### **1.0** **INTRODUCTION**

In coordination with the Arizona National Guard Cyber Joint Task Force (AZNG-CJTF) and the State of Arizona to conduct a network and web assessment.

Entity being assessed: ***NAME OF PARTICIPATING SCHOOL DISTRICT***

### **2.0** **CONTACT INFORMATION** – *contact phone numbers and email addresses for the main network/information technology point of contact during the engagement.*

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Title | Email | Phone |
|  | (e.g. Chief Information Officer) |  |  |
|  |  |  |  |

### **3.0 INTERNAL NETWORK SCOPE** – *the internal IP addresses and ranges that will be scanned and tested.*

|  |  |
| --- | --- |
| IP Subnet Range | Location: Cloud, SHDC, On-Prem,etc |
|  |  |
|  |  |
|  |  |

###

### **4.0 ACCESS MACHINE AND CREDENTIALED INFORMATION** – *If the assessment is being performed remotely, provide VPN, Network, and Web Application credentials to access internal ranges. Access information will be sent to the individuals conducting the assessment:***4.1 VPN Accounts:** *For accessing the internal network remotely.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | EIN: | Title | Email | VPN Account: |
| Jeremy Sanchez |  | Lead Cyber Team Operator | jeremy.sanchez@arizona.gov |  |
| Brett Woods |  | Cyber Team Operator | brett.woods@arizona.gov |  |
| Ronnie Marquez |  | Cyber Team Operator | ronald.marquez@arizona.gov |  |

**4.2 Privileged Domain Account:**  *For scanning the environment and providing the best possible analysis for the organization.

By default, Windows will assign new local accounts guest privileges if they are logged into remotely. This prevents remote vulnerability audits from succeeding. Please do not increase the amount of access that the Guest users obtain. This reduces the security of your Windows server.*

|  |  |
| --- | --- |
| Privileged Domain Account: | Email credentials were sent to: |
|  | jeremy.sanchez@arizona.gov |

**4.3 Web Application Credentials:**
*For accessing and scanning the Web Application.*

|  |  |  |
| --- | --- | --- |
| Web Application: | Account: | Email credentials were sent to: |
|  |  | jeremy.sanchez@arizona.gov |
|  |  | jeremy.sanchez@arizona.gov |

 **4.4 Assessment Machine:**

**Option 1:** Whitelist Assessment Machine *The assessment will be conducted using a specified machine from the Arizona Department of Homeland Security (AZDOHS). In order for this machine to access the environment, a few changes need to be made on your Firewall.*

*The machine’s IP (****159.87.132.40)*** *would need to be allowed through the firewall with the following ports opened:*

|  |
| --- |
| *Incoming TCP Port 22* |
| *Incoming TCP Port 8834* |
| *Outgoing TCP Port 25* |
| *Outgoing TCP Port 389* |
| *Outgoing TCP Port 443* |
| *Outgoing TCP Port 3128* |
| *Outgoing UDP Port 53* |

**Option 2:** Provide an Assessment Machine
 *If the organization would not like to whitelist the AZDOHS machine, please provide a computer with the proper resources allocated to it. The machine must include:*

* *CPU: 4 2GHz cores*
* *Memory: 32 GB RAM*
* *Disk space: 100 GB, not including space used by the host operating system*
*IP address of the resource provided:*

|  |
| --- |
|  |

### 5.0 **EXTERNAL NETWORK SCOPE** – *The external IP addresses and ranges that will be scanned and tested.*

|  |  |  |
| --- | --- | --- |
| Web Application Name | Web Application Production URL | Web Application UAT or DEV URL |
|  |  |  |
|  |  |  |
|  |  |  |

### 6.0  **DATE RANGE** - *The dates of engagement.*

|  |  |
| --- | --- |
| Date: | Time Window: |
|  |  |

###

### **7.0 Network Penetration Testing**

*The AZNG-CJTF will perform internal and external network penetration testing to identify and test network and host-based security vulnerabilities within the Internet-facing networked infrastructures operated by the* ***NAME OF PARTICIPATING SCHOOL DISTRICT****. This testing is to be performed by the members of AZNG-CJTF utilizing various software tools that are licensed and/or authorized for use by the AZNG-CJTF. At minimum, the internal and external network vulnerability assessment and testing must include the following phases:*

* Active Host Identification (Device Discovery) - AZ-CJTF will establish a profile of Internet Protocol (IP) ranges provided by the ***NAME OF PARTICIPATING SCHOOL DISTRICT***to identify active internal and external devices but shall not exceed within the scope of the subnet provided.
* Vulnerability Scanning - AZNG-CJTF will analyze available network services and the IP Stack fingerprints of all active external devices identified in the device discovery phase
* Vulnerability Validation - AZNG-CJTF will attempt to validate the results of vulnerability scanning to identify and disregard any false-positive results; and validate other positive results from automated testing.
* Exploitation - After establishing an understanding of external device roles, potential trust relationships, accessible network services, and potential vulnerabilities, AZNG-CJTF will attempt to gain access to target systems
* Post Exploitation - After completing the exploitation phase and achieving access to any vulnerable hosts and data, AZNG-CJTF will attempt to escalate privileges on any exploited host(s). AZNG-CJTF will attempt to leverage this access and access to data (i.e. password hashes and authentication tokens) on these hosts to gain additional access into the ***NAME OF PARTICIPATING SCHOOL DISTRICT***network (as applicable and within scope) and attempt to access additional systems and data.
* Re-testing - AZNG-CJTF recommends a follow-on scan in six months of completion of the original scan for devices that are identified as having a risk rating (or severity) of medium or higher as classified by automated scanning tools or AZNG-CJTF risk assessment methodology. Re-testing of vulnerabilities should begin no sooner than 60 days after completion of all phases of the network penetration testing engagement

### **8.0 Web Application Assessment**

*AZNG-CJTF is to provide web-application specific penetration testing in addition to external network penetration testing. AZNG-CJTF will perform web-application security testing of the* ***NAME OF PARTICIPATING SCHOOL DISTRICT*** *Internet-facing web-applications through unauthenticated and automated web application scanning. Testing is to be performed by Qualified Cybersecurity Professionals utilizing various web application assessment and exploitation techniques that must include but will not be limited to the following methods:*

* Input Validation Bypass – AZNG-CJTF will remove client-side validation routines and bounds checking restrictions to confirm controls are implemented on application parameters sent to the server.
* SQL Injection – AZNG-CJTF will submit specially crafted SQL commands in input fields to validate input controls are in place for the protection of database data.
* Cross-site Scripting – AZNG-CJTF will submit active content to the application in an attempt to cause a user's web browser to execute unauthorized and unfiltered code. This test is meant to validate user input controls.
* Parameter Tampering - AZNG-CJTF will modify query strings and parameters and hidden fields in an attempt to gain unauthorized access to user data or application functionality.
* Forceful Browsing – AZNG-CJTF will enumerate files located on a web server in an attempt to access files and user data not explicitly shown to the user within the application interface.
* Backdoors and Debug Options – AZNG-CJTF will identify code left by developers for debugging purposes that could potentially allow an intruder to gain additional levels of access.
* Configuration Subversion – AZNG-CJTF will assess the ***NAME OF PARTICIPATING SCHOOL DISTRICT*** web servers and application servers for improper configurations that could create attack vectors.
* Re-testing - AZNG-CJTF recommends a follow-on scan in six months of completion of the original scan for web-application specific vulnerabilities that are identified as having a risk rating (or severity) of medium or higher as classified by automated scanning tools or AZNG-CJTF’s risk assessment methodology. Re-testing of vulnerabilities should begin no sooner than 60 days after completion of all phases of the web-application testing engagement.

### 9.0  **REPORTING**

*The deliverable reports for both network and web application will be generated to provide the result of the scan.*Shall include, at a minimum:

* Executive Summary
* Information Security risks including vulnerabilities, exploits, and severity
* Recommended actions for remediation

### 10.0  **EXCEPTIONS**

*Any exceptions to the above information, including IP Addresses or URLS not to be scanned, days or times of day to avoid testing, and any other details that might be construed to belong to one of the above categories, but which is not to be assessed as part of this engagement are listed below:*

|  |
| --- |
| ***Exception List - Any Devices, IP’s, URLS, or ranges that should not be scanned, tested or are otherwise OUT OF SCOPE*** |
|  |
|  |
|  |

As the agency representative authorized to enter into this agreement, **I AGREE** to the scope of work for the ***NAME OF PARTICIPATING SCHOOL DISTRICT***.

**SIGN HERE**

**TITLE**