this Service Agreement may be subject to change in pricing and/or terms if not signed and returned within 60 days of receipt.

Insight Public Sector, Inc. internal use only:

Sales AE Name  
Rep ID Number  
MACS Customer No.  
Corp Division No.
**ADDENDUM A: PROJECT COMPLETION FORM**

This document serves to confirm that the Enterprise Network Security Assessment project has been completed and all of its deliverables have been met per the Service Agreement for Enterprise Network Security Assessment.

<table>
<thead>
<tr>
<th>1. Project Name: Enterprise Network Security Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Customer:</td>
</tr>
<tr>
<td>CUSTOMER NAME</td>
</tr>
<tr>
<td>CUSTOMER BUSINESS STREET ADDRESS</td>
</tr>
<tr>
<td>CUSTOMER BUSINESS CITY, STATE, ZIP</td>
</tr>
<tr>
<td>CUSTOMER CONTACT NAME</td>
</tr>
<tr>
<td>CUSTOMER CONTACT TITLE</td>
</tr>
<tr>
<td>CUSTOMER CONTACT EMAIL</td>
</tr>
<tr>
<td>CUSTOMER CONTACT PHONE</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. Project Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Phase(s) to be Billed:</td>
</tr>
</tbody>
</table>

5. Summary of Deliverables:

- [ ] First Deliverable
- [ ] Second Deliverable
- [ ] Third Deliverable
- [ ] Additional Deliverables...

6. Acceptance:

**Project Completion Declaration:** The Customer has received and reviewed all expected deliverables of the project, accepts all the services provided, and considers the terms of the Service Agreement fulfilled. Customer authorizes Insight Public Sector, Inc. to invoice any outstanding balance for services rendered.

**CUSTOMER NAME**

---

Authorized Signature

(Above name printed)

Title (printed)

Date