IT Cybersecurity Risk Assessment

SUMMARY OF WORK

1. **Project Description**
    a. The State Commission Information Technology Group is undertaking a project to perform a cybersecurity risk assessment of its Information Technology (IT) network.
    b. This Scope of Work is to be used to define Contractor expectations. All items noted in this Scope of Work shall be addressed in the Contractor's proposal. Any items not specifically noted as "by Owner" shall be assumed to be by Contractor.
    c. There are currently two networks and 3 VLAN networks in the main office. These networks are the following:
        i. SilverNet
            1. State Information Technology (IT) Network
            2. Connected to approximately 40 computers and other devices.
        ii. CoxNet
            1. Internet facing network.
            2. DMZ Zone
        iii. VLAN Networks
            1. Guest Wi-Fi
            2. IoT Network
            3. Surveillance Camera
    d. Our Power Delivery Group (PDG) computers, network and equipment are under a separate contract for risk analysis. The employees are included in this contract.
2. **Project Objective**
    a. The objective of this project is to comprehensively identify potential risks to our existing networks in their current configuration and provide a summary report with actionable solutions identified for management with estimated solution complexity, costs, and timelines for implementation.

3. **Scope of Work**
    a. The assessment should include information security guidance that is aligned with industry standards, best practices and methodologies outlined in the National Institute for Standards and Technology (NIST), Cyber Security Framework (CSF), and any other applicable standards.
    b. The following shall be performed as a part of the risk assessment:
        i. Preliminary Network Mapping
            1. The contractor shall perform their own mapping of the network prior to the start of penetration and perimeter testing.
            2. This shall include on-site visits for discussions with the various stakeholders and collection of pertinent data whether it be drawings or in field data collection.
            3. All testing and reporting shall be done referencing this network document.
            4. At the end of the project this document should be finalized and issued to Owner as a Visio file as well as a PDF.
        ii. Penetration Testing
            1. Includes the entire perimeter and any critical systems, this includes both the internal (LAN to LAN) and external (public- facing) perimeters.
        iii. Perimeter Testing
            1. Includes the entire perimeter and any critical systems, this includes both the internal (LAN to LAN) and external (public- facing) perimeters.
            2. Firewalls, authentication servers, etc. should be included in the testing.
            3. Perform an in-depth cybersecurity vulnerability assessment and penetration testing of infrastructure of Internal network – all internal systems including routers, switches, physical and virtual servers, data storage infrastructure, and public computers and other connected IT devices: including all Demilitarized (DMZ) systems to include flow of controls from external and internal systems.
                a. External network - all external public-facing systems including firewalls, FTP, web servers, and web service interface points.
            4. Enumerate systems on the network and validate them against known systems. Identify any unknown or unexpected systems.

5. Identify, analyze, and confirm vulnerabilities. It is expected that qualified Contractor personnel will know how to look deeper into potential vulnerabilities for other security holes, misconfigurations, and other problems to follow the vulnerability to its end. It is expected that the Contractor will share method and process (i.e., e-mail's screen shots, files, etc.) of successful penetration in addition to a list of open ports, missing patches, or possible vulnerabilities.
6. The Contractor shall conduct security risk assessment scans on mission-critical applications. All vulnerabilities reported as Critical/High shall be detailed in the 'Findings' section of the final deliverable. A complete list of vulnerabilities shall be provided in a separate appendix. Each vulnerability or risk identified shall be categorized as a Critical/High, Medium, or Low.
7. User Privilege Escalation: Throughout the assessment, the Contractor shall attempt to complete user privilege escalations in order to further compromise, or demonstrate the effectiveness of, the security of established controls within Owner's environment. This testing will assist in determining if access control systems are effectively enforcing user access and permission levels are configured correctly based on job function.
8. Segmentation Testing: The Contractor shall test the segmentation controls of all segregated network segments from a sample of completely isolated/segmented networks (ensuring that each type of segmentation point is represented, such as firewalls, VLAN on switch, etc.).
9. Wireless Scanning (both private and guest): The service provider shall identify rogue wireless devices and additional security architecture weaknesses related to the wireless networks.
10. Applications
    a. Provide authenticated application vulnerability scanning and penetration testing the security service provider will conduct security risk assessment scans on external facing applications.
    b. Identify application security vulnerabilities and perform active exploit through identified vulnerabilities (Note: Exploit should stop at the point of proof of compromise but not causing any business interruption).

11. Look for erroneous configurations that may lead to information leaks, theft of data, or even intrusion and denial of service attacks.
12. Brute Force Attack: The Contractor shall conduct a brute force attack to check for weak passwords. The objective of this test is to confirm whether passwords are meeting security best practices.
13. Social Engineering (Phone and E-mail): During the Social Engineering phase of the assessment, the Contractor shall attempt to impersonate and persuade Owner employees via telephone and/or e-mail to disclose proprietary information. This information may allow the service provider to access sensitive information and/or exploit the integrity and/or availability of data. The sophisticated methods that may be utilized are, but not limited to, as follows:
    a. Phishing/spear phishing Attacks – Sending an e-mail to a user falsely claiming to be an established legitimate organization in an attempt to scam the user into surrendering company sensitive/ information. The overall objective here is to measure end-user response to phishing, spear phishing, spam, and other email threats.
    b. Employee Impersonation – Calling employees and attempt to convince them to release sensitive information (e.g., passwords of systems, unpublished e- mail addresses, names of other employees, names, and virtual locations of systems).
    c. Pretexting – This method is the act of creating and using an invented scenario to persuade a targeted victim to release information or perform an action and is typically done over the telephone. It is more than a simple lie as it most often involves some prior research or set up and the use of pieces of known information (e.g., for impersonation: date of birth, Social Security Number, last bill amount or other specific company information to establish legitimacy in the mind of the target).

iv. Once the risk assessment and testing has been completed, the Contractor must remove all backdoors, software, and personnel access utilized for the project, and scrub any trace of test from the Owner's infrastructure.

4. Required Deliverables

a. Cybersecurity Risk Assessment Report

i. Executive Summary

1. Overall Report Results
2. Key Risk Areas
3. Maturity level score card against NIST CSF
4. Strategic Recommendations

ii. Report Details

1. Assessment Methodology
2. Detailed assessment results in both written and spreadsheet (Excel) format.
3. Detailed score card for each NIST CSF subcategory

iii. Recommendations

1. Risk Assessment
    a. Immediate remedies
        i. Should identify issues that are simple to implement and will have a positive impact on NIST scoring.
        ii. Should be presented in a risk-ranked format with complexity, cost, and timeline rankings
    b. Long-term remedies
        i. Should identify issues that are complex to implement, require funding sources to be secured, and will have a significant positive impact on NIST scoring and the overall health of the Owner's system.
        ii. Should be presented in a risk-ranked format with complexity, cost, and timeline rankings

iv. Project Plan

1. Identification of security projects based on individual or combined remedies as noted above in the recommendations section, with detailed activities and action plans.
2. Should include at a minimum the following:

a. Project Description
b. Priority (based on NIST benefit impact)
c. Risk Rank
d. Complexity
e. Cost
f. Timeline

b. Network Mapping
    i. Utilize drawing in references inside the report for consistent and agreed upon network perimeters
    ii. Visio File of Network Map
    iii. PDF File of Network Map