Vulnerability Assessment Statement of Work

Between:

Johnson County (JC)

And:

Texas Department of Information Resources (DIR)

JC
October 28, 2013

Texas Department of Information Resources
Office of the State CISO
300 West 15th Street, Suite 1300
Austin, TX 78701
512-475-4780

http://www.dir.texas.gov/security

Confidential

DEPARTMENT OF INFORMATION RESOURCES
P.O. Box 13564 ♦ Austin, TX 78711-3564 ♦ www.dir.texas.gov/security
Tel: (512) 475-4700 ♦ Fax: (512) 475-4759

1. PURPOSE

This Statement of Work (SOW) describes services to be provided to **Johnson County (JC)** by the **Department of Information Resources (DIR)** for the external Vulnerability Assessment and sets forth the responsibilities for each party.

Services shall begin on the execution of this agreement on behalf of JC and when all authorizations required from third parties under *Section 3.2* are provided to DIR.

2. PROJECT OBJECTIVES, SCOPE, AND ACTIVITIES

2.1 Objectives

The DIR Office of the State CISO will assess JC's network security by conducting a Vulnerability Assessment, which will be performed quarterly throughout the fiscal year. Refer to the quarterly scanning schedule in *Section 6.1* on page 6. DIR will assess JC's network security through Internet connectivity. The outcome of this engagement will assist JC with improving security posture based on the security needs within the organization.

2.2 Scope

DIR will:

- Conduct quarterly vulnerability scans and provide JC with the findings.
- Attempt to identify security vulnerabilities on all discoverable devices and hosts within the specified IP range on JC's network. All discovered devices and hosts within JC's network and system administrative control will be subject to scanning on a 24/7 basis until complete, except for those indicated in *Sections 8.2* and *9.2*; however, DIR does not guarantee that all devices or hosts will be assessed.
- Generate reports from the automated scanner based on the findings of the scan and provide JC with those results in PDF format.

2.3 Activities

DIR will perform numerous activities required for the completion of the Vulnerability Assessment. DIR will use automated vulnerability scanners to conduct quarterly assessments.

DEPARTMENT OF INFORMATION RESOURCES
P.O. Box 13564 ♦ Austin, TX 78711-3564 ♦ www.dir.texas.gov/security
Tel: (512) 475-4700 ♦ Fax: (512) 475-4759

3. CONDITIONS FOR PROVIDING SECURITY SERVICES

3.1 Access

The Internet shall be used for primary access to JC's systems unless otherwise noted and agreed upon. JC shall not employ special access restrictions against DIR that it does not apply to the rest of the public network over the course of regular business.

3.2 Network Control

JC must inform DIR if JC does not control its network access and/or its Internet service is provided via a third party. JC is responsible for obtaining all necessary approvals before the Vulnerability Assessment begins. JC shall provide all necessary contact information for the third parties that control its network access, Internet service, and/or web applications in *Section 7.4.*

3.3 Disclosure of Objectionable Material to Agency Executive Director

In conducting the services authorized by JC under this SOW, DIR may inadvertently uncover obscene, excessively violent, harassing, or otherwise objectionable material that may violate State or Federal law, including material that may infringe the intellectual property of a third party on JC devices or networks being assessed. The existence of all such objectionable and/or potentially illicit material shall be brought to the attention of JC's Executive Director or highest level executive by DIR so that JC may deal with the objectionable and/or potentially illicit material as it deems appropriate. If DIR encounters child pornography, as defined in the Child Sexual Exploitation and Pornography Act, 18 U.S.C., Chapter 110, in conducting the activities covered by the SOW, DIR shall report such to an appropriate law enforcement agency and provide the law enforcement agency access to the visual depictions of child pornography. If DIR accesses information that they perceive as a serious threat to human life or safety in conducting the activities covered by the SOW, DIR shall report such threat to an appropriate law enforcement agency.

3.4 Confidentiality

Pursuant to Texas Government Code, Sections 2054.077, 2059.055, and 552.139, except for the purposes of this SOW and to propose customized security profiles and mitigation strategies, DIR shall not disclose the data derived from the services provided under this SOW. However, DIR may provide a copy of the vulnerability assessment reports to the State Auditor's Office or the Legislature upon request, or other entity approved by JC, and DIR may disclose certain information to appropriate law enforcement agencies as set forth in Sections 3.3 and 4.2 of this SOW. DIR may use aggregated and anonymized statistics derived from the data for other purposes. DIR will also inform its Communications Technology Services Division and/or Network and Security Operations Center (NSOC) if vulnerabilities noted during the testing are from equipment owned or managed by the Communications Technology Services Division as set forth in Section 4.2.

DEPARTMENT OF INFORMATION RESOURCES
P.O. Box 13564 ♦ Austin, TX 78711-3564 ♦ www.dir.texas.gov/security
Tel: (512) 475-4700 ♦ Fax: (512) 475-4759

3.5 No Warranties and Limitation of Liability

DIR makes no representation or warranty that its security services will disclose all vulnerabilities. DIR hereby disclaims all warranties, both express and implied, including without limitation, the implied warranties of merchantability and fitness for a particular purpose. In no event shall DIR be liable for damages of any kind or nature that may arise from the services provided by DIR under this SOW.

3.6 Service Interruption

DIR will endeavor not to disrupt JC services. However, some scanning, probing, and Vulnerability Assessment tools are aggressive in their actions and may affect the serviceability of poorly configured or overextended systems or services. While DIR endeavors to use the safest methods to assess JC's systems, JC should be prepared to restore a damaged system from a recent, acceptable backup within an acceptable time as determined by JC. DIR will NOT conduct any deliberate Denial-of-Service attack. JC agrees not to hold DIR liable in the event of any service interruption(s) that may arise as a result of performance of the Vulnerability Assessment under this SOW. If either party becomes aware of a service interruption, that party will notify the other party's emergency contact.

4. RESPONSIBILITIES AND ASSUMPTIONS

4.1 JC Responsibilities

- JC shall add DIR's IP range, which shall be provided by DIR prior to the Vulnerability Assessment initiation, to JC's non-shun list within JC's IDS/IPS.
- JC shall not intentionally place an unsecured system or device in the assessment scope.
- JC's emergency contact list shall include staff capable of administering JC computer systems and who are on 24-hour notification during the Vulnerability Assessment.

4.2 DIR Responsibilities

DIR shall:

- Provide the services described in this SOW to JC at no cost to JC.
- Conduct the activities covered by this SOW within the engagement timeframe.
- Provide JC with the source IP addresses associated with the Vulnerability Assessment activities if JC detects DIR activities and requests confirmation if detected source IP addresses are associated with DIR's assessment activity.
- If DIR detects that JC is "shunning" or preventing DIR from completing Vulnerability Assessment activities, DIR shall contact JC and request that JC add DIR's IP range to JC's non-shun list within JC's IDS/IPS.
- Notify JC if anomalies such as system failure, inappropriate use of resources, or actual malicious attack are discovered during the Vulnerability Assessment.

DEPARTMENT OF INFORMATION RESOURCES
P.O. Box 13564 ♦ Austin, TX 78711-3564 ♦ www.dir.texas.gov/security
Tel: (512) 475-4700 ♦ Fax: (512) 475-4759

- If DIR encounters child pornography, as defined in the Child Sexual Exploitation and Pornography Act, 18 U.S.C, Chapter 110, in conducting the activities covered by the SOW, DIR shall report such to an appropriate law enforcement agency and provide the law enforcement agency access to the visual depictions of child pornography.
- If DIR encounters information that they perceive as a serious threat to human life or safety in conducting the activities covered by the SOW, DIR shall report such threat to an appropriate law enforcement agency and JC's Executive Director or highest level executive.

5. NOTES ON VULNERABILITY SCANNERS

- No 'known vulnerability' scanner is perfect. It is possible that an existing vulnerability may not have been found or that a vulnerability found may not actually be present. DIR uses vulnerability scanners that consistently perform at the top of their class. Verify and understand the vulnerability before deciding to remediate/mitigate it. In many cases, remediating/mitigating the vulnerability entails upgrading software.
- A vulnerability for "Agency A" may not be a vulnerability for "Agency B". Organizations have their own specific business plans and needs. Each organization must evaluate the need to provide a service with the risk that the service may be abused. For example, file transfer protocol (FTP) may be listed as a vulnerability; if the organization intends to provide the FTP services, there is no need to remediate/mitigate. However, if the business does not need to provide FTP services, it may decide to discontinue that service. Evaluate the risk of providing the service and accepting the risk versus not providing the service. This is a management decision.
- Vulnerability scanning tools attempt to identify the vendors of services and operating systems. This identification is not always accurate. JC should review the Vulnerability Assessment reports and verify the existence of the vulnerability and then follow the vendor's instruction for remediating/mitigating it.
- New vulnerabilities are discovered every day. DIR updates its tools before every Vulnerability Assessment to ensure that the highest number of known vulnerabilities is identified at the time the assessment is performed.

DEPARTMENT OF INFORMATION RESOURCES
P.O. Box 13564 ♦ Austin, TX 78711-3564 ♦ www.dir.texas.gov/security
Tel: (512) 475-4700 ♦ Fax: (512) 475-4759

6. PERIOD OF PERFORMANCE

6.1 Quarterly Scanning

The Vulnerability Assessment will commence on **October 28, 2013, @ 7:00 a.m. CST**. The following charts summarize approximate start and end dates for each project phase in each quarter. DIR will notify JC before the start of each quarter's scanning.

First Quarter Scanning

1. Perform Network Scanning 2. Generate and Deliver Reports	10/28/2013	11/8/2013

Second Quarter Scanning

1. Perform Network Scanning 2. Generate and Deliver Reports	1/27/2014	2/7/2014

Third Quarter Scanning

1. Perform Network Scanning 2. Generate and Deliver Reports	4/28/2014	5/9/2014

Fourth Quarter Scanning

1. Perform Network Scanning 2. Generate and Deliver Reports	7/28/2014	8/8/2014

6.2 WAVS Scanning

DIR will also perform a web application vulnerability scan (WAVS) on up to five JC URLs. The following chart summarizes approximate start and end dates for each project phase.

1. Perform Web Application Vulnerability Scanning 2. Generate and Deliver Reports	10/28/2013	11/8/2013

DEPARTMENT OF INFORMATION RESOURCES
P.O. Box 13564 ♦ Austin, TX 78711-3564 ♦ www.dir.texas.gov/security
Tel: (512) 475-4700 ♦ Fax: (512) 475-4759

7. CONTACTS

7.1 Organization Name and Address

Agency Name	Johnson County (JC)
Address	2 N Mill Street
City, State, Zip	Cleburne, Texas 76028
Agency No.	

7.2 Engagement Contacts

7.2.1 DIR Contacts

Primary Contact	**Name**	Ted James, IT Security Program Manager		
	Phone Number	512-463-4220	**Mobile**	
	Email	ted.james@dir.texas.gov		
Secondary Contact	**Name**	Edward Block, Deputy Chief Information Security Officer		
	Phone Number	512-463-8807	**Mobile**	
	Email	edward.block@dir.texas.gov		
Emergency Contact	**Phone**	512-350-3282 (24/7 emergency phone)		

7.2.2 JC Contacts

Signature Authority	**Name**	Roger Harmon		
	Position	County Judge		
	Phone Number		**Cell**	
	Email			
Primary Contact/ ISO	**Name**	Chris Holt		
	Position	System Administrator		
	Phone Number	817-556-6366	**Cell**	817-726-0513
	Email	cholt@johnsoncountytx.org		
Secondary Contact	**Name**	Dan Milam		
	Position	IT Director		
	Phone Number	817-556-6366	**Cell**	817-715-1375
	Email	dmilam@johnsoncountytx.org		
Additional Contact	**Name**			
	Position			
	Phone Number		**Cell**	
	Email			
Additional Contact	**Name**			
	Position			
	Phone Number		**Cell**	
	Email			

DEPARTMENT OF INFORMATION RESOURCES
P.O. Box 13564 ♦ Austin, TX 78711-3564 ♦ www.dir.texas.gov/security
Tel: (512) 475-4700 ♦ Fax: (512) 475-4759

7.3 JC Emergency Contacts

The people listed below have been designated as JC's emergency contacts and are listed in the order of escalation.

Alert Escalation	Name	Number	Cell
1st Alert	Chris Holt	817-556-6366	817-726-0513
2nd Alert	Dan Milam	817-556-6366	817-715-1375
3rd Alert			

7.4 Third Party Contact Information

Organization Name	Sagentic Web Design
Contact Name	Kenny Haferkamp
Contact Phone Number	(817) 760-0098
Contact Email Address(es)	support@sagentic.com

DEPARTMENT OF INFORMATION RESOURCES
P.O. Box 13564 ♦ Austin, TX 78711-3564 ♦ www.dir.texas.gov/security
Tel: (512) 475-4700 ♦ Fax: (512) 475-4759

8. ENGAGEMENT IP ADDRESS RANGES

8.1 IP Addresses and Ranges

JC provided the IP addresses and/or ranges listed below for the Vulnerability Assessment. JC has direct or indirect administrative control over the listed IP addresses, and the addresses are listed by preference. Please note that DIR may not assess all hosts or IP ranges given time, resources, or other project constraints.

1.	66.143.87.130 – 66.143.87.254	2.	
3.		4.	
5.		6.	
7.		8.	
9.		10.	

8.2 IP Addresses to Exclude

JC requested that DIR not assess the IP addresses and/or ranges listed below.

#	IP Address or IP Address Range	Reason for Exclusion
1.		
2.		
3.		
4.		
5.		

8.3 Special Instructions

In accordance with JC's instructions, the following conditions will be adhered to during the course of the assessment:

Note special instructions here.

DEPARTMENT OF INFORMATION RESOURCES
P.O. Box 13564 ♦ Austin, TX 78711-3564 ♦ www.dir.texas.gov/security
Tel: (512) 475-4700 ♦ Fax: (512) 475-4759

9. ENGAGEMENT URLS (FOR WAVS)

9.1 URLs

JC provided the URLs listed below (up to **five**) for the Vulnerability Assessment. JC has administrative control over the URLs listed, and the URLs are listed by preference. Please note that DIR may not assess all URLs given time, resources, or other project constraints.

1.	http://www.johnsoncountytx.org/
2.	http://johnsoncountytaxoffice.org/
3.	http://jctxsheriff.org/
4.	http://johnsoncountyelections.com/
5.	http://www.hammcreek.com/

9.2 URLs to Exclude

JC requested that DIR not assess the URLs listed below.

#	URL	Reason for Exclusion
1.		
2.		
3.		

9.3 WAVS Special Instructions

In accordance with JC, the following special instructions will be adhered to during the course of WAVS assessment:

Note special instructions here.

10. DELIVERABLES

DIR will deliver to JC all reports generated by the automated vulnerability scanning tools used, which will detail the findings from the Vulnerability Assessment.

DEPARTMENT OF INFORMATION RESOURCES
P.O. Box 13564 ♦ Austin, TX 78711-3564 ♦ www.dir.texas.gov/security
Tel: (512) 475-4700 ♦ Fax: (512) 475-4759

11. ACCEPTANCE AND AUTHORIZATION

JC certifies that the information provided by JC in this SOW is accurate, and JC agrees to notify DIR immediately if any inaccuracies are found before, during, or after the Vulnerability Assessment.

JC hereby executes this SOW by its duly authorized representative below and authorizes DIR to conduct the Vulnerability Assessment described in this SOW.

By: Roger Harmon – JC County Judge

(Signature)

10-28-13

(Date)

By: Brian Engle – DIR Chief Information Security Officer

(Signature)

11/19/13

(Date)

DIR Office of the General Counsel

11-19-13