Security Posture Assessment
For New Mexico State Government

Security assessments shall be a comprehensive evaluation of New Mexico State entity’s current network and computing environment. Safeguarding information and ensuring confidentiality, integrity, and availability of this information within an environment of increasingly sophisticated security threats requires a strong, enterprise-wide information security program validate by a reputable third party security assessment.

The Team security experts shall provide New Mexico State Entity (NMSE) executives, managers, and information technology personnel (IT staff) with a global view of the information security posture of New Mexico State Entity (Figure 1: System Security Assessment Coverage) through the following:

- An understanding of current vulnerability threat pairs of information systems of NMSE;
- Will assist NMSE in identifying its weakest link before an intruder does;
- Assessment findings in detail sufficient to permit NMSE to prioritize and enhance required information security mechanisms;
- Assessment findings of NMSE’s current information security posture based on Federal Institution’s Guidelines and the Health Insurance Portability and Accountability Act (HIPAA);
- Assessment findings of NMSE’s current information security posture based on internationally recognized International Organization for Standardization (ISO) 27002 standards and best practices;
- Information Security Audit as per standard federal institution’s guidelines;
- Recommendations for requirement traceability matrix to mitigate current threats and achieve baseline security for **High-Impact systems**;
- Complete coverage (assessment shall be performed on all systems within a state entity) not just sampling;

![Figure 1 Systems Security Assessment Coverage](image-url)
1. **Security Posture Assessment Methodology**

The Team’s assessments should be comprehensive and based on proven methodologies. Assessment shall be performed using redundant benchmark assessment tools to ensure cross-validation and uniformity of process and consistency of results. The assessment effort will be divided into three major categories: internal, external and remote assessment.

Assessments shall include the operations, processes and technologies associated with directly defending against interruption, interception, modification, and fabrication to the NMSE network, information systems and information operations. To ensure complete information security posture assessment, the process will include analysis and review of policies, information systems, network peripherals, information security devices (firewalls, intrusion prevention and detection systems), remote access services, wireless access points, printers, back-up systems, log management systems, voice over IP systems, disaster recovery techniques and physical security.

2. **Services to be Performed**

   **A. Network Vulnerability Analysis**

   - **Network posture assessment**
     A review of NMSE network architecture to determine how it effectively isolates untrusted outside networks from gaining access to NMSE’s internal, trusted networks and information
     - Review of current network architecture and analysis of individual nodes, servers, and peripherals
     - Assessment of current authentication methods (user and hardware perspective)
     - Network topology review and assessment of current services
     - Critical node assessment for failover analysis

   - **Review all communication channels, protocols, and data flow**
     A review of NMSE network design and implementations to determine how effectively it isolates insiders based on their roles and need to access NMSE’s information resources:
     - Data flow analysis
     - Assessment of physical and logical connections
     - Network Assets inventory and classification
     - Protocols used for communication
     - Dial-in and remote connection assessments

   - **Security posture assessment**
     A thorough review of security controls of NMSE covering policy, processes, procedures, people, access controls, network, communications, systems and compliance from inside, remote and outside:
     - Perimeter analysis
     - External analysis
     - Internal analysis
     - Remote connection analysis
       - Remote access services and virtual private network analysis
     - Application service providers and trusted networks analysis

*This proposal contains proprietary and confidential information.*
Applications Security Review
- Analysis of potential vulnerabilities, threats and attacks to NMSE’s web applications
- Analysis of information leakage using popular search engines
- Analysis of Input validation, access controls, and review of password policies
- Analysis of HTML TRACE support

B. Penetration Testing and Analysis

Penetration testing
A test designed with an adversarial intent to gain unauthorized access to portions of NMSE’s network from the perspective of a trusted user and adversary from inside, remote and outside.
- Perform reconnaissance and penetration testing on the network from internal nodes, remote nodes and external nodes
- Perform analysis on possible secondary exploits
- Red teaming refers to the work performed to provide an adversarial perspective
- Perform analysis and review of remote connection services (remote access servers, virtual private networks, terminal services, etc.)

Analysis of penetration test performed
- Basic attack mapping analysis and attack trees
- Analysis of data integrity compromises
- Risk matrix of the discovered vulnerabilities

C. Verification of Systems Security Requirements

System access control
- Review NMSE’s access control mechanisms
- Access and review the type of software used (commercial, common operating system)
- Review logon failure procedures and policies
- Review and assess access control techniques that utilize personal identification numbers (PIN) and passwords (or biometrics)
- Review of management controls and oversight of the function of issuing and maintaining access control to PINs and Passwords

Monitoring and anomaly detection
- Review and assess system design for online access to NMSE’s information-includes monitoring and anomaly detection capabilities
- Review, access, and test the capability of the monitoring and anomaly detection systems to detect and mitigate unauthorized access to systems and information
- Review and assess reports generated by the monitoring and anomaly detection systems

Security awareness
- Review and verify security awareness training procedures for employees
- Review of security awareness training materials
- Proper use of information and systems
- Proper protection of NMSE’s information
D. Recommendations for Security Enhancement

- **Internal and external security standards and practices**
  - Develop requirement traceability matrix and recommend baseline user training
  - Assist in developing forms and procedures for incident reporting and response

- **Perimeter defense and network performance enhancement**
  - Map required or preferred tools to current vulnerabilities
  - Recommend/install patches and protection mechanisms for the identified vulnerabilities
  - Recommend/develop/review rules for the new security technologies procured
  - Recommend/design enhanced network architecture

3. Deliverables

A. Security assessment executive summary

B. Security posture assessment approach

C. Snapshot of current information security
  - Consolidated report of all the scanners
  - Top 5 vulnerable hosts
  - Top 5 vulnerable subnets
  - Summary of high, medium and low vulnerabilities

D. Security posture assessment
  - External security posture, internal security posture, and remote security posture
  - Network topology (external, remote and internal)
  - Application and web security
  - Desktop security (sampling)

E. Penetration testing summary
  - SANS Top 20
  - Analysis of top 10 target ports (by reports, source, destination)
  - Attack types and attack methods used
  - Common hacker techniques
  - Data integrity analysis

F. Information Security Audit as per Standard Federal Institutions Guidelines (Summary)
  - Health Insurance Portability and Accountability Act (HIPAA)

G. Recommendations
1. How many years have you been providing these types of security services?

2. What percentage of your business is derived from these security services?

3. How many customers do you have in this security sector?

4. What percentage of that staff has security certification to perform this type of work? And what are their certifications?

5. What is your average number of years and overall experience in performing vulnerability scanning penetration testing? How about social engineering?

6. What are the average number of years and overall experience with dial-in/RAS security testing?

7. Please explain the process of initial and ongoing training of your security monitoring staff.

8. Provide a brief overview of your security services as it relates to this scope of work.

9. Please provide a list of supporting products to conduct security testing.

10. Explain how you will complete an assessment to include specific information on your implementation timeline, infrastructure requirements, and other related items.

11. Do you use third parties to provide your service? If so, then explain the services they provide and how you ensure the quality and availability of those services.

12. Please provide an example of how your services detected and addressed a recent security incident.

13. Will your service require the use of proprietary technology that NMSE must purchase or install? If so, then please list all pertinent information related to this technology, including hardware, software, networking, middleware and database requirements.

14. Explain how you use external data to analyze potential threats to NMSE’s environment.

15. Explain your methodology for reducing false positives/negatives and for classifying security-related events that represent a risk to NMSE.

16. Provide details on your methodology for collecting and analyzing vulnerability and intrusion data.