



**PURCHASING ITEM
FOR
COUNCIL AGENDA**

1. Agenda Item Number:

5

2. Council Meeting Date:

July 11, 2013

TO: MAYOR & COUNCIL

3. Date Prepared: June 25, 2013

THROUGH: CITY MANAGER

4. Requesting Department: City Manager

5. SUBJECT: Award Agreement #IT3-918-3172 for Network Security Audit Services

6. RECOMMENDATION: Recommend awarding Agreement #IT3-918-3172 for Network Security Audit Services to Terra Verde Services in an amount not to exceed \$35,000.

7. HISTORICAL BACKGROUND/DISCUSSION: A routine security audit is necessary to ensure that citizen data is adequately protected. The audit will also identify any risks to City computer systems that could impair city services. Funding for this audit was identified in the FY12/13 budget. This audit will check security documents and processes along with the network infrastructure to identify if there are any risks to the City's various systems. Any risks identified will be prioritized by the severity of the issue. IT will then develop a strategy to mitigate those risks, which may include the need for additional professional services. If additional services are needed, they will be competitively procured as a separate process utilizing funds identified in the FY13/14 budget. The last audit was performed over 5 years ago.

8. EVALUATION PROCESS: Staff issued a Request for Qualifications and Experience (RFQE) in September 2012. The RFQE was advertised and all registered vendors capable of providing network security auditing services were notified. Sixteen (16) responses were received. An evaluation committee reviewed all responses and narrowed them down to the three (3) highest scoring responses. Those three vendors were then interviewed and the committee determined that Terra Verde Services was the most experienced and the best qualified to audit the City's network security policies and procedures. The City entered into negotiations with Terra Verde Services and staff is recommending the award to Terra Verde Services based on their qualifications and experience.

9. FINANCIAL IMPLICATIONS: Funds are available from the following account: 101.1280.5219.0.0.0 General Funds, Information Tech Infrastructure, and Consultant Services.

10. PROPOSED MOTION: Approve awarding Agreement #IT3-918-3172 for Network Security Audit Services to Terra Verde Services in an amount not to exceed \$35,000.

APPROVALS

11. Requesting Department

Patrick Hait, IT Infrastructure Manager

12. Department Head

Steven Philbrick, Chief Information Officer

13. Procurement Officer

Carolee Stees, CPPB

14. City Manager

Rich Dlugas

**CITY OF CHANDLER
PROFESSIONAL SERVICES AGREEMENT**

Project No. IT3-918-3172

Project Name: IT Network Security Audit

THIS AGREEMENT is made and entered into this 29 day of June, 2013, by and between the City of Chandler, a Municipal Corporation of the State of Arizona, hereinafter referred to as "CITY", and TERRA VERDE SERVICES, hereinafter referred to as "CONSULTANT".

WHEREAS, the Mayor and City Council of the City of Chandler is authorized and empowered by provisions of the City Charter to execute contracts for professional services; and

WHEREAS, CONSULTANT represents that CONSULTANT has the expertise and is qualified to perform the services described in the Agreement.

NOW THEREFORE, in consideration of the mutual promises and obligations set forth herein, the parties hereto agree as follows:

1. CONTRACT ADMINISTRATOR:

1.1. To provide the professional services required by this Agreement CONSULTANT shall act under the authority and approval of the IT Project Manager or designee, (the Contract Administrator), who shall oversee the execution of this Agreement, assist the CONSULTANT with any necessary information, audit billings, and approve payments. The CONSULTANT shall channel reports and special requests through the Contract Administrator.

1.2. CITY reserves the right to review and approve any/all changes to CONSULTANT'S key staff assigned to the CITY project by the firm during the term of this Agreement.

2. **SCOPE OF WORK:** CONSULTANT shall provide those services described in Exhibit B attached hereto and made a part hereof by reference.

3. **ACCEPTANCE AND DOCUMENTATION:** Each task shall be reviewed and approved by CITY to determine acceptable completion. All documents, including but not limited to, data compilations, studies, and reports which are prepared in the performance of this Agreement, shall be and remain the property of CITY and shall be delivered to CITY before final payment is made to CONSULTANT.

4. **FEE SCHEDULE:** For the services described in paragraph 2 of this Agreement, CITY shall pay CONSULTANT a fee not to exceed the sum of Thirty-five Thousand dollars (\$35,000) in accordance with the fee schedule attached hereto as Exhibit C and incorporated herein by reference.

5. **TERM:** Following execution of this Agreement, CONSULTANT shall commence work on July 22, 2013 and shall complete all services described herein within thirty-five (35) non-contiguous business days, not to exceed ninety (90) calendar days from the start of the project.

6. **COOPERATIVE USE OF CONTRACT.** In addition to the City of Chandler and with approval of the CONSULTANT, this Contract may be extended for use by other

municipalities, school districts and government agencies of the State. A current listing of eligible entities may be found at www.maricopa.gov/materials and then click on 'Contracts', 'S.A.V.E.' listing and 'ICPA'. Any such usage by other entities must be in accordance with the ordinance, charter and/or procurement rules and regulations of the respective political entity.

If required to provide services on a school district property at least five (5) times during a month, CONSULTANT shall submit a full set of fingerprints to the school district in accordance with A.R.S. 15-512 of each person or employee who may provide such service. The District shall conduct a fingerprint check in accordance with A.R.S. 41-1750 and Public Law 92-544 of all CONSULTANTS, sub-CONTRACTORS or vendors and their employees for which fingerprints are submitted to the District. Additionally, the CONSULTANT shall comply with the governing body fingerprinting policies of each individual school district/public entity. CONSULTANT, sub-contractors, vendors and their employees shall not provide services on school district properties until authorized by the District.

Orders placed by other agencies and payment thereof will be the sole responsibility of that agency. The CITY shall not be responsible for any disputes arising out of transactions made by other agencies who utilize this Agreement.

7. TERMINATION:

7.1. Termination for Convenience: CITY reserves the right to terminate this Contract or any part thereof for its sole convenience with thirty (30) days written notice. In the event of such termination, CONSULTANT shall immediately stop all work hereunder, and shall immediately cause any of its suppliers and subcontractors to cease such work. As compensation in full for services performed to the date of such termination, the CONSULTANT shall receive a fee for the percentage of services actually performed. This fee shall be in the amount to be mutually agreed upon by the CONSULTANT and CITY, based on the agreed Scope of Work. If there is no mutual agreement, the Management Services Director shall determine the percentage of work performed for each task detailed in the Scope of Work and the CONSULTANT's compensation shall be based upon such determination and CONSULTANT's fee scheduled included herein.

7.2 Termination for Cause: City may terminate this Contract for Cause upon the occurrence of any one or more of the following events:

- 1) If CONSULTANT fails to perform pursuant to the terms of this Agreement
- 2) If CONSULTANT is adjudged a bankrupt or insolvent;
- 3) If CONSULTANT makes a general assignment for the benefit of creditors;
- 4) If a trustee or receiver is appointed for CONSULTANT or for any of CONSULTANT'S property;
- 5) If CONSULTANT files a petition to take advantage of any debtor's act, or to reorganize under the bankruptcy or similar laws;
- 6) If CONSULTANT disregards laws, ordinances, rules, regulations or orders of any public body having jurisdiction;
- 7) Where Agreement has been so terminated by CITY, the termination shall not affect any rights of CITY against CONSULTANT then existing or which may thereafter accrue.

- 7.3. Availability of Funds for the next Fiscal Year.** Funds may not presently be available under this agreement beyond the current fiscal year. No legal liability on the part of the CITY for services may arise under this agreement beyond the current fiscal year until funds are made available for performance of this agreement. The CITY may reduce services or terminate this agreement without further recourse, obligation, or penalty in the event that insufficient funds are appropriated. The City Manager shall have the sole and unfettered discretion in determining the availability of funds.
- 8. INSURANCE REQUIREMENTS:** CONSULTANT shall provide and maintain the insurance as listed in Exhibit D attached hereto and made a part hereof by reference.
- 9. ENTIRE AGREEMENT:** This Agreement constitutes the entire understanding of the parties and supersedes all previous representations, written or oral, with respect to the services specified herein. This Agreement may not be modified or amended except by a written document, signed by authorized representatives or each party.
- 10. ARIZONA LAW:** This Agreement shall be governed and interpreted according to the laws of the State of Arizona.
- 10.1.** Pursuant to the provisions of A.R.S. § 41-4401, the Consultant hereby warrants to the City that the Consultant and each of its subcontractors ("Subcontractors") will comply with all Federal Immigration laws and regulations that relate to the immigration status of their employees and the requirement to use E-Verify set forth in A.R.S. §23-214(A) (hereinafter "Consultant Immigration Warranty").
- 10.2.** A breach of the Consultant Immigration Warranty (Exhibit A) shall constitute a material breach of this Contract that is subject to penalties up to and including termination of the contract.
- 10.3.** The City retains the legal right to inspect the papers of any Consultant or Subcontractor employee who works on this Contract to ensure that the Consultant or Subcontractor is complying with the Consultant Immigration Warranty. The Consultant agrees to assist the City in the conduct of any such inspections.
- 10.4.** The City may, at its sole discretion, conduct random verifications of the employment records of the Consultant and any Subcontractors to ensure compliance with Consultants Immigration Warranty. The Consultant agrees to assist the City in performing any such random verification.
- 10.5.** The provisions of this Article must be included in any contract the Consultant enters into with any and all of its subcontractors who provide services under this Contract or any subcontract. "Services" are defined as furnishing labor, time or effort in the State of Arizona by a Consultant or subcontractor. Services include construction or maintenance of any structure, building or transportation facility or improvement to real property.
- 10.6.** In accordance with A.R.S. §35-393.06, the Consultant hereby certifies that the offeror does not have scrutinized business operations in Iran.
- 10.7.** In accordance with A.R.S. §35-391.06 the Consultant hereby certifies that the offeror does not have scrutinized business operations in Sudan.
- 11. CONFLICT OF INTEREST:**
- 11.1. No Kickback.** CONSULTANT warrants that no person has been employed or retained to solicit or secure the Agreement upon an agreement or understanding for a

commission, percentage, brokerage or contingent fee; and that no member of the City Council or any employee of the CITY has any interest, financially or otherwise, in the firm unless this interest has been declared pursuant to the provisions of A.R.S. section 38-501. Any such interests were disclosed in CONSULTANT'S proposal to the CITY.

- 11.2. Kickback Termination.** CITY may cancel any contract or agreement, without penalty or obligation, if any person significantly involved in initiating, negotiating, securing, drafting or creating the agreement on behalf of the CITY is, at any time while the Agreement or any extension of the Agreement is in effect, an employee of any other party to the Agreement in any capacity or a CONSULTANT to any other party to the Agreement with respect to the subject matter of the Agreement. The cancellation shall be effective when written notice for CITY is received by all other parties, unless the notice specifies a later time (A.R.S. 38-511).
- 11.3. No Conflict.** CONSULTANT stipulates that its officers and employees do not now have a conflict of interest and it further agrees for itself, its officers and its employees that it will not contract for or accept employment for the performance of any work or services with any individual business, corporation or government unit that would create a conflict of interest in the performance of its obligations pursuant to this project.
- 11.4. Arizona Law.** This Agreement shall be governed and interpreted according to the laws of the State of Arizona.
- 11.5. Jurisdiction and Venue.** The parties agree that this Agreement is made in and shall be performed in Maricopa County. Any lawsuits between the Parties arising out of this Agreement shall be brought and concluded in the courts of Maricopa County in the State of Arizona, which shall have exclusive jurisdiction over such lawsuits.
- 11.6. Fees and Costs.** Except as otherwise agreed by the parties, the prevailing party in any adjudicated dispute relating to this Agreement is entitled to an award of reasonable attorney's fees, expert witness fees and costs including, as applicable, arbitrator fees; provided, however, that no award of attorney's fees shall exceed ten percent (10%) of the damages awarded the prevailing party unless the non-prevailing party has been determined to have acted in bad faith or in a frivolous manner during the adjudication.

12. **NOTICES:** All notices or demands required to be given pursuant to the terms of this Agreement shall be given to the other party in writing, delivered by hand or registered or certified mail, at the addresses set forth below, or to such other address as the parties may substitute by written notice given in the manner prescribed in this paragraph.

In the case of City:
City of Chandler
Purchasing Division
P.O. Box 4008, Mail Stop 901
Chandler, AZ 85244-4008
480.782. 2400

In the case of CONSULTANT:
Edward Vasko
Terra Verde Services
7400 E Pinnacle Peak Rd, Suite 100
Scottsdale, AZ 85255
480.840.1744

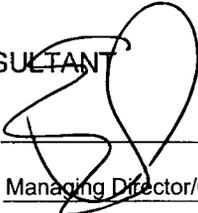
Notices shall be deemed received on date delivered, if delivered by hand, and on the delivery date indicated on receipt if delivered by certified or registered mail.

IN WITNESS WHEREOF, the parties have hereunto subscribed their names to this 29 day of June 2013.

CITY OF CHANDLER

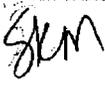
CONSULTANT

Mayor Date

By: 
Title: Managing Director/Co-Founder

APPROVE AS TO FORM

ATTEST: If Corporation

City Attorney 

Secretary

ATTEST:

City Clerk

SEAL

EXHIBIT A

**Consultant Immigration Warranty
To Be Completed by Consultant Prior to Execution of Contract**

A.R.S. § 41-4401 requires as a condition of your contract verification of compliance by the Consultant and subcontractors with the Federal Immigration and Nationality Act (FINA), all other Federal immigration laws and regulations, and A.R.S. § 23-214 related to the immigration status of its employees.

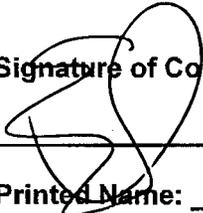
By completing and signing this form the Consultant shall attest that it and all subcontractors performing work under the cited contract meet all conditions contained herein.

Contract Number: IT3-918-3172		
Name (as listed in the contract): Terra Verde Services		
Street Name and Number: 7400 E Pinnacle Peak Road, Suite 100		
City: Scottsdale	State: AZ	Zip Code: 85255

I hereby attest that:

1. The Consultant complies with the Federal Immigration and Nationality Act (FINA), all other Federal immigration laws and regulations, and A.R.S. § 23-214 related to the immigration status of those employees performing work under this contract;
2. All subcontractors performing work under this contract comply with the Federal Immigration and Nationality Act (FINA), all other Federal immigration laws and regulations, and A.R.S. § 23-214 related to the immigration status of their employees.

Signature of Consultant (Employer) or Authorized Designee:



Printed Name: Edward Vasko

Title: Managing Director/Co-Founder

Date (month/day/year): June 29, 2013

EXHIBIT B SCOPE OF WORK

Consultant shall execute a technology network security audit of the City's network architecture and infrastructure as defined by the following objectives and tasks:

1 Project and Contract Management

Consultant will assign a project manager (PM) for the management of the SOW. The PM will meet with the City's Project Manager to discuss, formulate and finalize steps to be taken to complete the network security audit work. City Project Manager will approve all deliverables and associated invoices for this task order as well as providing oversight and guidance to ensure that completion of this task order meets the City's goals and budget.

2 Audit Objectives Details – Control Assessment Objectives and Targets of Evaluation

- 1) 6.2 - Information Security Policy and Controls
- 2) 6.2.5 - Phase I: Interim Findings – First Deliverable Acceptance
- 3) 6.3 - Technical and Physical Controls Assessment
- 4) 6.3.3 - Physical Security, Environmental Security and General Safety security controls.
- 5) 6.3.4 - Communications and Operations Management
- 6) 6.3.5 - Personnel Security and Awareness Training
- 7) 6.3.6 - Regulatory Compliance
- 8) 6.3.7 - Database Infrastructure Security
- 9) 6.3.8 – Phase II: Interim Findings – Second Deliverable
- 10) 6.4 - Audit Evidence – Evidence Evaluation
- 11) 6.4.1 – 6.4.7 - Reporting and Findings Presentations - Third Deliverable and Acceptance

The audit is intended to address the following City Objectives:

- To provide guidance for the City in reducing vulnerabilities that lead to cyber security risks.
- To provide validation for prioritization to remediate known information systems security gaps.

3 Points of Contact

Primary Point of Contact

Name: Mitchell L. Robinson
Title: IT Security Administrator
Organization: City of Chandler
Address: 275 E. Buffalo Street, Chandler, AZ 85225
Phone: (480) 782-2455
E-Mail: mitchell.robinson@chandleraz.gov

Name: Kyle McMaster

Title: Project Manager
Organization: City of Chandler
Address: 275 E. Buffalo Street, Chandler, AZ 85225
Phone: (480) 782-2464, E-Mail: kyle.mcmaster@chandleraz.gov

Other Contacts:

Name: Carolee Stees
Title: Purchasing Agent
Organization: City of Chandler
Address: 175 S. Arizona Avenue, Chandler, AZ 85244-4008
Phone: (480) 782-2405, E-Mail: carolee.stees@chandleraz.gov

Name: John Babcock
Title: IT Security Analyst
Organization: City of Chandler
Address: 275 E. Buffalo Street, Chandler, AZ 85225
Phone: (480) 782-2612, E-Mail: john.babcock@chandleraz.gov

Name: Monique Bond
Title: IT Coordinator – Contracts and Budgets
Organization: City of Chandler
Address: 275 E. Buffalo Street, Chandler, AZ 85225
Phone: (480) 782-2479, E-Mail: monique.bond@chandleraz.gov

Name: Patrick Hait
Title: IT Infrastructure Manager
Organization: City of Chandler
Address: 275 E. Buffalo Street, Chandler, AZ 85225
Phone: (480) 782-2481, E-Mail: patrick.hait@chandleraz.gov

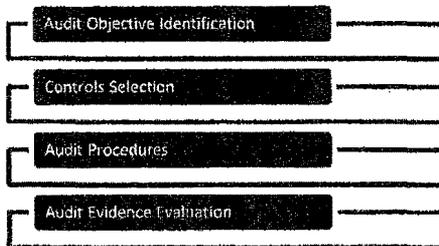
4 Project Scope

The scope of this information systems network security audit is limited in scope and is not comprehensive and shall provide services to the City in identification of cyber security exposures, vulnerabilities, threats and the associated risks. The findings and results of this project shall give remediation guidance and set prioritization to close security gaps.

- **Administrative Controls Assessment**
 - Information Security Policies and Controls
 - Policy Review/SETA Assessment
- **◆ Phase I: Interim Findings – First Deliverable Acceptance**
- **Technical and Physical Controls Assessment**
 - Network Topology and Equipment Assessment
 - Firewall Audit
 - External Vulnerability Assessment
 - External and Internal Network Scanning #1
 - Network Penetration Tests
 - Internal Vulnerability assessment

- External and Internal Network Scanning #2
- Physical Entry Controls assessment
- Audit Logging assessment
- Security Awareness Training Program
- Regulatory Compliance
- Database Infrastructure Security
- ◆ **Phase II: Interim findings – Second Deliverable Acceptance**
- **Phase III: Reporting**
 - Audit Evidence – Evidence Evaluation
 - Reports - Initial draft
 - Reports - Draft reviews
 - Final Reports
- **Findings Presentation(s) – Third Deliverable Acceptance**

5 Audit Program Execution



6 Consultant and City Roles and Responsibilities

6.1 General Consultant and City Auditing Processes

- a. The Consultant shall provide the software and tools to complete this project that include but are not limited to the following: kali, Nessus, sqlmap, Samurai, TVS Report creator (proprietary), Solarwinds, ncat, nmap, perl, ruby, proprietary scripts, TVS scanner whitelancer, W3af, Arachni, Burp Suite Pro, nikto, OWASP ZAP, WAFFIT, and general operating system native commands.
- b. The Consultant shall use industry standards of IT internal controls frameworks to include but not limited to PCI-DSS, HIPAA, NIST, ITIL, ISO27002, and ISACA 's CoBIT and State of Arizona Security Standards. The Consultant shall define and present the audit methodologies and overall tasks to the City prior to starting the processes.
- c. The Consultant shall conduct bi-weekly status meetings with relevant City personnel. The status meetings shall include a written status report in electronic format. The Consultant shall provide drafts of the status meeting notes to the City within 24 hours of the each meeting.
- d. The Consultant shall accomplish the network discovery by utilizing both automatic tools and documentation available. Documentation could be verbal and/or written.
- e. Interviews with staff must be pre-scheduled. The Consultant shall provide prior notice and the objectives, of the interview one week in advance so that the appropriate and responsible is present to respond and provide information.

- f. The City shall provide, network diagrams, server configuration standards, and pertinent documentation for discovery to the Consultant.
- g. The City shall accommodate firewall rules needed to allow the Consultant's access to all network segments under the city's administration. The Consultant shall not be held responsible for analysis exclusion of devices non-reachable by scanners.
- h. The Consultant shall execute multiple server and network equipment scanning tools on production systems. The Consultant shall compile and utilize information found in the discovery and enumeration phases to further gain an understanding of the City's network.
 - i. Conduct pre-approved, authorized and scheduled external attacks and penetration tests designed to identify security vulnerabilities relative to the City's network infrastructure. Perform the assessment against mission critical systems and supporting architectures. Determine if existing security controls and countermeasures are effective against known and recently identified hacking and intrusion techniques. The Consultant may use specially designed techniques as applicable in accordance with US and State of Arizona Laws.
 - ii. It is imperative that the Consultant engage with City management and staff via prior notification of plans to attempt these assessments. Notify City of instances performance or outage impacts affecting production systems and citizen facing applications.
 - iii. Use licensed commercial, known freeware and security assessment tools to test accessibility to network resources. Provide a list of tools to be used for assessment scanning and testing of controls to City staff for review prior to conducting any tests. The Consultant's team will exercise due care as to not disable user accounts. Selected critical vulnerabilities found within the targeted systems of evaluation shall be assessed to include deeper penetration and exploitation where applicable. It is imperative that the Consultant engage with management and staff via prior notification of plans to attempt intrusions during penetration testing and document all activities related to all penetration testing.
- i. The Consultant shall review the audit objectives and provide detailed audit procedures that will be executed to complete tasks within sections 6.2 through 6.5.

6.2 Information Security Policies and Controls

- 6.2.1 Assess, evaluate and report findings for the existence of and practices in the enforcement of information technology systems security policies and controls for the organization.
- 6.2.2 Assess, evaluate and report findings for the drafts of the City Security Policy and Encryption Standards and offer recommendations to ensure the completeness of the draft document with the goal of approval and adoption by City and Information Systems Management.
- 6.2.3 Assess, evaluate and report findings in determination of evidence that the policies address the City's current vulnerabilities, risk levels and provide flexibility for protection against future technological risks, business and security strategies.
- 6.2.4 Assess, evaluate and report findings for information technology security policies that are not developed or implemented.

6.2.5 Phase I: Interim Findings – First Deliverable Acceptance

6.3 Technical Network and Physical Controls Assessment

- 6.3.1 Network Security Topology and Equipment Assessment
- 6.3.2 The Consultant shall assess, evaluate and report findings of network security practices and controls for the City's network devices listed from the enumeration tasks by performing the following:
 - 6.3.2.1 Utilizing Network Scanning Tools, as defined by the Consultant, perform external and internal vulnerability scans to assess, evaluate and report findings of the network traffic routing and filtration rules of network firewalls, and servers. This will include conducting scanning, attack and penetration tests using various security assessment tools designed to identify vulnerabilities, threats and risks associated with the use of the Internet and Internal protected data hosts. These devices shall include but not be limited to, DMZ and Internal servers, Web Servers, FTP servers, E-Mail servers, and Firewalls, inclusive of supporting network devices and services. Due care is to be taken to avoid impacting performance to users.
 - 6.3.2.2 Assess, evaluate and report findings related to selected key network control points to include, but not limited to:
 - (a) Network Firewall Configuration and Administration
 - (b) Anti-Virus, Spyware/Malware Protection
 - (c) Encryption of sensitive data transmitted over the network(s)
 - (d) Network operating systems and systems software configuration controls
 - (e) Network Security administration and monitoring practices
 - (f) URL Filtering and Internet Resource Controls
 - (g) Logical and physical network perimeter access to City data main center

- 6.3.2.3 Assess, evaluate and report findings of the configuration of the City's DMZ's (Demilitarized Zones) physical and virtual servers and supporting infrastructure to ascertain that traffic allowed to physical and Virtual Hypervisor Infrastructure servers within the partially collapsed DMZ are within adequately controlled tolerance levels.
- (a) Ascertain that a complete repository of network device configuration baselines is maintained and compared against actual configuration settings.
 - (b) Evaluate the use of Intrusion Prevention and Detection systems (IPS/IDS) to ensure they are designed and configured to effectively inspect all inbound and outbound network activity and identifies suspicious patterns.
 - (c) Evaluate that filtered messages are automatically quarantined and moved to a SPAM folder for future disposition or deleted on a temporal basis or approved as release candidates
 - (d) Review URL Content filtering systems to ensure that configuration settings and applied policies effectively mitigate risks which prevent City network employee(s) Internet users from accessing inappropriate websites, threat yielding content, productivity loss, and network bandwidth consumption.
 - (e) The Consultant shall enumerate, examine, observe, ascertain and report on the security posture of the following:
- 6.3.2.4 Technology Infrastructure Analysis and Network Security Audit – Perimeter and Internal LAN and WLAN's:
- 6.3.2.4.1 Assess, evaluate and report findings for network and security devices, their policy controls and practices affecting:
- (a) **Firewalls** – Assess, evaluate and report findings of configuration and security effectiveness active City network firewalls.
 - (b) **Anti-Virus/Spyware Malware Prevention** – Assess, evaluate and report findings of the presence and operation effectiveness of the City's Anti-Virus/Malware protection suite. Assess the completeness and effectiveness of the City's desktop firewall deployment.
 - (c) **IPS/IDS Systems** – Assess, evaluate and report findings of IPS policies for the existence of attack logging and blocking
 - (d) **DNS – External and Internal** – Assess, evaluate and report findings of security posture of internal and external DNS implementations against security best practices of administration and management.
 - (e) **Servers Systems (Physical and Virtual)** – Assess server infrastructure's hardening and security postures to ascertain weaknesses, vulnerability threat levels and required remediation needed to meet Federal and State cyber security standards.
- 6.3.2.4.2 Penetration Testing of DMZ and External Network Hosts
- (f) **(Multiple DMZ's and Internal) Hosts** - Assess, evaluate and report on findings to ascertain the effectiveness of countermeasures which prevent;
 - (g) **SQL Injection Successes** – Assess, evaluate and report detailed findings of successful SQL injection attacks against external and internal hosts.
 - (h) **Brute Force Password Attack Successes** – Assess, evaluate and report detailed findings of brute force password attacks against external and internal hosts.
 - (i) **Web server Attack Successes** – Assess, evaluate and report detailed findings of web server vulnerabilities in the DMZ and critical internal hosts.

- (j) **DMZ Firewall and IPS/IDS Penetration Response** – Assess, evaluate and report detailed findings of DMZ Firewall, external and internal IPS / IDS systems to ascertain the ability to prevent, detect, alert and report on attacks.
- (k) **Gather Information or Data Leakage from Internal Network in response to Internet based attacks of the DMZ hosts** – Assess, evaluate and report detailed finding on any resulting data leakage or ownership of external hosts.
- (l) **Root Owner (PWND Systems)** – Assess, evaluate and report on possibility of Root / administrative access and ownership of DMZ servers and supporting systems can be achieved by unauthorized malicious individuals through approved penetration testing.
- (m) **Report on successes / failures** – Assess, evaluate and report detailed findings relating to all external facing and internal facing penetration tests.

6.3.3 Physical Security, Environmental Security and General Safety security controls.

- 6.3.3.1 **Locations – IT Building Data Center and Chandler City Hall Data Center**– Assess, evaluate and report findings of physical, environmental controls and protections of the City's Data and Server rooms. Report findings relating to remediation or required improvements to these facilities.
- 6.3.3.2 **Fire detection, prevention and suppression** – Assess, evaluate and report findings for fire suppression and prevention systems deployed.
- 6.3.3.3 **Restricted areas, authorization, methods and controls** – Assess, evaluate and report findings of the existence of access controls relating to data networks and supporting equipment for restricted areas. Assess, evaluate and report findings relating to the use and practice of proper authorization to access restricted areas of City facilities controls such as; Cameras, Badging systems, and keys.
- 6.3.3.4 **Motion Detectors, Physical Intrusion Detection, Sensors, and Alarms** – Assess, evaluate and report findings for the existence and operations of burglar detection, their associated sensors and alarm functions.
- 6.3.3.5 **Fencing, security guards, and security badge types** – Evaluate and assess for reasonable use of security fencing, on premise armed/unarmed security personnel (Guards). Report all findings relating to deficiencies and inadequate protections.
- 6.3.3.6 **General Safety** – Assess, evaluate and report general safety findings. The City provides for detailed safety inspections. Report all findings relating to general safety issues.

6.3.4 Communications and Operations Management (Network Performance and Tactical, operations)

- 6.3.4.1 **Network Security Monitoring and Logging** – Assess, evaluate and report findings relating to the existence of and ability to monitor, log network security attacks, delineate and report on network security threats, correlate to affected hosts and affect tactical response, fixes, and documentation of network security attacks and incidents.
- 6.3.4.2 **Notification and Alerting** – Assess, evaluate and report findings relating to the existence of and ability to receive automated, sufficiently detailed systems outage notifications, with expected acceptable responses and recovery time.

6.3.5 Personnel Security and Awareness Training

- 6.3.5.1 **Security Awareness Training** – Assess, evaluate and report findings regarding the existence of a Security Awareness Program in a learning management system. Evaluate the program to assess whether the security awareness program learning modules and system administration demonstrates the ability to track and report course completions, delineates the responsibilities of staff to attend mandatory computer based and classroom security awareness training offering, and covers NCIC TOC for IT and Police staff.

6.3.6 Regulatory Compliance

- 6.3.6.1 **Regulatory Compliance** - Assess, evaluate, report findings where gaps exist in the presence of effective controls to meet State, Federal regulations and technology industry standard practices that ensure protections against breaches to PII, ePHI, credit card data, Internal confidential and sensitive information and data.

6.3.7 Database Infrastructure Security

- 6.3.7.1 **MSSQL DB Environments** – Assess security controls for databases within the MSSQL database clusters and standalone environments.
- 6.3.7.2 **Oracle DB Environments** – Assess security controls for databases within the Oracle database clusters and standalone environments.

6.3.8 Phase II: Interim Findings – Second Deliverable Acceptance

6.4 Audit Evidence – Evidence Evaluation

- 6.4.1 The Consultant shall review, compile, formulate and deliver evidence evaluation reports, audit findings impacts, analyses with risk levels within scorecard formatted reports, to include all remediation solutions and recommendations.
- 6.4.2 One “Confidential” labeled protected hardcopy report of the detailed audit evidence report.
- 6.4.3 One “Confidential” labeled digitally secured electronic copy of the detailed audit evidence report.
- 6.4.4 One “Confidential” labeled, protected hardcopy report of the detailed, scorecard formatted audit findings report with remediation recommendations

6.4.5 One "Confidential" labeled, digitally secured, scorecard formatted audit findings report.

6.4.6 One "Confidential" labeled, digitally secured, findings presentation.

6.4.7 Findings Presentation(s) – Third Deliverable Acceptance

6.5 Consultant Services Engagement Assumptions:

The scope and timeline of this project are based on the following assumptions. If these prove to be untrue, the deliverables and/or finish date may need to change, which may also impact total cost.

- ✦ Significant rework of the environment will not be necessary in order to conduct the assessment.
- ✦ Consultant will not be responsible for:
 - Third party software functionality within City’s existing technical environment;
 - Management decisions with respect to this project;
 - Data consistency and integrity issues; and
 - Activities related to system programming and certification of reporting results.
- ✦ Regulatory requirements are subject to change. Consultant will work with City to ensure the latest criteria are used. Changes may impact the overall hours and requirements needed to complete this engagement.

During the various phases of this project, Consultant may assign more than one resource to complete the evaluations within each phase. As such, Consultant may require access to more than one internal City resource. Although Consultant does not anticipate this to be an issue, the risk of delay can progressively increase as additional simultaneous resources are involved. Consultant will make every possible effort to minimize impact to City resources. Nonetheless, City of Chandler Information Technology staff may be required to escort Consultant, provide access to facilities, answer evaluation questionnaires, provide documentation and/or configurations, and participate in project meetings.

6.6 Technical Inventory

Network Components	Count
Primary Site: Phoenix	2
Number of Employees	1900
Number of External Host	18
Number of External IP Addresses	60

6.7 Deliverables

Sections	Audit Objectives Project Plan
6.2.2 Phase I: Administrative Controls Assessment	
6.2.1 - 6.2.3	Information Security Policies and Controls
6.2.4	Policy review / SETA assessment
6.2.5 ♦ Phase I: Interim Findings – First Deliverable Acceptance	
6.3 Phase II: Technical and Physical Controls Assessment	
6.3.1 – 6.3.2	Network Topology and Equipment Assessment
6.3.2.1 – 6.3.2.2, 6.3.2.3, 6.3.2.4.1 – 6.3.2.4.2	Firewall Audit
6.3.2.1 – 6.3.2.2, 6.3.2.3, 6.3.2.4.1 – 6.3.2.4.2	External Vulnerability Assessment
6.3.2.1 – 6.3.2.2, 6.3.2.3, 6.3.2.4.1 – 6.3.2.4.2	Scanning #1 - External and Internal Network
6.3.2.1 – 6.3.2.2, 6.3.2.3, 6.3.2.4.1 – 6.3.2.4.2	Internal Vulnerability assessment
6.3.2.1 – 6.3.2.2, 6.3.2.3, 6.3.2.4.1 – 6.3.2.4.2	Scanning #2 - External and Internal Network
6.3.2.4.2	Network Penetration Tests
6.3.3	Physical Entry Controls assessment

Sections	Audit Objectives Project Plan
6.3.4	Communications and Operations Management (Network Performance and Tactical, operations)
6.3.4.1-6.3.4.2	Audit Logging assessment - Network Security Monitoring and Logging, Notifications, Alerting
6.3.5, 6.3.5.1	Security Awareness Training Program
6.3.6	Regulatory Compliance
6.3.7	Database Infrastructure Security
6.3.8 ♦ Phase II: Interim findings – Second Deliverable Acceptance	
6.4	Phase III: Reporting
6.4.1-6.4.6	Audit Evidence – Evidence Evaluation
6.4.1-6.4.6	Reports - Initial draft
6.4.1-6.4.6	Reports - Draft reviews
6.4.1-6.4.6	Final Reports
6.4.7 Findings Presentation(s) – Third Deliverable Acceptance	
♦ Project ends	
Total working days: 35	

6.7.1 Supporting Requirements Documents

- 6.7.1.1 Consultant has completed the Pre-Engagement -Non-Disclosure Agreement-With Data Destruction – MSWord – **Completed and on file.**
- 6.7.1.2 Consultant shall complete a Contractual Engagement documents with the City of Chandler purchasing and information technology divisions that includes the Non-Disclosure Agreements – with Data Destruction clauses- MSWord
- 6.7.1.3 Consultant shall complete, Attachment C -Third Party Connection Requirements – MSWord and return it to the City prior to the engagement to provision network scanning and access controls.
- 6.7.1.4 Consultant shall complete a Third Party Connection Agreement – MSWord and return it to the City prior to the engagement to ensure that connectivity of scanning devices and responsibilities are met with respect to network access controls.
- 6.7.1.5 Organizational Roles and Responsibilities –Management, Technical, Administrative – Organizational Charts –
- ❖ City of Chandler IT shall provide a City of Chandler IT Organizational Chart
 - ❖ Consultant shall provide Consultant’s Organization Chart
- 6.7.1.6 Consultant shall provide Consultant Audit Framework “Checklists” Documentation to the City

6.8 Glossary

802.1q - The IEEE's 802.1Q standard was developed to address the problem of how to break large networks into smaller parts so broadcast and multicast traffic wouldn't grab more bandwidth than necessary. The standard also helps provide a higher level of security between segments of internal networks. The ability to move end stations to different broadcast domains by setting membership profiles for each port on centrally managed switches is one of the main advantages of 802.1Q VLANs.

802.1X - IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

802.11x - IEEE 802.11 is a set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard **IEEE 802.11-2012** has had subsequent amendments. These standards provide the basis for wireless network products using the Wi-Fi brand.

6.8.1 References

- Previous TCBA Audit - 2008
- ISO, NIST, and SANS Audit Frameworks
- City of Chandler Security Policies
- Current and Strategic planning for Network and Security Technology Infrastructure
- Planned Technology Business systems upgrades, refreshes and migration to cloud based systems
- Internally Developed Audit Framework

**EXHIBIT C
FEE SCHEDULE**

Sections	Audit Objectives Project Plan	
6.2.2 Phase I: Administrative Controls Assessment		
6.2.1 - 6.2.3	Information Security Policies and Controls	
6.2.4	Policy review / SETA assessment	
6.2.5 ♦ Phase I: Interim Findings – First Deliverable Acceptance		\$10,000
6.3 Phase II: Technical and Physical Controls Assessment		
6.3.1 – 6.3.2	Network Topology and Equipment Assessment	
6.3.2.1 – 6.3.2.2, 6.3.2.3, 6.3.2.4.1 – 6.3.2.4.2	Firewall Audit	
6.3.2.1 – 6.3.2.2, 6.3.2.3, 6.3.2.4.1 – 6.3.2.4.2	External Vulnerability Assessment	
6.3.2.1 – 6.3.2.2, 6.3.2.3, 6.3.2.4.1 – 6.3.2.4.2	Scanning #1 - External and Internal Network	
6.3.2.1 – 6.3.2.2, 6.3.2.3, 6.3.2.4.1 – 6.3.2.4.2	Internal Vulnerability assessment	
6.3.2.1 – 6.3.2.2, 6.3.2.3, 6.3.2.4.1 – 6.3.2.4.2	Scanning #2 - External and Internal Network	
6.3.2.4.2	Network Penetration Tests	
6.3.3	Physical Entry Controls assessment	
6.3.4	Communications and Operations Management (Network Performance and Tactical, operations)	
6.3.4.1-6.3.4.2	Audit Logging assessment - Network Security Monitoring and Logging, Notifications, Alerting	
6.3.5, 6.3.5.1	Security Awareness Training Program	
6.3.6	Regulatory Compliance	
6.3.7	Database Infrastructure Security	
6.3.8 ♦ Phase II: Interim findings – Second Deliverable Acceptance		\$10,000
6.4 Phase III: Reporting		
6.4.1-6.4.6	Audit Evidence – Evidence Evaluation	
6.4.1-6.4.6	Reports - Initial draft	
6.4.1-6.4.6	Reports - Draft reviews	
6.4.1-6.4.6	Final Reports	
6.4.7 Findings Presentation(s) – Third Deliverable Acceptance		\$15,000
♦ Project ends		
		Total working days: 35

**EXHIBIT D
INSURANCE REQUIREMENTS**

Indemnification:

1. **Indemnification.** To the fullest extent permitted by law, CONSULTANT, its successors, assigns and guarantors, shall defend, indemnify and hold harmless City and any of its elected or appointed officials, officers, directors, commissioners, board members, agents or employees from and against any and all allegations, demands, claims, proceedings, suits, actions, damages, including, without limitation, property damage, environmental damages, personal injury and wrongful death claims, losses, expenses (including claim adjusting and handling expenses), penalties and fines (including, but not limited to, attorney fees, court costs, and the cost of appellate proceedings), judgments or obligations, which may be imposed upon or incurred by or asserted against the City by reason of this Agreement or the services performed or permissions granted under it, or related to, arising from or out of, or resulting from any negligent or intentional actions, acts, errors, mistakes or omissions caused in whole or part by CONSULTANT, or any of its subcontractors, or anyone directly or indirectly employed by any of them or anyone for whose acts any of them may be liable, relating to the discharge of any duties or the exercise of any rights or privileges arising from or incidental to this Agreement, including but not limited to, any injury or damages claimed by any of CONSULTANT's and subcontractor's employees.

Insurance:

1. **General.**
 - A. At the same time as execution of this Agreement, the CONSULTANT shall furnish the City of Chandler a certificate of insurance on a standard insurance industry ACORD form. The ACORD form must be issued by an insurance company authorized to transact business in the State of Arizona possessing a current A.M. Best, Inc. rating of A-7, or better and legally authorized to do business in the State of Arizona with policies and forms satisfactory to CITY. Provided, however, the A.M. Best rating requirement shall not be deemed to apply to required Workers' Compensation coverage.
 - B. The CONSULTANT and any of its subcontractors, subconsultants or sublicensees shall procure and maintain, until all of their obligations have been discharged, including any warranty periods under this Agreement are satisfied, the insurances set forth below.
 - C. The insurance requirements set forth below are minimum requirements for this Agreement and in no way limit the indemnity covenants contained in this Agreement.
 - D. The City in no way warrants that the minimum insurance limits contained in this Agreement are sufficient to protect CONSULTANT from liabilities that might arise out of the performance of the Agreement services under this Agreement by CONSULTANT, its agents, representatives, employees, subcontractors, sublicensees or subconsultants and the CONSULTANT is free to purchase any additional insurance as may be determined necessary.
 - E. Failure to demand evidence of full compliance with the insurance requirements in this Agreement or failure to identify any insurance deficiency will not relieve the CONSULTANT from, nor will it be considered a waiver of its obligation to maintain the required insurance at all times during the performance of this Agreement.
 - F. **Use of SubContractors:** If any work is subcontracted in any way, the CONSULTANT shall execute a written agreement with Subcontractor containing the same

Indemnification Clause and Insurance Requirements as the City requires of the CONSULTANT in this Agreement. The CONSULTANT is responsible for executing the Agreement with the Subcontractor and obtaining Certificates of Insurance and verifying the insurance requirements.

2. Minimum Scope And Limits Of Insurance. The CONSULTANT shall provide coverage with limits of liability not less than those stated below.
 - A. *Commercial General Liability-Occurrence Form.* CONSULTANT must maintain "occurrence" form Commercial General Liability insurance with a limit of not less than \$2,000,000 for each occurrence, \$4,000,000 aggregate. Said insurance must also include coverage for products and completed operations, independent Consultants, personal injury and advertising injury. If any Excess insurance is utilized to fulfill the requirements of this paragraph, the Excess insurance must be "follow form" equal or broader in coverage scope than underlying insurance.
 - B. *Automobile Liability-Any Auto or Owned, Hired and Non-Owned Vehicles Vehicle Liability.* CONSULTANT must maintain Business/Automobile Liability insurance with a limit of \$1,000,000 each accident on CONSULTANT owned, hired, and non-owned vehicles assigned to or used in the performance of the CONSULTANT's work or services under this Agreement. If any Excess or Umbrella insurance is utilized to fulfill the requirements of this paragraph, the Excess or Umbrella insurance must be "follow form" equal or broader in coverage scope than underlying insurance.
 - C. *Workers Compensation and Employers Liability Insurance:* CONSULTANT must maintain Workers Compensation insurance to cover obligations imposed by federal and state statutes having jurisdiction of CONSULTANT employees engaged in the performance of work or services under this Agreement and must also maintain Employers' Liability insurance of not less than \$1,000,000 for each accident and \$1,000,000 disease for each employee.
 - D. *Professional Liability.* If the Agreement is the subject of any professional services or work performed by the CONSULTANT, or if the CONSULTANT engages in any professional services or work adjunct or residual to performing the work under this Agreement, the CONSULTANT must maintain Professional Liability insurance covering errors and omissions arising out of the work or services performed by the CONSULTANT, or anyone employed by the CONSULTANT, or anyone whose acts, mistakes, errors and omissions the CONSULTANT is legally liable, with a liability limit of \$1,000,000 each claim and \$2,000,000 all claims. In the event the Professional Liability insurance policy is written on a "claims made" basis, coverage must extend for 3 years past completion and acceptance of the work or services, and the CONSULTANT, or its selected Design Professional will submit Certificates of Insurance as evidence the required coverage is in effect. The Design Professional must annually submit Certificates of Insurance citing that the applicable coverage is in force and contains the required provisions for a 3 year period.
3. Additional Policy Provisions Required.
 - A. *Self-Insured Retentions Or Deductibles.* Any self-insured retentions and deductibles must be declared and approved by the City. If not approved, the City may require that the insurer reduce or eliminate any deductible or self-insured retentions with respect to the City, its officers, officials, agents, employees, and volunteers.
 - B. *City as Additional Insured.* The policies are to contain, or be endorsed to contain, the following provisions:

1. The Commercial General Liability and Automobile Liability policies are to contain, or be endorsed to contain, the following provisions: The City, its officers, officials, agents, and employees are additional insureds with respect to liability arising out of activities performed by, or on behalf of, the CONSULTANT including the City's general supervision of the CONSULTANT; Products and Completed operations of the CONSULTANT; and automobiles owned, leased, hired, or borrowed by the CONSULTANT.
2. The CONSULTANT's insurance must contain broad form contractual liability coverage and must not exclude liability arising out of explosion, collapse, or underground property damage hazards ("XCU") coverage.
3. The City, its officers, officials, agents, and employees must be additional insureds to the full limits of liability purchased by the CONSULTANT even if those limits of liability are in excess of those required by this Agreement.
4. The CONSULTANT's insurance coverage must be primary insurance with respect to the City, its officers, officials, agents, and employees. Any insurance or self-insurance maintained by the City, its officers, officials, agents, and employees shall be in excess of the coverage provided by the CONSULTANT and must not contribute to it.
5. The CONSULTANT's insurance must apply separately to each insured against whom claim is made or suit is brought, except with respect to the limits of the insurer's liability.
6. Coverage provided by the CONSULTANT must not be limited to the liability assumed under the indemnification provisions of this Agreement.
7. The policies must contain a severability of interest clause and waiver of subrogation against the City, its officers, officials, agents, and employees, for losses arising from Work performed by the CONSULTANT for the City.
8. The CONSULTANT, its successors and or assigns, are required to maintain Commercial General Liability insurance as specified in this Agreement for a minimum period of 3 years following completion and acceptance of the Work. The CONSULTANT must submit a Certificate of Insurance evidencing Commercial General Liability insurance during this 3 year period containing all the Agreement insurance requirements, including naming the City of Chandler, its agents, representatives, officers, directors, officials and employees as Additional Insured as required.
9. If a Certificate of Insurance is submitted as verification of coverage, the City will reasonably rely upon the Certificate of Insurance as evidence of coverage but this acceptance and reliance will not waive or alter in any way the insurance requirements or obligations of this Agreement. If any of the required policies expire during the life of this Agreement, the CONSULTANT must forward renewal or replacement Certificates to the City within 10 days after the renewal date containing all the necessary insurance provisions.