County of Marin, CA

Request for Proposal

Information Security Risk Assessment

Issue Date: 1/20/2015

Table of Contents

TIMELINE

- Release of the RFP: 1/20/2015
- RFP Notice of Intent Deadline: 2/9/2015
- Deadline for Written Questions: 2/17/2015
- County issues Written Responses to Written Questions: 2/24/2015
- RFP Submission Deadline: 3/18/2015
- Tentative start date for contract: 4/15/2015

The above dates are subject to change as deemed necessary by the County

I. INTRODUCTION

The County of Marin ("County") Information Services and Technology ("IST") department invites responses to a Request for Proposal ("RFP") to provide a Privacy and Security Risk Assessment for multiple County departments pursuant to the Health Insurance and Portability Accountability Act of 1996 (HIPAA)/Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).

In 1996, the United States Congress passed the Health Insurance Portability and Accountability Act (HIPAA). The Administrative Simplification provisions (Title II) of this law require an adaptation and implementation of standards for the privacy, security and arrangement of electronic healthcare transactions. The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) of the American Recovery and Reinvestment Act of 2009 (ARRA) and the HIPAA Omnibus Rule of 2013 contain provisions that significantly affected the HIPAA Privacy and Security Rules. The HIPAA Privacy Rule and the HIPAA Security Rule (collectively, the "HIPAA Rules") were issued by the United Sates Department of Health and Human Services in 2002 and 2003, respectively. While assessing compliance with the HIPAA Rules will be a priority, compliance with additional privacy and security regulations and contractual requirements will be included in the scope of this project.

A. Definitions

For the purposes of this RFP process, the following definitions apply:

- **Agency** means the County of Marin.
- **Analysis** means the HIPAA/HITECH Act Privacy and Security Risk Assessment requested through this RFP.
- **Compliance** means meeting the requirements of the HIPAA/HITECH and Security Rules.
- **Contract** means a written agreement between the County and Vendor selected to provide a HIPAA/HITECH Privacy and Security Risk Assessment.
- **Covered Entities** Health plans, health care clearinghouses, and health care providers who electronically transmit any health information in connection with transactions for which the County has adopted standards, including all the departments who directly or indirectly are involved in those transactions.
- **ePHI** means electronic Protected Health Information.
- **HIPAA** means the Health Insurance Portability and Accountability Act of 1996.
- **HIPAA Privacy Rule** means the provisions regarding the privacy of individually identifiable health information located in 45 CFR Part 160 and Subparts A and E of Part 164 as well as any amendments.
- **HIPAA Security Rule** means the provisions regarding security standards for the protection of electronic protected health information located in 45 CFR Part 160 and Subparts A and C of Part 164 as well as any amendments.
- **HITECH Act** means the Health Information Technology for Economic and Clinical

Health Act of 2009 as well as any amendments.

- **ISO 27001** Information technology - Security techniques - Information security management systems - Requirements, published by International Standard Organization (ISO) in 2013.
- **ISO 27002** Information technology – Security techniques - Code of practice for information security management published by International Standard Organization (ISO) in 2013.
- **IST** means the County of Marin Information Services and Technology Department.
- **NIST** National Institute of Standards and Technology.
- **PHI** means Protected Health Information.
- **Proposal** means a formal, written response to this RFP submitted by a Vendor.
- **Request for Proposal ("RFP")** means all documents, including those attached or incorporated by reference, used for soliciting proposals to provide a HIPAA/HITECH Privacy and Security Risk Assessment.
- **Remediation Plan** A list of prioritized controls (based on level of identified risks, ease of implementation, time, and cost of implementation) to reduce the risks to an acceptable level.
- **Vendor** means any person or organization who submits a Proposal in response to this RFP.
- **Risk Assessment** An accurate and thorough systematic method for identifying, evaluating, and prioritizing the potential risks in a systematic (qualitative or quantitative), repeatable, and measurable way.
- **Steering Committee** Group of County stakeholders who will supervise the project and approve the milestones and reports provided by the vendor.

B. Notice of Intent (Mandatory)

Those intending to submit a Proposal must notify by email the County Contact, listed in paragraph C on page 7 by **2/9/2015, PST**, of their intent to submit a Proposal**.** The Notice of Intent does not compel submission of a Proposal. However, only those Vendors who submit a timely Notice of Intent will have their Proposal considered. If the Vendor has not received confirmation within 24-hours of submission of their Notice of Intent, it is the responsibility of the Vendor to verify receipt of the Notice of Intent with the County Contact.

C. Correspondence

All correspondence, including Proposals, shall be submitted to:

County of Marin
Attn: Maria Eckdish
1600 Los Gamos Drive, Suite 275
San Rafael, CA 94903
E-Mail: meckdish@marincounty.org

All inquiries are public information. Vendors may contact only the individual identified above on any matter related to this RFP. Failure to comply may result in a vendor being barred from consideration under this RFP.

Questions regarding this RFP must be written and should be emailed with a subject line of "County of Marin Security Assessment" to

meckdish@marincounty.org

County's written responses to timely questions will be sent to all vendors who have submitted a Notice of Intent no later than **2/24/2015, PST.**

D. Proposal Submission Deadline

All Proposals must be received at the address listed in Paragraph C on page 7, no later than **4:00 p.m. on 3/11/2015, PST**. Submit to County:

- **1 signed, completed, unbound original technical and cost proposal.** Facsimile or electronically transmitted Proposals will not be accepted in lieu of a hard copy sent by U.S. mail, or hand delivered. Postmarks will not be accepted in lieu of actual receipt. Late Proposals will not be considered.
- **1 electronic copy (via e-mail) of the original technical and cost proposal in addition to the hard copy.**

The first page of the original proposals should be marked "Original" and the first page of the electronic copy should be marked "Copy."

II. PROPOSAL REQUIREMENTS

A. Purpose

The County of Marin, through its IST department is requesting proposals for a vendor to perform a Privacy and Security Risk Assessment ("Analysis") for all departments that fall within the scope of the project. The purpose of this RFP is to select a qualified vendor to perform a risk assessment, identify areas, and make specific recommendations to enhance Privacy and Security Rule compliance.

B. Summary of Scope Of Work

The scope of work shall consist of visiting various County departments and offices to perform the assessment. The assessment will cover both technical and non-technical aspects of security and compliance, as detailed in **Section VII., Scope of Work**. A written summary of all problem areas shall include specific remediation recommendations for HIPAA/HITECH Privacy and Security compliance. The Vendor shall have the staff and resources to complete the requirements of this RFP for the project, including the written summary within one hundred twenty (120) days after contract signing.

III. PROPOSAL SUBMISSION

A. General

1. Proposal Submission - To be considered, all Proposals must be submitted in the manner set forth in this RFP. It is the Vendor's responsibility to ensure that its Proposal arrives on or before the specified time.
2. All interested and qualified Vendors are invited to submit a Proposal for consideration. Submission of a Proposal indicates that the Vendor has read and understands this entire RFP, will include all appendices, attachments, exhibits, schedules, and addendum (as applicable), and agrees that all requirements of this RFP have been satisfied.
3. Proposals must be submitted in the format described in this Section. Proposals are to be prepared in such a way as to provide a straightforward, concise description of capabilities to satisfy the requirements of this RFP. Emphasis should be concentrated on conformance to the RFP instructions, responsiveness to the RFP requirements, and on completeness and clarity of content.
4. Proposals must be complete in all respects as required in this Section. A Proposal may not be considered if it is conditional or incomplete.
5. Proposals must be received at the designated location, specified in paragraph C on page 7, no later than the date and time specified in paragraph D on page 7.
6. All Proposals and materials submitted become the property of the County.

B. Proposal Presentation

One unbound original of each Proposal is required. Additionally, each Proposal must be submitted in a separate sealed envelope, plainly marked "**Response to RFP for Information Security Risk Assessment."** Failure to submit the Proposal as requested may result in rejection of the Proposal. No facsimiles or emails will be accepted.

The costs for developing proposals are solely the responsibility of the applicants. The County will not provide reimbursement for such costs. The Proposal documents shall become the property of the County upon submission.

C. Proposal Format

Each Proposal must be submitted as a single document on standard 8 ½ x 11 paper (paper up to 11 x 17 is permissible for charts, spreadsheets, etc.) in the following format and must contain, as a minimum, all listed items in the sequence indicated.

1. Letter of Transmittal, which MUST:
    a. Identify the submitting organization.
    b. Identify the name and title of the person authorized by the organization to contractually obligate the organization.
    c. Identify the name, title, telephone number and email address of the person authorized to negotiate the contract on behalf of the organization.
    d. Identify the name, title, telephone number, and email address of the person to be contacted for clarification.
    e. Explicitly indicate acceptance of the Proposal evaluation and selection method in this RFP.
    f. Certify that all statements in the Proposal are true and acknowledge that if the Proposal contains any false statements, the County may declare the Contract made as a result of the Proposal to be void.
    g. Acknowledge receipt of any and all amendments to this RFP.
    h. Be signed by the person authorized to contractually obligate the organization.
2. Table of Contents.
3. Executive Summary: A high-level synopsis of the organization's response to the RFP. This should include a brief overview of the engagement, identify the main features and benefits of the proposed work, and describe how the proposed solution will address the stated high level business and technical goals.
4. Corporate Experience: A description of the company, number of years performing security assessments (must have a minimum of five (5) years of experience), recent client references (minimum three (3)), public sector experience, and key differentiators.
5. Staff Experience: Vendors must submit resumes of all proposed professional staff members who will be performing services under the Contract. Experience narratives shall be attached that describe the specific relevant experience of the

staff members in relation to the role that member will perform for this Contract. The narrative(s) must include the name of the individual(s) proposed and should include a thorough description of the education, knowledge, and relevant experience as well as any certifications or other professional credential that clearly shows proposed staff member's expertise.

Additionally, please provide an explanation of how many and what type of full and part time staff will be assigned (including types of staff such as Certified Information Systems Security Professional (CISSP), Certified in Healthcare Privacy Compliance (CHPC), legal, technical, administrative, etc.) to this project and justify this allocation of staff time.

6. Project Plan: Vendors must provide a detailed project plan for each phase of the project. The project plan should include the tasks, duration, resources, milestones, dependencies, and deliverables.
7. Response to Section VII. – Scope of Work.
8. Copies of insurance policies, binders, or certificates evidencing the following insurance coverage:
   a. Comprehensive general liability (including auto and non-owned auto, bodily injury and property damage): $1,000,000 combined single limit.
   b. Workers' Compensation: Statutory levels.
9. Non-Disclosure Agreement – Include as a separate attachment
10. Cost: Vendors must provide an itemized cost analysis / price breakdown for their final offer. The cost analysis must be in accordance with the requested services in **Section VII., Scope of Work** and will be subject to the requirements of items 1 and 2 of section D on page 10, **Specifications**.

D. Specifications

1. Cost **-** The contract is subject to the Cal Multiple Award Schedules (CMAS) terms and conditions between the Contractor and the State of California, except as specified below:
   a. This is a fixed-price, deliverables contract. All costs must be inclusive of labor and other direct costs, including travel.
   b. Progress payments will be made upon written acceptance of the key deliverables. Itemized invoices must be submitted in triplicate to:

      County of Marin
      Attn: Maria Eckdish
      1600 Los Gamos Drive, Suite 275
      San Rafael, CA 94903
      E-Mail: meckdish@marincounty.org

   c. Payment withholding will apply. Ten percent (10%) of the invoiced amount will be withheld pending final completion, receipt, and acceptance by IST of the final deliverable.

2. Best and Final Offer **-** The Vendor may submit a Best and Final Offer.

3. Oral Presentation - If selected as a Finalist, the Vendor shall agree to provide the County the opportunity to interview proposed staff members identified by the Evaluation Committee in the Finalist notification letter at an oral presentation. A statement of concurrence is required.

IV. PROPOSAL EVALUATION AND SELECTION

A. Evaluation Process

If only one Vendor submits a Proposal, the County may, at its sole discretion, enter into negotiations with that Vendor to provide the Services or it may reject that Proposal.

Should more than one Vendor submit a Proposal, the following evaluation process will be used to select the vendor.

B. Evaluation Criteria

1. Initial Review - All Proposals will be initially evaluated to determine if they meet the following minimum requirements:
   a. The Proposal must be complete, in the required format, and be in compliance with all the requirements of this RFP.
   b. Vendors must meet the requirements as stated in the Minimum Vendor Requirements as outlined in paragraph C on page 13.
   c. Failure to fully comply with any of the requirements of the RFP or to provide all requested information may result in the Proposal being rejected and given no consideration. The determination of compliance with the terms and conditions of this RFP shall be in County's sole judgment and its judgment shall be final and conclusive.
2. Evaluation Point Summary - Each proposal received in response to this RFP that meets minimum requirements will be evaluated. While cost is an important consideration in the evaluation process, selection will be based on the determination of which Proposal best meets the needs of the County and the requirements of this RFP. The following is a summary of evaluation factors with point value assigned to each. These, along with the general requirements, will be used in the evaluation of Vendor proposals.

	Points
Corporate Experience	15
Proposed Staff Experience	15
Completeness of Project Plan	15
Response to Section VII. - Scope of Work	25
Total Cost	30
Total Points	**100**

3. Overall, the County is interested in responses demonstrating the Vendor's previous experience in performing similarly complex HIPAA Privacy and Security Risk Assessments and its proposed approach to leverage that experience in meeting the requirements. Specific and unique corporate experience should be clarified.

4. Proposals will be evaluated on the factors that have been assigned a point value. The Vendors with the highest scores will be selected as finalist vendors based upon the proposals submitted. Finalist vendors may be asked to submit revised Proposals for the purpose of obtaining best and final offers. The Vendor whose Proposal is most advantageous to the County, in its sole discretion, taking into consideration the Evaluation Criteria, will be recommended for contract award as specified in Paragraph C on this page.

C. Contract Award

1. The Contract, if awarded, will be awarded to the vendor submitting the Proposal deemed by the County, in its sole discretion, to be experienced and fiscally responsible and whose Proposal is determined to be the most cost effective and advantageous to the County. The Vendor submitting the Proposal deemed, by the County, in its sole discretion, to be the most advantageous will be asked to enter into the Contract negotiation stage.
2. The County is not required to award the Contract to the Vendor that submits the least costly Proposal. Furthermore, the County reserves the right to award one or more contracts to one or more vendors as a result of this RFP.
3. The Vendor selected should be prepared to accept the terms of this RFP for incorporation into a Contract resulting from this RFP, as well as any terms and conditions required by the state and federal funding sources for this RFP.
4. If an agreement to enter into a Contract cannot be reached with the selected vendor, then the negotiations with that Vendor will be terminated. At the sole discretion of the County, negotiations may then be opened with another vendor and the process repeated, or the County may elect to reject all submitted Proposals and terminate this RFP process. Once negotiations with a particular Vendor are terminated, the County will not reopen negotiations with that Vendor.
5. The County may elect at any time to terminate the RFP process, including rejecting all submitted Proposals.
6. A Notice of Award will be mailed to all Vendors at the address specified in the proposal, advising if they were selected to enter into Contract negotiations with the County and shall be deemed received three [3] business days after mailing.

D. Use and Disclosure of Proposals

1. Information contained in the vendor's proposal that is company confidential must be clearly identified in the proposal itself. The County will be free to use all information in the vendor's proposal for the County's purposes. The vendor understands that the County is a public agency subject to the disclosure requirements of the California Public Records Act and/or Freedom of Information Act.
2. This RFP process shall extend until the date stated on the County's written Notice of Award or the date stated on the County's written notice of cancellation of this RFP

process that will be issued to all Vendors.

3. Unless the vendor provides all information required by this RFP process, the Proposal may, at the sole discretion of the County, be rejected and given no consideration. Any vendor attempting to influence this RFP process by interfering or colluding with other vendors or with any County employee may be disqualified.

4. Any vendor submitting a Proposal understands and agrees that submission of his/her/its Proposal shall constitute acknowledgment and acceptance of, and intent to comply with, all the terms and conditions contained in this RFP. The determination of the compliance with the terms and conditions of this RFP shall be in the County's sole judgment and its judgment shall be final and conclusive.

V. PROCUREMENT CONDITIONS

A. Contingencies

1. Initiation of this RFP process does not commit the County to finalize a Contract or to pay any costs associated with the preparation of any Proposal, nor to enter into a Contract with the vendor submitting the least costly Proposal.

2. The County reserves the right, in its sole discretion to:

   a. Accept or reject any or all Proposals, or any part thereof;

   b. Reject any Proposal for failure to submit the Proposal in conformity with the requirements, or the terms and conditions, of this RFP;

   c. Waive informalities and irregularities in a Proposal, or to waive any deviations from the requirements or specifications of this RFP that are included in any Proposal, if deemed to be in the best interest of the County;

   d. Negotiate with qualified vendors; or

   e. Cancel in part or in its entirety this RFP process, at any time.

B. Modifications

In the event this RFP process is amended, cancelled, or terminated prior to entering into contract with the selected Vendor, County's written notice of amendment, cancellation, or termination of this RFP process will be sent to all Vendors who submitted a Notice of Intent.

C. Inaccuracies or Misrepresentations

If in the course of the RFP process or in the administration of a resulting contract, the County determines that the Vendor has made a material misstatement or misrepresentation, or that materially inaccurate information has been provided to the County, the Vendor may be terminated from the RFP process. In the event a contract has been awarded, the contract may be terminated.

D. Incurred Costs

The County shall not be liable for any costs of work performed in the preparation and production of a Proposal, or for any work performed prior to the effective date of a Contract. By submitting a Proposal, the Vendor agrees not to make any claims for, or have any right to, damages because of any misunderstanding or misrepresentation of the terms and conditions of this RFP, because of any misinformation, or lack of information.

E. Proposal Confidentiality

1. All Proposals will become the sole property of the County. At such time as a Vendor agrees to enter into a Contract with the County, or the County decides to terminate this RFP process without entering into a Contract, all Proposals and related documents become a matter of public record, with the exception of those parts of a Proposal which are trade secrets, as that term is defined by statute.
2. If any part of a Proposal contains any trade secrets that the vendor does not want disclosed to the public, the Vendor shall mark that part of the Proposal as a "trade secret." The County, however, shall not in any way be liable or responsible for the disclosure of any Proposal or any part thereof if disclosure is required under the Public Records Act (Government Code, Section 6250 et seq.) or pursuant to law or legal process.
3. In addition, by submitting a Proposal, a vendor agrees to save, defend, keep, hold harmless, and fully indemnify the County, its elected officials, officers, employees, agents, and volunteers from all damages, claims for damages, costs, or expenses, whether in law or in equity, that may at any time arise or be set up for not disclosing a trade secret pursuant to the Public Records Act.

F. Negotiations

The County may require the potential Vendor(s) selected to participate in negotiations, and to submit revisions to pricing, scope of work, technical information, and/or other items from their Proposal(s) as may result from these negotiations.

VI. CONTRACT INFORMATION

A. Contract Development

If the County chooses to fund and proceed with the Information Security Risk Assessment it will enter into a Contract with the selected Vendor. NOTE: The County will work with the selected Vendor to develop a Contract. Revisions to the budget and/or scope of work may be necessary.

B. Standard Contract Language

Attached is the County's standard contract. The successful Vendor will be required to

comply with the terms and conditions presented in this contract.

C. Governing Laws

This RFP and any resulting agreement, contract and purchase order shall be governed by all applicable federal, state and local laws, codes or ordinances and regulations, including but not limited to those promulgated by CAL-OSHA, FED-OSHA, EPA, EEOC DFEH, and HIPAA. Additionally, the County of Marin is a nuclear free zone in which work on nuclear weapons and/or the storage or transportation of weapons-related components and nuclear material is prohibited or appropriately restricted. The County is prohibited or restricted from contracting for services or products with, or investigating County funds in any nuclear weapons contractor.

VII. SCOPE OF WORK

This includes the systematic and technical risk assessment, audit, review, and other due diligence activities in order to identify the risks and provide a remediation plan to manage those risks. The following services must be included.

A. Information Security Risk Assessment

The goal of acquiring this service is to assess the County's risk in compliance with regulatory requirements, industry standards and best practices (HIPAA Rules - 1996, HITECH Act - 2009, HIPAA Omnibus Rule - 2013 and ISO/IEC 27002:2013) and create a plan for reducing the level of identified risks. This includes conducting a systematic risk assessment in order to identify County's information assets, evaluate and analyze the potential risks, and recommend mitigation options to provide a clear, meaningful, risk assessment report.

There is no single risk assessment methodology that will work for all organizations and all situations. The County is open to different options on how the risk assessment shall be performed, but the methods must be in accordance with NIST SP 800-33.

The Vendor must meet the following major objectives:

1. Establish whether the County is operating in compliance with requirements (HIPAA:1996,HITECH Act 2009, and HIPAA Omnibus Rule) considering each of the following HIPAA Privacy and Security standards:
    a. 163.306 General Requirements
    b. 164.308 Administrative Safeguards
    c. 164.310 Physical Safeguards
    d. 164.312 Technical Safeguards
    e. 164.316 Policies, Procedures and Documentation
    f. 164.502(b) Standard: Minimum Use and Disclosure of PHI
    g. 164.530(a) Standard: Personnel Designations
    h. 164.530(b) Standard: Training
    i. 164.530(c) Standard: Safeguards
    j. 164.530(d) Standard: Complaints to the Covered Entity
    k. 164.530(e) Standard: Sanctions
    l. 164.530(f) Standard: Mitigation
    m. 164.530(g) Standard: Refraining from Intimidating and Retaliatory Acts
    n. 164.530(h) Standard: Waiver Rights
    o. 164.530(i) Standard: Policies and Procedures
    p. 164.530(j) Standard: Documentation

2. Evaluate County's compliance with essential security policies, standards, and practices based on the International Organization for Standardization's ISO/IEC International Standard 27002:2013.
3. Identify and evaluate all information assets (data, information systems, and information processing facilities) which store, maintain, support or transmit ePHI.
4. Evaluate and measure the potential risks to identified information assets (to include the cost of failure related to privacy or security breaches and other information security threats) associated with how the different departments/divisions collect, use, manage, store, maintain, disclose, and dispose of information. Assess existing security measures currently in place and the effectiveness of those measures.
5. For "addressable" HIPAA specifications that are determined to be unreasonable or inappropriate, formally document alternative security measures that are being implemented and how the alternative measures meet the standard. If not applicable, formally document the reason why the HIPAA implementation specification is not reasonable and appropriate and how the higher level standard is being met.
6. Provide a prioritized list of realistic options/controls for enhancing security. The vendor may suggest different types of remediation options/controls (e.g. policy, procedure, technology or technical control) for each identified risk. Each option should include an estimated cost and effort and be mapped to the appropriate standard (e.g. HIPAA, ISO 27002:2013. Controls).
7. Provide documentation that fulfills the risk assessment requirements and provide an admissible report for state and federal audits.
8. Provide procedures to enable the County to be able to repeat the performed risk assessment in the future, with or without the help of the vendor. The output should be at least comparable to the previous Risk Assessment reports.
9. During the assessment, the Vendor should consider the County's current policies, standards, guidelines, procedures, contractual requirements, other documents, and controls currently in place. In this regard, the Vendor should also:
    a. Compare HIPAA, Privacy, and Security Rule requirements with all applicable California state privacy, security and confidentiality statute and contractual requirements and identify which state statutes are more restrictive than the federal law and the extent to which the County meets the most restrictive requirements. Analysis/comparison to include all primary sources for regulatory citations.
    b. Conduct onsite visits of all departments within scope in order to evaluate the physical structures and determine if building or space modifications are required for compliance.
    c. Review and evaluate the HHS HIPAA Breach incident reporting and response practices, procedures, and policies.
    d. Interview selected management and staff members regarding common privacy and security related practices within branches/programs and between branches/programs to include, but not be limited to use, disposal, storage, and encryption practices or procedures.
    e. Review a sampling of contracts, Joint Powers Agreements, Memoranda of Understanding, Government Service Agreements, Business Associate

Agreements, and other organizational relationships for HIPAA Privacy and Security compliance.

f. Review policies, procedures, and practices for HIPAA Privacy and Security compliance, including the review of all HIPAA-related agreements for new hires (County employees, independent contractors, temporary employees, volunteers, etc.).

g. Review the HIPAA Privacy and Security training program currently used by the County to determine if there are gaps between training content and HIPAA Privacy and Security standards or state privacy and security statutes. Evaluate the training program and recommend appropriate changes to improve training quality and efficiency. Identify training requirements for staff, management, and executive levels and determine if some training should be procured externally.

h. Analyze the current physical and electronic PHI-handling and monitoring practices against the requirements of HIPAA Privacy and Security regulations and identify gaps between current practices and required practices under HIPAA Privacy and Security Rules.

B. Technical Risk Assessment

The goal of acquiring this service is to identify and evaluate IT technical information security risks within the County infrastructure and provide technical solutions to enhance security in order to help County to reach the desired level of assurance.

In general, Technical Risk Assessments consist of several different security assessment services (e.g. Penetration Testing, Vulnerability Assessment, Denial of Service Testing, Social Engineering, Security Architecture and Configuration review, etc.), may employ various tools and techniques, and can be performed with different approaches and methodologies.

Regardless of what services are proposed, they should be proposed in a modular way so that individual components can be chosen separately.

The following services must be provided to meet the RFP requirements:

1. **Network Security Assessment** - Provides the County with a security focused network architecture review highlighting current strengths and weaknesses of implemented controls and the business drivers for those controls that remediate access and services to and from County's IT infrastructure. The vendor should consider different assessment scenarios such as level of access and point of access during their assessments. The Technical Security Assessment Report should include:

    a. Network Topology

    b. Network Switches Configuration

    c. Endpoints access

    d. Firewalls Configuration

    e. IDP/IDS Configuration

    f. Router Configuration

    g. Virtual Private Network (VPN) Configuration

h. WLAN Configuration

i. Other Network based security controls e.g. Content Filtering, Antispam, etc.

2. **Host / Server Security Assessment** - Provides the County with a security focused host/server architecture review, with additional security-related information about the County's host/server operating system configurations that cannot be obtained through network scanning. The additional granularity of the host/server security assessment should enable the County to identify and assess the presence and effectiveness of technical controls and the level of compliance with County policies and other relevant industry standards and best practices. Focus should be given to:

   a. Hardening issues - Provide an in-depth review of a system's security configuration, and evaluating if available the security controls that are being used based on the roles and functions of the host.

   b. Identify known vulnerabilities and OS and 3rd party software issues.

   c. Identify host dependencies from the Service/End User standpoint and interconnection between multiple services which can compromise an end user service.

3. **Endpoint Security Assessment** – The vendor may choose a random number of workstations (focus area will be defined by project steering committee) and peripheral endpoints in different departments/divisions to perform the assessment. Provides the County with an assessment of endpoints/workstations and end user security industry standards and best practices, which incudes but is not limited to:

   a. Workstation Configuration

   b. Anti-Malware

   c. Endpoint Encryption

   d. User Rights (Local/Domain)

   e. Media Access

   f. Clean Desk Policy/Practice

   g. Password Practices

   h. OS and Third-Party Software Patching

   i. Peripheral Device (network printers, scanners) configuration

4. **Application Security Assessment**

   a. Conduct an Application Security Assessment that analyzes the Internet, Extranet, and Intranet applications for existence and strength of application security controls. Conduct this assessment in accordance to the OWASP top 10 reference and other baselines for application security (e.g. assessment of authentication mechanisms and authorization mechanisms, session context control mechanisms, audit logging, intrusion detection and deterrence).

b. Conduct an Application Security Assessments that targets the security capabilities of critical applications. Assess if the applications have capabilities to secure information/data communications and whether the capabilities have been fully utilized. To accomplish this, the Vendor must qualitatively assess vulnerabilities that exist within targeted applications relative to both technical and non-technical security controls.

c. For County in-house developed applications, the overall security framework used for the application development process must be reviewed.

d. The application security review should evaluate available security features and security-relevant configuration items within the application to conclude if those controls have been configured to provide the County with the level of protection required by business, regulatory, and corporate drivers.

C. Non-Technical Risk Assessment

The Vendor must review HIPAA Privacy and Security training and other security awareness efforts in the County to determine if there are gaps between training content and HIPAA Privacy and Security standards, state privacy and security statutes, and general level of information security awareness among different levels of County staff. The efficiency of training initiatives should also be evaluated.

The Vendor must perform awareness testing by conducting surveys of selected users to determine if they understand their basic security responsibilities, people to contact if they have questions, and where to obtain current Privacy and Security policies and procedures.

The Vendor must perform the following to effectively execute awareness testing:

1. **End User Security Awareness Assessment**

   a. Interview County personnel responsible for Privacy and Security to determine the techniques used for presenting security awareness.

   b. Review County policies for security awareness to determine if they contain the elements necessary for an effective security awareness program.

   c. Review security awareness presentations and other materials.

   d. In conjunction with Project staff develop and conduct surveys based on policies and awareness presentations that will be distributed to randomly selected employees. Assess survey results to determine a relative level of comprehension of the topics presented in security awareness materials**.**

   e. Provide Social Engineering assessment in order to evaluate County personnel's responses to unauthorized walk-up, phone, and/or email requests for sensitive information.

   f. Perform Social Engineering using deception techniques through phone and email transports to solicit sensitive information from County personnel by employing techniques (e.g., Phishing, Social Engineering, etc.). This mechanism should test the sensitivity level of employees to suspicious requests and evaluates if personnel response is consistent with County's stated security policies and security awareness trainings.

g. Recommend, in order of importance, the topics to be included in the training and awareness programs.

h. Describe how the County could incorporate program specific information into the training programs.

2. **Physical Security Assessment** - Physical security is one of the three basic tenets of HIPAA.

   a. The Vendor must evaluate the effectiveness of the physical controls in place at selected facilities as compared to HIPAA specifications.

   b. The Vendor must perform the physical security review by visiting facilities and documenting the physical security controls that are currently implemented.

   c. In conjunction with the social engineering review, the Vendor may also attempt to breach physical security controls in a non-threatening manner to determine if personnel are following physical security policies. Breaches may take the form of “tailgating” (following an authorized person through a doorway into a protected area), trickery, or walking into office areas where staff should challenge unauthorized people. The Vendor must compare the results of the walkthroughs to County policies and the HIPAA standards to identify those areas where physical controls are lacking or need reinforcement.