**Statement of Work under STC 918A**

# Agency and/or Division: Agency - Division

# Project Number and/or Name: Project #####

# (Under State Term Contract 918A)

# Issue Date: Month Day, Year

# Deadline for Questions: Month Day, Year at X:XX

# Due Date for SOW Response: Month Day, Year at X:XX

# Contact Person: Name

# Agency – Division

# Email

# Telephone

# General Information

Written questions regarding this Statement of Work (SOW) shall be emailed to the contact person listed above at the email address provided. Please include **Project ######** in the subject line of the email. All questions will be addressed and responses will be e-mailed to each Vendor on the Security Assessment Services Contract. No verbal questions will be accepted. The questions should be submitted in the following format:

|  |  |  |
| --- | --- | --- |
| Citation | Vendor Question | Agency Response |
| SOW Section, Page Number |  |  |

SOWs are to be sent via email or one (1) electronic copy on a password protected USB Drive with password sent separately to the Contact Person listed above.

SOWs must be received no later than **Month Day, Year at X:XX**. SOWs received after the Due Date for the SOW Response will be not be considered.

This SOW is subject to and governed by the terms and conditions in ITS-400279 (i.e. State Term Contract 918A).

# Security Assessment Services Project Description

The AGENCY / DIVISION is responsible for the overall approach to information security at the agency and the operational security aspects of its hosted systems and applications. The AGENCY / DIVISION oversees general vulnerability scans and periodic security assessments. Audits are conducted internally and by third-parties to ensure regulatory requirements are met. AGENCY / DIVISION is looking to assess the security posture of its applications and systems and this assessment should be based on the NIST 800-53 rev. 4 standards. The overall objective of this assessment is to strengthen the cybersecurity posture of the agency by identifying and prioritizing those deficiencies that are key for the protection of the citizen’s data.

# Purpose

The purpose of this Statement of Work (SOW) is for State Agencies to be able to quickly procure proactive cybersecurity services from leading commercial providers in order to better protect systems identified as Restricted and Highly Restricted and to meet requirements set forth by the State Chief Information Officer (SCIO) and the Enterprise Security and Risk Management Office (ESRMO). This SOW will assist State Agencies in procuring proactive cybersecurity services consistent with the State’s Continuous Monitoring Plan.

# Scope

The Vendor shall perform an assessment of the State of North Carolina’s security posture in order to provide detailed analysis of: identification of application, system and network vulnerabilities; gaps in IT security governance; assessment of patching methodologies; current network security capabilities and potential existing security incidents. The assessment and reporting will be based on the NIST 800-53 MODERATE security controls.

The assessment will consist of external and internally accessible systems, hosts and applications with the agency’s environment and shall consider, at a minimum, all of the following to be within the scope of work:

1. Identification of application, system, and network vulnerabilities and assessment of patching methodologies.
   1. The assessment will be limited to publicly accessible hosts residing in the Agency network segments deemed to be part of the DMZ or Transaction Zones (TZ) that provide shared hosting environments. This includes underlying Network Management and Out of Band zones and segments that provide network communications and services to the publicly accessible hosts. The private addresses or servers will also be in scope, but access will be through other means.
   2. AGENCY network segments in scope for this assessment will be provided upon award of the assessment and will be listed in CIDR notation (x.x.x.x/1, y.y.y.y/2, z.z.z.z/3, etc.). Network segments will be identified as belonging to the LAN, WLAN, VPN NAT pool or publicly accessible hosts in the DMZ and TZ.
   3. Conduct vulnerability scanning and current patching methodology assessment for AGENCY hosts, and end points (desktops and laptops). Scans for servers must be completed outside of normal business hours, 6:00PM to 7:00AM.(or as directed by the agency) Scan activity must be coordinated with the ESRMO prior to it being initiated.
   4. Conduct penetration testing for publicly accessible systems when initial vulnerability scanning identifies potential high impact vulnerabilities. AGENCY and the Vendor together will select the systems for penetration testing during the security assessment engagement.
   5. In the event penetration testing gains access to a system, the testing should assess the ability of the attacker to leverage the system for access to additional systems and networks.
   6. Conduct web application testing based on the current OWASP top 10 listing. There are approximately xx web servers.
   7. An inventory of all applications, data storage devices and systems, and identification and authentication measures.
   8. An inventory of all agency hardware and its operating systems and network management systems.
2. The existing network infrastructure and configuration, including all interconnectivity and supported protocols and network services offered.
3. Publicly-available information and data accessible via agency Web sites. The vendor shall perform a security Assessment against approximately xx web sites that are part of a software as a service deployment with \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
4. Gaps in IT security governance - Review and make recommendations on AGENCY incident management plan.
5. Current vulnerabilities - Review current vulnerability and patching process. Specifics to be supplied to vendor at start of engagement. Make recommendations on best practices to better secure the state.
6. Existing security systems and components, including antivirus, firewalls, and network monitoring. Vendor shall assess current network security capabilities and their ability to identify and potentially stop cyber-attacks, data loss, and misuse of IT resources. These network security resources include firewalls, Intrusion Prevention Systems and end point security applications.

**Proposal Materials to be Submitted**

At a minimum, the Vendor’s Proposal shall include the following items in this specific order and clearly marked as such:

1. A description of the Vendor’s approach to the assessment so the desired results can be achieved, including how they will run their on-site kick-off meeting which will be held in CITY in an AGENCY conference room at a mutually agreed upon date between AGENCY and the awarded Vendor.
2. Resumes of all personnel assigned to perform the assessment. The Vendor shall include the qualifications of the personnel and explain why this is a good match. A resume shall not exceed three pages in length.
3. Cost – This project requires a not to exceed bid amount to complete the assignment and the cost shall be all inclusive of travel expenses and other incidental costs associated with the project. Costs and expenses relating to the preparation of a proposal and its submission are to be borne solely by the Vendor. This security assessment is anticipated to be a large assessment; therefore, the hourly rate shall not exceed the rates provided with the proposal for STC 918A. Costs should be broken down by the sections listed below: 1, 2, 3.
   1. **Single hourly rate** which will apply to all work efforts, regardless of type or complexity. Also, it will apply to all Vendor personnel, regardless of required skill or experience levels. The single hourly rate will cover all costs, including direct and overhead expenses. Travel, per diem and other miscellaneous costs will be absorbed in the single rate. Note: This single hourly rate shall not exceed the rates awarded under STC 918A.
   2. **Number of Hours to Complete the Project** (this number must be the same as provided in the timetable/schedule below).
   3. **Assessment Category** AGENCY believes the assessment is classified as a (Small/Medium/Large) assessment. Vendor must indicate whether this project would be categorized as a small, medium or large assessment based on the requirements stated herein.
4. Vendor personnel assigned to perform the assessment shall sign a Non-Disclosure Agreement.
5. Any other relevant materials the Vendor feels are appropriate.

# Information Security Risk Assessment SOW Deliverables

The awarded Vendor shall conduct the tasks (document review, employee interviews, vulnerability scanning, penetration testing, network packet analysis, architecture reviews and other work as needed) to compile data required to provide a detailed security assessment report which provides AGENCY the requested information in the format noted below based on the project description and scope.

### The awarded vendor shall provide services for the following:

Penetration Testing Services

Penetration testing consists of evaluating the security of the agency’s cyber assets by attempting to gain, with the Agency’s permission as with all services described herein, unauthorized access into the computer system, application, or network. The process involves an active analysis for any potential vulnerability that could result from poor or improper configuration, known and unknown software/hardware flaws, or operational weaknesses in processes and technical countermeasures. The analysis is carried out from the position of an advisory/hacker and involves active exploitation of vulnerabilities where the contracting team attempts to compromise cyber assets. The team shall attempt to gain access and leverage that access to gain additional privileges or access to other hosts throughout the defined scope of the assessment. The Penetration Test service attempts to exploit vulnerabilities that have been identified in an organization’s systems (hosts, applications, database, or other computer related resources). The results of this service shall detail the risk exposure for an agency’s systems and demonstrate how vulnerabilities can be exploited to gain access to their systems. Suggested remediation actions to lower an agency’s risk exposure shall also be provided.

During the penetration test, the vendor’s team shall not delete any live data, make every attempt not to disrupt current operations, and not perform any Denial of Service attacks. The team shall only concern themselves with discovering and exploiting vulnerabilities which provide greater than intended system access to the system or network that is being tested. The vendor shall be limited to the scope identified in the Rules of Engagement with the Agency, even if the test team identifies access to other networks. A data exfiltration test of pseudo PII is an option within the Penetration Test as well.

Network Mapping

The Network Mapping service activity consists of identifying assets on an agreed upon IP address space or network range(s). The vendor shall attempt to determine open ports and services, hosts, servers, and operating systems running on the network. Identified assets during the Network Mapping shall serve as the target and scope of a Network Vulnerability Scan Service.

Vulnerability Scan

The Vulnerability Scan service comprehensively identifies IT vulnerabilities associated with Agency systems that are potentially exploitable by attackers. The results shall provide agencies with guidance on remediation steps to close any identified vulnerabilities and minimize an agency’s attack footprint.

Phishing Assessment [Optional – Agency Discretion]

The Phishing Assessment can include scanning, testing, or both and is part of the 1 week external test. **[Agencies may decide the level of testing performed for the Phishing Assessment]**

* Phishing Scan - The Phishing Scan service measures the susceptibility of an Agency’s personnel to social engineering attacks, specifically email spear-phishing attacks. The vendor team shall generate and send a phishing email to a targeted list of email addresses provided and agreed upon by the Agency. Within the email, a user will be asked to click on a suspicious/malicious link. The team shall be able to track the percentage of users that clicked on the link, providing insight into the effectiveness of a security awareness program or measure the susceptibility of an attack from this vector. During the Phishing Scan, no malicious activity shall be conducted as it is only a metrics gathering technique. The vendor shall ensure firewall rules are in place to accept replies which originate from the Agency network ranges and that replies from non-Agency networks are denied/dropped at the firewall. All testing activities are conducted from an offsite location agreed upon by the vendor and Agency.
* Phishing Test - The Phishing Test will test the response and detection capability of an organization if an attack is successful. The vendor team shall generate and send a specially crafted phishing email to a targeted list of email addresses provided and agreed to by the POC. If a user (victim) happens to accept the email and open the attachment or click on the supplied link, a back end communications channel will be attempted to an attack server. This attack server shall then allow the vendor to communicate with the victim machine. Once the vendor is able to access the victim machine, they shall verify that the victim machine is in the scope of the testing. If the victim machine is not in scope, the vendor shall notify and work with the POC to clean up the victim machine. If the victim machine is in scope, the vendor shall use the victim machine to attempt to discover and exploit additional hosts on the Agency network. This will replicate real-life hacking attacks and security breaches; however the vendor shall be working in coordination with the POC, and be able to report back on how entry was gained, what additional access was gained, and how the connection ended. The vendor shall ensure lab firewall rules are in place to accept replies which originate from Agency network ranges and that replies from non-Agency networks are denied/dropped at the vendor lab firewall.

Wireless Assessment

The Wireless Assessment can include wireless access point (WAP) detection, penetration testing or both and is performed while onsite at the Agency’s facility. Wireless Network Detection will occur during an onsite portion of the assessment. Engineers shall conduct a walkthrough of Agency facilities to identify and evaluate IEEE 802.11 Wireless Access Points (WAPs) that exist within an Agency’s physical office location(s) and work with POC to determine if any rogue access points are in use. Wireless penetration testing analyzes the current wireless infrastructure to identify weaknesses and attempt to exploit them to gain additional access to an Agency network. During the wireless penetration test, the vendor identifies WAPs and attempts to exploit and gain access to the network through those WAPs. Once access is gained to the wireless network, the team shall attempt to map out the network and discover vulnerabilities. This service cannot be performed remotely.

Web Application Assessment

The Web Application Assessment can include scanning, testing or both. The test provides a deep and detailed security look at an application, which is of particular interest to a Agency.

The Web Application Scan service identifies web application specific vulnerabilities and assesses the security posture of selected Agency’s web applications against the Open Web Application Security Project (OWASP) Top Ten common vulnerabilities. The service looks for a wide variety of vulnerabilities such as Cross-Site scripting and SQL injection, service configuration mistakes and errors, as well as specific application problems. The results of this analysis shall detail the risk exposure for an agency’s Web applications and demonstrate how vulnerabilities in these applications can be exploited. Potential operational impacts for testing shall be reviewed with the POC and plans adjusted accordingly. Depending on web application accessibility, assessment activities may be conducted from vendor Test facilities or onsite at a Agency location. Accounts to access a Web Application shall be created by the Web Application Administrators for the vendor to utilize. Suggested remediation actions to lower an agency’s risk exposure shall also be provided.

Operating System Security Assessment (OSSA)

The Operating System Security Assessment (OSSA) service assesses the configuration of select host operating systems (OS) against standardized configuration baselines such as Security Technical Implementation Guides (STIGS). The results identify deviations from State required baselines and recommended remediation steps to bring configurations into compliance. All assessment activities are conducted onsite at the Agency’s location. Administrator or root-level access will be required for this service.

Database Assessment

The Database Assessment determines the configuration of selected databases against configuration baselines in order to identify potential misconfigurations and/or database vulnerabilities. For example, the service will attempt to identify holes, weaknesses and threats to the information stored within the database. The vendor shall identify default usernames and passwords, perform a limited User Rights Review (URR), identify patch-management issues, and review various other security vulnerabilities and configuration problems. The results identify deviations from baselines, if applicable, as well as insecure configurations that are applied on assessed databases. In addition, recommended remediation actions shall also be provided. All assessment activities are conducted onsite at a customer location or over a secure connection the customer has initiated with the testing team. As part of the service, a DBA username and password with admin privileges are required.

The Vendor shall provide a written report demonstrating the comprehensive review that was performed utilizing the following outline as a sample document construct:

* 1. Executive Summary
  2. Assessment Methodology and Approach
  3. Detailed Reporting of:
     1. Identified gaps in information security governance through examination of existing Statewide policies and state statutes
     2. A Matrix of discovered vulnerabilities and recommended remediation or mitigation strategies
        1. Details of the vulnerabilities by host or node risk ranked by criticality (high, medium, low)
           1. Detailed description
           2. Status of external exposure (i.e. publicly accessible)
           3. Verification of vulnerability
           4. Mitigation Recommendation
     3. Specific results of penetration testing on selected systems
     4. Identified gaps surrounding current patching strategies and tools
     5. Identified gaps in network security firewalls, IPS and monitoring capabilities and recommended strategies to identify
     6. Identified misconfigurations and potential breaches found through examination of network traffic
  4. Conclusion
     1. General summary of the findings by areas and by NIST 800-53 rev 4 security control (e.g. SI-2 and control descriptor)
     2. Overall summary of the security posture of AGENCY
     3. Prioritization and recommended remediation plan with estimated costs to address overall assessment results
        1. Short Term
        2. Long Term
  5. Appendices
     1. List of tools used in the performance of the assessment
     2. Screen captures, logs and other supporting documentation

AGENCY reserves the right to have the Vendor present the written report at least once to Agency management.

# Timetable/Schedule

The Vendor must provide with their SOW a timetable for completion for the security assessment requested in this SOW. Vendor must provide the number of hours required to complete the project. The assessment must begin within two weeks after the SOW is awarded.

**Execution of Statement of Work**

By signing below, the Vendor certifies that:

* this SOW Response was signed by an authorized representative of the Vendor
* this SOW is subject to all terms and conditions of STC 918A
* the undersigned Vendor offers and agrees to furnish the services set forth in the SOW, if accepted by the State.

**Failure to execute/sign SOW response prior to submittal shall render it invalid.**

|  |  |  |
| --- | --- | --- |
| VENDOR: | E-MAIL: | |
| STREET ADDRESS: | P.O. BOX: | ZIP: |
| CITY & STATE & ZIP: | TELEPHONE NO | TOLL FREE NO |
| TYPE OR PRINT NAME & TITLE OF PERSON SIGNING: | FAX NUMBER: | |
| AUTHORIZED SIGNATURE: | DATE: | |

**ACCEPTANCE OF STATEMENT OF WORK**

If any or all parts of this SOW are accepted, an authorized representative of AGENCY shall affix their signature hereto and this document along with the provisions of STC 918A shall then constitute the written agreement between the parties. A copy of this acceptance will be forwarded to the successful Vendor(s).

|  |
| --- |
| **FOR AGENCY USE ONLY** |
| Offer accepted this day of , 20 , as indicated on attached certification or purchase order, |
| by \_(Authorized representative of AGENCY) |