SAN JOAQUIN VALLEY AIR POLLUTION CONTROL DISTRICT
REQUEST FOR PROPOSALS

Cybersecurity Risk Assessment

Table of Contents

INTRODUCTION

The San Joaquin Valley Air Pollution Control District (SJVAPCD) invites qualified parties to submit proposals for the services outlined in this Request for Proposal (RFP), in accordance with the terms and conditions provided. For the purpose of this RFP, the terms "Proposer," "Contractor," "Consultant," "Bidder," and "Firm" may be used interchangeably.

SJVAPCD seeks proposals from qualified third-party service providers to conduct a comprehensive cybersecurity risk assessment and penetration testing. This RFP outlines the proposed services' general objectives, scope, and requirements. The vendor's proposal is expected to address all of the items defined in Section V of this RFP. SJVAPCD reserves the right to adjust the project's final scope as deemed necessary.

The selected vendor will provide SJVAPCD with a detailed report summarizing the findings, identified risks and vulnerabilities, and recommendations for improvement and compliance. This report will serve as a roadmap for prioritizing and addressing cybersecurity risks that align with SJVAPCD's strategic objectives and compliance obligations.

SJVAPCD requires a meticulous and thorough cybersecurity risk assessment that transcends traditional technical evaluations and includes a holistic examination of our cybersecurity posture that leaves nothing off the table. This comprehensive assessment aims to identify vulnerabilities, assess risks, and recommend actionable strategies to mitigate identified threats, thereby enhancing our resilience against cyber threats and ensuring compliance with applicable standards, including The Federal Information Security Management Act (FISMA) and relevant National Institute of Standards and Technology (NIST) Special Publications.

The scope of the Comprehensive Security Assessment includes, but is not limited to, the following key high-level umbrella components:

- Technical Vulnerability Assessment: An in-depth analysis of external and internal network infrastructure, applications, and systems to identify vulnerabilities that adversaries could exploit.
- FISMA Compliance Assessment, identifying the level of compliance in all areas including:
    - Information System Inventory:
        - Evaluate the information system inventory against the requirements of the Federal Information Processing Standards (FIPS) publication 200 to ensure comprehensive and accurate accounting of the agency's assets, examining the processes for maintaining this inventory in line with NIST Special Publication (SP) 800-53, Control CM-8 (Information System Component Inventory).
    - Risk Categorization:
        - Assess the agency’s risk categorization against FIPS 199 standards to confirm that systems are categorized based on the potential impact of security breaches and validate that the process follows guidance from NIST SP 800-60.
    - Security Controls:
        - A rigorous evaluation of the existing security controls against the NIST SP 800-53 standards to ensure they are appropriately implemented and effectively mitigate identified risks.
    - Risk Assessment:

        - Analyze the risk assessment process to ensure compliance with NIST SP 800-30, verifying that the agency systematically identifies, evaluates, and plans to mitigate risks.
    - System Security Plan:
        - Review all SSPs to confirm it comprehensively outlines the security controls, consistent with NIST SP 800-18 (Guide for Developing Security Plans for Federal Information Systems).
    - Certification and Accreditation
        - Verify the certification and accreditation process to ensure it meets the NIST SP 800-37 standards, which provide guidelines for applying the Risk Management Framework to federal information systems.
    - Continuous Monitoring
        - Evaluate the effectiveness of the continuous monitoring program, ensuring it is aligned with the guidelines of NIST SP 800-137 (Information Security Continuous Monitoring).

SECTION I: BACKGROUND/INFORMATION

SJVAPCD consists of eight counties in California's Central Valley: San Joaquin, Stanislaus, Merced, Madera, Fresno, Kings, Tulare, and the San Joaquin Valley Air Basin portion of Kern.

SJVAPCD is a public health agency whose mission is to improve the health and quality of life for all Valley residents through efficient, effective and entrepreneurial air quality management strategies. Our Core Values have been designed to ensure that our mission is accomplished through commonsense, feasible measures that are based on sound science.

The Valley Air District is governed by a fifteen-member Governing Board consisting of representatives from the Board of Supervisors of all eight counties, one Health and Science member appointed by the Governor, one Physician appointed by the Governor, and five Valley city representatives.

To embrace the challenge of the changing threat landscape and environment, SJVAPCD is on a cybersecurity maturity journey to align with the industry cybersecurity framework/practices to ensure the availability, integrity, and confidentiality of SJVAPCD's information systems and data.

The San Joaquin Valley Air Pollution Control District (SJVAPCD) operates a comprehensive technological infrastructure to support its air quality management mission in the Central California San Joaquin Valley, including:

- A wireless network with 36 Wireless Access Points (WAPs) for coverage across various locations.
- Wired ethernet utilized in all main offices for the majority of LAN links to endpoints.
- Two pathways for connectivity between three main sites: a Virtual Private Wire Service (VPWS) link at 1000Mbps and a site-to-site VPN tunnel using AT&T fiber at 1000Mbps at the main Fresno site and 100Mbps connections at the two smaller sites.
- Approximately 90 network hardware devices comprising the infrastructure, including firewalls behind every WAN connection.

- Remote unmanned networks connecting to the main network using cellular static IP WAN links, including 25 regulatory and 29 community monitoring stations that actively share data back to the main Fresno site over the public internet.
- A voice network with over 300 endpoints for supporting internal and external communications.
- Over 400 Windows workstation endpoints in use.
- A server environment featuring over 120 endpoints, primarily on VMware hypervisor systems, configured with about 90% Windows servers and 10% Linux servers.
- Server rooms at each of the three main sites, equipped with keycard access, climate control, fire suppression, and KVM consoles requiring credentials for access.
- A dedicated, climate-controlled room at each main site for a site-wide UPS system supporting each server room directly.
- Physical security measures for backup tapes and license documents.
- A mix of services, the vast majority of which are hosted on-prem, with a few provided via SaaS providers.
- Local County DMV system access via Horizon View clients on dedicated workstation systems.
- Identity management handled using Microsoft Active Directory.

SECTION II: CONTACT PERSON:

Questions regarding the content of intent of this RFP or procedural matters should be addressed via e-mail to **Imtiaz.Haq@valleyair.org**

Imtiaz Haq, Director of Information Systems
SJVAPCD
1990 E. Gettysburg Ave.
Fresno, CA 93726
(559) 230-6047
Imtiaz.Haq@valleyair.org

SECTION III: SCHEDULE OF EVENTS

Date	Event
8-May-24	RFP Released
15-May-24	Bidder's Conference
20-May-24	Proposals Due to SJVAPCD - No Later Than 1:00 pm
20-May-24 – 27-May-24	Proposal Evaluations
28-May-24	References Follow Up
30-May-24	Vendor Selection/Contract Release
20-June-24	Anticipated Contract Execution

It is not mandatory for prospective vendors to attend the Bidder's Conference in order to submit a proposal and receive serious consideration. However, the SJVAPCD assumes

no responsibility for advising non-attendees regarding specific details provided during this meeting. The Bidder's Conference will be held via Zoom conference at 10:00 am on Wednesday, May 15, 2024. Please contact **Tim Van Dyne** at **Tim.VanDyne@valleyair.org** by the close of business on Tuesday, May 14, 2024, if you plan to attend. The conference link will be shared with the vendors who RSVP'd to attend.

SECTION IV: SCOPE OF WORK/DELIVERABLES

Objective:

This section outlines our objective to secure a detailed and actionable cybersecurity risk assessment and improvement plan from a reputable 3rd party vendor, adhering strictly to NIST standards and FISMA requirements. The service provider will be expected to deliver a thorough audit of our cybersecurity practices across various facets such as policy adherence, security controls, maturity assessment, and incident response capabilities. Through identifying and addressing critical security deficiencies, the project aims to substantially elevate the SJVAPCD's existing security measures and regulatory compliance.

Essential deliverables, including an executive summary, comprehensive findings report, step-by-step remediation roadmap, action plan prioritizing proposed security enhancements, and presentation for organizational stakeholders, will ensure actionable insights and a clear direction for advancing the organization's cybersecurity maturity and resilience.

FISMA Compliance Requirements

The FISMA mandates comprehensive guidelines and requirements for the security of federal information systems and data. As an entity required to comply with FISMA, the SJVAPCD seeks to ensure its cybersecurity framework adheres strictly to the standards set forth by this act. This RFP invites proposals from vendors skilled in evaluating and enhancing information security frameworks to meet the stringent requirements of FISMA compliance.

This RFP seeks proposals from vendors with demonstrated expertise in evaluating and enhancing information security frameworks within the context of FISMA compliance. The selected vendor will be expected to conduct an exhaustive cybersecurity risk assessment and penetration testing across all relevant information systems. This encompasses a thorough review and analysis of existing security measures, identification of vulnerabilities, and recommendation of remediation strategies to fortify the SJVAPCD's cybersecurity posture against potential threats.

The successful proposal will address key components of FISMA compliance and integrate the following elements into a cohesive security assessment framework:

- **System Security Plan (SSP)**: Development or update of SSP to accurately represent the security measures for protecting information systems.
- **Information System Inventory**: Strategies for creating and updating a comprehensive inventory of all information systems, detailing network boundaries and system connections.
- **Data Categorization**: Utilizing NIST SP 800-60 and FIPS 199 for risk level categorization to inform risk management and security control decisions.
- **Risk Assessment**: Frameworks for thorough evaluation and prioritization of potential threats and vulnerabilities.

- **Accreditation & Certification**: Procedures in line with NIST SP 800-37 for the verification of security controls.
- **Continuous Monitoring**: Programs for ongoing security assessments to maintain compliance and identify risks.
- **Annual Review**: Protocols for annual evaluations to verify the effectiveness of information security policies and practices.
- **Security Controls**: A set of controls from NIST SP 800-53, 800-171, 800-30, 800-37, 800-64, 800-160, and 800-39 to protect information systems and data.

The successful proposal will demonstrate a comprehensive approach to FISMA compliance, integrating these elements into a cohesive security assessment framework. By aligning with FISMA's rigorous standards, the SJVAPCD aims to enhance its information systems' overall security and resilience against emerging cyber threats by embracing its compliance requirements.

SJVAPCD Responsibilities

The SJVAPCD specific responsibilities include, but are not limited to, the following:

a. Providing the service provider access to documents deemed by the SJVAPCD to be in-scope for the engagement.
b. Designating a Point of Contact (PoC) exclusively to work with the contractors POC to facilitate focused discussions and timely decision-making.
c. Providing site access to all locations deemed to be in-scope for the engagement during regular business hours (Monday through Thursday, 7:30am-5:30pm, and alternating Fridays, 8:00am-5:00pm),
d. Specifying if any endpoints or services are to be omitted from certain types of testing processes.

Service Provider Responsibilities

The service provider will be responsible for tasks as necessary to fully implement this project, including, but not limited to, the following:

a. Performing total project management, including overseeing and coordinating with the SJVAPCD and others carrying out portions of the project.
b. Designating a Point of Contact (PoC) exclusively for SJVAPCD to facilitate focused discussions and timely decision-making.
c. Working closely with SJVAPCD's designated Point of Contact (PoC) to ensure seamless coordination and information exchange.
d. Ensuring that all legal requirements relating to the project are met, including obtaining necessary permits, licenses, and permission where applicable.
e. Ensuring all assessment activities, including vulnerability scanning, targeted or open-ended penetration testing, and anything that could impact business as usual, will be conducted strictly within timeframes approved by SJVAPCD to minimize impact on operational continuity and service availability.

Minimum Scope Objectives in Major Areas:

External & Internal Vulnerability Assessment and Penetration Testing

Scope:

The process should involve Black Box testing initially, followed by White Box testing, in order to achieve a relevant view of both perspectives. This exercise should include, *but not be limited to*:

- **Phase 1: Black Box Testing**
  - Discovering publicly accessible systems, applications, and services.
  - Identify potential vulnerabilities in the infrastructure, including web applications, email servers, DNS servers, etc.
  - Conduct manual testing techniques to validate automated scan results and identify logical flaws that automated tools may miss.
  - Perform social engineering tests identifying how far into the physical and electronic system an attacker can penetrate before rejection.
- **Phase 2: White Box Testing & Vulnerability Assessment**
  - Conduct a thorough examination with an insider's knowledge.
  - Perform targeted vulnerability scanning and manual penetration testing on identified critical systems and applications, leveraging detailed knowledge provided by SJVAPCD.
  - Review source code and development processes of applications for risks & vulnerabilities that could be exploited by an attacker.
  - Assess the security configurations of all systems at all relevant sites.
  - Perform social engineering tests identifying how far into the physical and electronic system an attacker can penetrate before rejection.

Full Assessment: This is not limited to automated scanning but includes manual testing to exploit vulnerabilities, social engineering tactics to assess human-factor risks, custom exploit development, etc.

All vulnerability assessment and penetration testing should include, and not be limited to, all of the following major areas in its scope.

Wireless Network Security Review

Scope:

- **Inventory and Documentation:** in accordance with NIST SP 800-53, Control CM-8 (Information System Component Inventory)
- **Policy and Configuration Review:** in accordance with NIST SP 800-53, focusing on security controls applicable to wireless networking such as AC-18 (Wireless Access) for access control and IA-3 (Device Identification and Authentication)
- **Signal Footprint Analysis:** in accordance with NIST SP 800-48 Rev. 1, Guide to Securing Wireless LANs
- **Network Segmentation and Access Control:** in accordance with NIST SP 800-53 controls such as SC-7 (Boundary Protection)
- **Physical Security Controls:** in accordance with NIST SP 800-53, particularly PE controls related to physical access to information systems
- **Beyond Wi-Fi:** in accordance with NIST SP 800-121 Rev. 2, Guide to Bluetooth Security

Database Security Review

Scope:

- **Inventory and Documentation**: in accordance with NIST SP 800-53 Control CM-8 (Information System Component Inventory).
- **Configuration and Patch Management Review**: in accordance with NIST SP 800-53 Controls CM-2 (Baseline Configuration) and CM-3 (Configuration Change Control).
- **Authentication and Authorization**: in accordance with NIST SP 800-53 Controls AC-2 (Account Management) and AC-6 (Least Privilege).
- **Data Encryption**: in accordance with NIST SP 800-53 Controls SC-28 (Protection of Information at Rest) and SC-8 (Transmission Confidentiality and Integrity), Control SC-27 (Cryptographic Protection).
- **Backup and Recovery**: in accordance with NIST SP 800-53 Controls CP-9 (Information System Backup) and CP-10 (Information System Recovery and Reconstitution).
- **Audit and Logging**: Assess SQL Server auditing and logging practices, emphasizing NIST SP 800-53 AU-2 (Audit Events) and AU-12 (Audit Generation), to monitor access to sensitive data and detect anomalous activities effectively.

Software Development Life Cycle (SDLC) Security Review

Scope:

- **Development Practices and Standards**:
  - **Secure Coding Guidelines**:
    - **Guidelines Adoption and Integration**: Review the adoption and implementation of secure coding guidelines for VB.Net and C#. Ensure alignment with NIST SP 800-53 Controls SI-2 (Flaw Remediation) and SI-10 (Information Input Validation), confirming that guidelines effectively mitigate vulnerabilities.
    - **Integration into Development Lifecycle**: Assess integration of secure coding practices across the SDLC, ensuring compliance with NIST SP 800-53 Controls SA-8 (Security Engineering Principles) and SA-11 (Developer Security Testing and Evaluation).
    - **OWASP Compliance**: Evaluate adherence to OWASP's Secure Coding Practices to address common web vulnerabilities and improve software security posture.
- **Developer Awareness and Utilization**:
  - **Developer Awareness Programs**: Verify coverage of secure coding principles, including alignment with NIST SP 800-53 Control AT-2 (Security Awareness Training). Evaluate ongoing education and resource accessibility for developers.
  - **Practical Application of Secure Coding Guidelines**: Assess adherence to secure coding practices through randomized code reviews, focusing on compliance with NIST SP 800-53 Controls SA-11 and SI-10.
- **Developer Training**:
  - **Training Program Assessment**: Evaluate the comprehensiveness and relevance of developer training programs, ensuring alignment with NIST SP 800-53 Controls AT-2 and AT-3 (Role-Based Security Training). Confirm that training covers secure coding practices, vulnerability management, and defensive coding techniques as outlined by OWASP.
- **Third-party Libraries and APIs Security**:
  - **Vetting Process**: Assess procedures for selecting third-party libraries and APIs, ensuring alignment with NIST SP 800-53 Controls SA-4 (System and Services Acquisition) and CM-8 (Information System Component Inventory).

    - **Vulnerability Management**: Review processes for identifying and managing vulnerabilities in third-party components, aligning with NIST SP 800-53 Controls SI-2 and RA-5 (Vulnerability Scanning).
- **SaaS/PaaS Integrations Security**:
    - **Integration Security Assessment**: Review security measures for integrating SaaS/PaaS solutions, focusing on data protection, authentication, and secure API communication. Ensure practices comply with NIST SP 800-53 Controls SC-28, SC-8, and IA-5 (Authenticator Management).
- **CI/CD Pipeline Security**:
    - **Pipeline Security Controls**: Assess the integration and effectiveness of security mechanisms within the CI/CD pipeline, such as automated security scanning tools (SAST/DAST) and manual review gates. Ensure compliance with NIST SP 800-53 Controls SA-11 and SI-2 (Flaw Remediation).
    - **Deployment Environment Security**: Review security measures in deployment environments, focusing on segregation of duties and secure deployment practices in accordance with NIST SP 800-53 Controls AC-5 (Separation of Duties) and CM-2 (Baseline Configuration).
- **Source Code Management**:
    - **Access Control and Branch Management**: Evaluate security configurations within GitLab or similar environments, ensuring compliance with NIST SP 800-53 Controls AC-2, AC-6 (Least Privilege), and audit requirements per AU-2 (Audit Events).
- **Secrets Protection**:
    - Review the management and protection of secrets used in the development process, such as API keys and credentials, ensuring alignment with NIST SP 800-53 Control SC-28 (Protection of Information at Rest) for cryptographic protection of sensitive data.
- **Data Risk Governance**:
    - Assess data governance practices to ensure data classification, handling, and security align with NIST SP 800-53 Controls RA-2 (Security Categorization) and MP-4 (Media Storage and Access), focusing on risk management of data used and stored within the development environments.
- **Software Bill of Materials (SBOM)**:
    - Evaluate the processes for creating and maintaining an SBOM, ensuring transparency and security of software components as per best practices recommended by NIST for supply chain security. This evaluation should consider compliance with NIST SP 800-161 (Supply Chain Risk Management Practices).

<u>Backup Security Review</u>

Scope:

- **Backup Policy and Procedure Evaluation**:
    - **Backup Frequency and Scheduling**: Assess backup schedules to align with NIST SP 800-53 Control CP-9 (Information System Backup), ensuring they adequately reflect the criticality and usage patterns of different data types.
    - **Data Classification and Prioritization**: Review prioritization and classification of backup data according to sensitivity, ensuring policies comply with NIST guidelines for data categorization.
- **Backup Data Encryption**:

    - **Encryption Practices Assessment**: Evaluate encryption standards for data at rest and in transit, ensuring compliance with NIST SP 800-53 Controls SC-28 (Protection of Information at Rest) and SC-8 (Transmission Confidentiality and Integrity).
    - **Key Management Practices**: Review management of cryptographic keys against NIST guidelines for cryptographic key management.
- **Secure Off-Site Storage Practices**:
    - **Vendor and Storage Security**: Assess off-site storage locations and third-party vendor management processes to ensure compliance with NIST SP 800-53 Controls PE (Physical and Environmental Protection) and SA-9 (External Information System Services).
- **Backup and Recovery Testing**:
    - **Testing and Recovery Integration**: Evaluate testing frequency and disaster recovery plan integration, verifying alignment with NIST SP 800-53 Controls CP-9 (Information System Backup) and CP-10 (Information System Recovery and Reconstitution).
- **Access Control to Backup Data**:
    - **Comprehensive Access Review**: Ensure access controls for backup data and management interfaces align with NIST SP 800-53 Controls AC-2 (Account Management) and AC-3 (Access Enforcement).
- **Backup Data Lifecycle Management**:
    - **Retention and Disposal Compliance**: Review data retention schedules and secure disposal practices to ensure they meet NIST SP 800-53 Controls AU-11 (Audit and Accountability) for retention and MP-6 (Media Sanitization) for secure disposal.

<u>IoT Security Review</u>

Scope:

1. **Device Security:**
    - **Device Hardening:** In accordance with NIST SP 800-53 Control CM-7 (Least Functionality).
    - **Authentication and Access Control:** In accordance with NIST SP 800-53 Controls AC-2 (Account Management) and AC-3 (Access Enforcement).
2. **Network Security:**
    - **Data Encryption:** In accordance with NIST SP 800-53 Control SC-8 (Transmission Confidentiality and Integrity).
    - **Network Segmentation and Access Control:** In accordance with NIST SP 800-53 Control AC-4 (Information Flow Enforcement).
3. **Data Protection and Privacy:**
    - **Data Lifecycle Management:** In accordance with NIST SP 800-53 Control MP-4 (Media Storage and Access) and NIST SP 800-88 (Guidelines for Media Sanitization).
    - **Privacy Impact Assessment:** In accordance with NIST SP 800-53 Control AR-2 (Privacy Impact and Risk Assessment).

<u>Physical Security Review</u>

Scope:

1. **Physical Access Controls:**
    - **Entry and Exit Points:** In accordance with NIST SP 800-53 Control PE-3 (Physical Access Control).
    - **Visitor Management:** In accordance with NIST SP 800-53 Control PE-2 (Physical Access Authorizations).
2. **Environmental Controls:**
    - **Protection from Environmental Hazards:** In accordance with NIST SP 800-53 Controls PE-12 (Emergency Power) and PE-13 (Fire Protection).
    - **Climate and Temperature Controls:** Ensuring systems meet NIST SP 800-53 standards for environmental protection.
3. **Monitoring and Surveillance:**
    - **Surveillance Systems:** In accordance with NIST SP 800-53 Control PE-6 (Monitoring Physical Access).
    - **Incident Response and Notification:** Assess procedures for rapid and effective response to security incidents.
4. **Physical Security Barriers:**
    - **Perimeter Security:** Review adequacy of barriers like fences and gates, ensuring compliance with NIST SP 800-53's physical security controls.
    - **Secure Areas:** In accordance with NIST SP 800-53, ensure restricted access to critical IT infrastructure and sensitive information.

Policy and Procedure Review

Scope:

1. **Policy Comprehensiveness and Alignment**:
    - **Review of Existing Policies**: Assess the organization's existing information security policies for comprehensiveness and relevance, ensuring they cover key areas such as access control, data protection, incident response, and user training. This evaluation should reference NIST SP 800-53 to ensure policies align with federal guidelines for information security.
    - **Regulatory Compliance**: Evaluate policies for compliance with applicable laws, regulations, and standards, ensuring the organization meets all legal and contractual obligations related to information security.
2. **Procedure Effectiveness and Implementation**:
    - **Operational Procedures Review**: Examine the operational procedures derived from security policies to assess their effectiveness in daily operations. This includes reviewing procedures for access management, data encryption, backup, and disaster recovery, ensuring they are implemented and followed consistently, as guided by NIST SP 800-53's operational controls.
    - **Integration with Business Processes**: Assess how security procedures are integrated with business processes, ensuring security measures do not impede operational efficiency while maintaining a strong security posture.
3. **Policy and Procedure Updates**:
    - **Review Cycle**: Evaluate the process for reviewing and updating security policies and procedures, ensuring there is a regular review cycle that accounts for emerging threats, technological changes, and regulatory updates. This should align with NIST SP 800-53's PM-9 (Risk Management Strategy) control, emphasizing the need for policies and procedures to adapt to the evolving risk landscape.

- **Stakeholder Engagement**: Assess the involvement of relevant stakeholders in the policy review and update process, ensuring that feedback from IT staff, business units, legal, compliance, and external partners is considered.

4. **Training and Awareness**:
   - **Employee Training Programs**: Review the organization's security awareness and training programs to ensure they effectively communicate policies and procedures to all employees, as required by NIST SP 800-53's AT-2 (Security Awareness Training) control.
   - **Effectiveness of Training**: Evaluate the effectiveness of training programs in instilling good security practices among employees, including the measurement of training outcomes and changes in employee behavior.
   - **Role-Based Training**: Assess the implementation of role-based security training as recommended by NIST SP 800-53 AT-3 (Role-Based Security Training), ensuring that specialized training is provided based on the employees' roles and access to sensitive information.

Third-party Vendor Security Assessment

Scope:

1. **Vendor Risk Management:**
   - **Risk Assessment Process:** In accordance with NIST SP 800-161 M2.
   - **Vendor Security Policies Review:** In accordance with NIST SP 800-53.
2. **Contractual Security Requirements:**
   - **Security Clauses in Contracts Review:** In accordance with NIST SP 800-161.
   - **Compliance Verification Procedures:** In accordance with NIST SP 800-161.
3. **Vendor Access and Data Protection:**
   - **Access Control and Monitoring:** In accordance with NIST SP 800-53 AC-2 and AC-3.
   - **Data Protection Measures Review:** In accordance with NIST SP 800-53 SC controls.
4. **Incident Response and Reporting:**
   - **Vendor Incident Response Capabilities Review:** In accordance with NIST SP 800-53 IR controls.
   - **Incident Reporting Mechanisms Evaluation:** In accordance with NIST SP 800-53 IR controls.

Disaster Recovery and Business Continuity Planning Review

Scope:

1. **Plan Comprehensiveness and Alignment:**
   - **DR and BC Plans Review:** In accordance with NIST SP 800-34.
   - **Alignment with NIST SP 800-53:** Compliance check with CP-2, CP-6, and CP-7.
2. **Implementation and Testing:**
   - **Plan Implementation Review:** Evaluation guided by general principles in NIST SP 800-34.
   - **Testing and Exercises:** In accordance with NIST SP 800-34 testing recommendations.
3. **Training and Awareness:**
   - **Employee Training Programs:** In accordance with NIST SP 800-50 and SP 800-53 AT-2.
   - **Awareness Initiatives:** Review of awareness practices to ensure a culture of

preparedness.

4. **Plan Updates and Maintenance:**
    - **Review and Update Cycle:** In accordance with NIST SP 800-34.
    - **Stakeholder Involvement:** Evaluation of stakeholder engagement in plan maintenance and updates.

Deliverables:

Objective:

Produce a comprehensive package of deliverables from a qualified service provider, encompassing the entirety of the cybersecurity risk assessment, audit, and subsequent retesting processes. This package aims to provide the organization with a holistic view of its cybersecurity posture, alignment with NIST standards, adherence to FISMA risk management practices, and a clear path toward remediation and improvement of identified vulnerabilities and compliance gaps across all evaluated areas.

Integration with Previous Sections:

This package of consolidated deliverables takes into account the findings and recommendations from all previously mentioned Minimum Scope Objectives sections addressed in the RFP, ensuring a holistic approach to cybersecurity risk management. By providing a comprehensive overview of the organization's security posture, detailed insights into specific vulnerabilities and compliance gaps, and a clear, actionable path toward remediation and improvement, these deliverables aim to enhance the organization’s resilience against cyber threats and ensure compliance with NIST standards and FISMA requirements.

Executive Summary Report:

- A high-level document synthesizing key findings from the comprehensive cybersecurity risk assessment and audit, including insights from specific sections such as incident response, cybersecurity maturity, configuration management, etc. The report will highlight critical vulnerabilities, compliance issues, and overall risk posture, ensuring senior management clearly understands the organization's cybersecurity strengths and weaknesses.

Detailed Findings and Recommendations Report:

- An exhaustive report detailing the findings from the entire cybersecurity risk assessment and audit scope, including retests of critical findings. This document will provide an in-depth analysis of vulnerabilities, non-compliances, and other security issues identified and categorized by system components, data types (e.g., financial, HR, credit card processing), and relevant NIST and FISMA guidelines. It will also include actionable recommendations for addressing each identified issue.

Prioritized Action Plan:

- A prioritized action plan derived from the remediation roadmap, focusing on short-term and long-term strategies to enhance the organization's cybersecurity framework. This plan will identify key priorities for immediate action, considering factors such as risk reduction potential, compliance urgency, and operational impact, to guide the organization in effectively allocating resources toward the most critical areas.

Presentation of Findings to Stakeholders:

- A formal presentation to communicate the findings, recommendations, remediation roadmap, and prioritized action plan to key stakeholders, including senior

management, IT and security teams, and relevant department heads. This presentation will facilitate a comprehensive understanding of the organization's current cybersecurity posture, the steps needed for improvement, and the role of various stakeholders in supporting cybersecurity initiatives.

Industry Standard Certification:

- If during the course of analyzing the state of the SJVAPCD information systems, the findings lend themselves to the achievement of compliance with any known industry certifications such as Cybersecurity Maturity Model Certification (CMMC), ISO/IEC 27001, etc. that effectively comprised of a subset of standards related to FISMA requirements, the service provider should officially acknowledge this and certify SJVAPCD if applicable.

Schedule of Deliverables

Date	Event
30-Aug-24	All Deliverables Due
5-Sep-24	Presentation to ITS Management
13-Sep-24	Presentation to Executive Management

*Dates can be adjusted as needed

SECTION V: REQUIRED QUALIFICATIONS

Persons or firms proposing to bid on this proposal must be qualified and experienced in representing and advising governmental agencies and must submit qualifications demonstrating this ability in penetration testing and cybersecurity risk/maturity assessment.

Proposer must submit the following:

1. Summary of years of service experiences in the relevant space;
2. Resumes or similar statement of qualifications of person or persons who may be designated to perform the pen test and/or cybersecurity risk/maturity assessment.
3. List of representative clients;
4. Summary of the methodology/approach of penetration testing and risk/maturity assessment;
5. Sample delivery reports for the required deliverables.
6. Summary of proposer's general qualifications to meet required qualifications and fulfill statement of work, including additional Firm personnel and resources beyond those of the designated persons.

SECTION VI: BIDDERS CONFERENCE

To address any questions related to this RFP and provide prospective vendors the opportunity to understand the project scope and requirements more clearly, the SJVAPCD will host a Bidders Conference. The conference is scheduled for May 15, 2024, and will be conducted via Zoom.

Prospective vendors are not required to participate in this conference to submit a proposal or be considered seriously. However, attendance is strongly recommended due to the detailed discussions of technical aspects expected during this meeting. The SJVAPCD will not be responsible for providing individual briefings to non-attendees about the details discussed in the meeting.

The agenda for the conference is outlined as follows:

- The introduction of SJVAPCD staff involved in the project.
- Review of the RFP.
- A question and answer session to clarify any queries from the participants.

Please confirm your intention to attend this conference by May 15, 2024, by contacting Tim.VanDyne@valleyair.org. Details for accessing the Zoom meeting will be provided upon confirmation of attendance.

SECTION VII: PROPOSAL DESCRIPTION

Each proposal submitted must include, at a minimum, the following four sections:

1. Company profile
2. Technical proposal
3. Project management
4. Pricing summary

The SJVAPCD's evaluation process will primarily focus on responses as presented in these sections. A title page reflecting your proposal title, your firm's name, address, telephone number, fax number, the name and contact information of your firm's contact person, and date is also requested.

Company Profile

At a minimum, this section should include:

- Specific responses to each item in Section V of this RFP. This should include your firm's understanding of the item and how you propose to complete each task.

Technical Proposal

At a minimum, this section should provide detailed descriptions of:

- The methodologies and technologies proposed for conducting the cybersecurity risk assessment, including any specialized software or tools.
- Detailed plans for vulnerability assessment, penetration testing, and other security testing measures that will be employed.
- Proposed strategies for identifying, classifying, and mitigating risks in accordance with NIST standards and FISMA requirements, focusing on the unique cybersecurity challenges identified in the RFP.

Project Management

At a minimum, this section should include:

- A brief statement of your firm's understanding of the work to be done for this project.
- Descriptions of the relevant experience your firm has in the analysis, auditing, testing, or otherwise engaging with other teams & systems in the context of a cybersecurity risk assessment involving systems similar to the ones in this RFP.

- Projected implementation schedule milestones from receipt of contract to final test and acceptance. The integrator will review the SJVAPCD proposed schedule and provide input as necessary.
- How your firm plans to manage the overall project.

Cost Proposal

This section must include your estimated cost for the specific items requested in this RFP, including options where indicated. Additionally, your firm is encouraged to propose any alternative options regarding the various subsystems, maintenance and service, training, etc.

To assist the SJVAPCD in the evaluation process, this section should be formatted to reflect easily:

- Major end item and total system cost breakdown for each major area of assessment that is listed in Section IV, preferably in terms of subsystems as defined throughout Section IV.
- Project management and/or any integrator fee structure.

Proposal cost should be summarized in a Cost Detail Sheet that provides line-item detail and a section that grand totals the quoted amount necessary for the components of the project.

Name and Address - The Cost Proposal must list the name and complete address of the Proposer in the upper left-hand corner.

Cost Proposal – The SJVAPCD anticipates awarding a fixed price contract. Cost must be itemized for each assessment piece and cost information must be provided as listed below:

1. Detail must be provided by the following categories:

   A. **Labor** - The Cost Proposal must list the fully-burdened hourly rates and the total number of hours estimated for each level of professional and administrative staff to be used to perform the tasks required by this RFP. Costs should be estimated for each of the components of the work plan.

   B. **Subcontractor Costs** - List subcontractor costs and identify subcontractors by name. Itemize subcontractor charges per hour or per day.

   C. **Travel Costs** - Indicate amount of travel cost and basis of estimate to include trip destination, purpose of trip, length of trip, airline fare or mileage expense, per diem costs, lodging and car rental.

   D. **Other Direct Costs** -This category may include such items as postage and mailing expense, printing and reproduction costs, etc. Provide a basis of estimate for these costs.

Prohibited Interest

Each proposal must contain a written statement disclosing to the SJVAPCD any financial interest in the proposer's business or in this transaction held by any SJVAPCD Board member or any SJVAPCD officer or employee. The SJVAPCD reserves the right to refuse any proposal if the SJVAPCD determines a conflict of interest exists. A conflict of interest

may be determined to exist in any instance where a SJVAPCD officer or employee participates in or influences any decision-making process affecting a bid or contract in any way whatsoever.

SECTION VIII: PROPOSAL EVALUATION

The SJVAPCD will evaluate proposals based on the following criteria:

- Completeness and clarity of the proposal.
- Firm's experience in information security auditing and analysis.
- Project management experiences for this particular type of implementation; how your firm proposes to implement this engagement, assure end-to-end process integrity, and your overall project management approach to this task – including scheduling, team composition, etc.
- Responses from references.
- Competitiveness of pricing as outlined in the Pricing Summary section.

Proposals will be primarily assessed based on the documentation provided. However, the SJVAPCD may invite firms to deliver oral presentations, or request additional information as part of the evaluation process.

The SJVAPCD will have sole discretion in evaluating proposals and deciding which best meets the SJVAPCD's needs. The SJVAPCD reserves the right to negotiate with any firm, accept a proposal other than the lowest-priced, and reject any or all proposals if deemed in the SJVAPCD's best interest.

SECTION IX: PROPOSAL DEADLINE

An electronic PDF copy of your proposal submitted in response to this RFP must be sent via e-mail to:

Imtiaz Haq, Director of Information Systems
SJVAPCD
1990 E. Gettysburg Ave.
Fresno, CA 93726
(559) 230-6047
Imtiaz.Haq@valleyair.org

Tim Van Dyne, Senior Network Systems Security Analyst
SJVAPCD
1990 E. Gettysburg Avenue
Fresno, CA 93726
Tim.VanDyne@valleyair.org

For consideration, the proposal must be received no later than **May 20, 2024**.

SECTION X: LIST OF APPENDICES

1. NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations
   URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
2. NIST SP 800-48 Rev. 1 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
   URL: https://csrc.nist.gov/publications/detail/sp/800-48/rev-1/final
3. NIST SP 800-121 Rev. 2 - Guide to Bluetooth Security
   URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf
4. NIST SP 800-88 - Guidelines for Media Sanitization
   URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
5. NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations
   URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
6. NIST SP 800-34 - Contingency Planning Guide for Federal Information Systems
   URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-34r1.pdf
7. NIST SP 800-218 – Secure Software Development Framework (SSDF)
   URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf
8. Federal Information Security Management Act (FISMA), NIST Risk Management Project
   URL: https://csrc.nist.gov/projects/risk-management