AGENDA ITEM NO.
C11

COUNTY OF HUMBOLDT

For the meeting of: April 3rd, 2018

Date: March 5, 2018

To: Board of Supervisors

From: Connie Beck, Director 3/12/18
Department of Health and Human Services

Subject: Agreement with Tevora Business Solutions Inc. for HIPAA Security Risk Assessment

RECOMMENDATION(S):

That the Board of Supervisors:

1) Approve the agreement with Tevora Business Solutions Inc. for fiscal year 2017-2018 to provide a Risk Assessment, External Penetration, and Internal Vulnerability Scanning service for DHHS-Information Services;

2) Authorize the Chairperson to execute three (3) originals of the agreement; and

3) Direct the Clerk of the Board to route two (2) fully executed originals of the agreement to the Department of Health and Human Services (DHHS) Contract Unit for forwarding to DHHS-Information Services.

SOURCE OF FUNDING:
Social Services Funds

Prepared by Aaron Crosby, Security Analyst CAO Approval

REVIEW:
Auditor MAM County Counsel JBB Human Resources TLB Other

TYPE OF ITEM:
___X___ Consent
_____ Departmental
_____ Public Hearing
_____ Other _____

PREVIOUS ACTION/REFERRAL:

Board Order No. _____

Meeting of: _____

BOARD OF SUPERVISORS, COUNTY OF HUMBOLDT
Upon motion of Supervisor Wilson Seconded by Supervisor Bass

Ayes Bass, Fennell, Sundberg, Bohn, Wilson
Nays
Abstain
Absent

and carried by those members present, the Board hereby approves the recommended action contained in this Board report.

Dated: 4/3/18
By: _____
Kathy Hayes, Clerk of the Board

DISCUSSION:
The Chief Information Security Officer (CISO) of County of Orange has vetted this vendor's professional service and provided Regional Cooperative Agreement (RCA) language to their contract to allow smaller counties the opportunity to complete the regulatory requirement of a HIPAA Security Rule Risk Assessment as required in 45 CFR 164.308(a)(1)(II)(A)-Risk analysis.

A HIPAA Security Rule Risk Assessment entails identification of risks that may impact the security and organizational objectives of confidential systems/data. Risk Analysis is an essential aspect of the IT security and risk management program and is required by the following:

- 45 CFR 164.308(a)(1)(II)(A)-Risk Analysis
- IRS publication 1075 section 9.3.14.2 – Risk Assessment
- State Administration Manual (SAM) sections 5305.6 and 5305.7
- DHCS 2016 Medi-Cal Privacy and Security Agreements section VII(A)

County of Humboldt is currently unable to meet these regulatory requirements to provide a Risk Analysis report to the California Department of Public Health Director, and State of California Office of Information Security. The report would also be required if audited by the Office of Civil Rights, the enforcement branch for HIPAA.

FINANCIAL IMPACT:
Approval of the agreement with Tevora Business Solutions Inc. for professional services is $67,910. This agreement will reside in fund 1160, Budget Unit 511 and be funded through a combination of federal, and state and local funds. There is no impact to the county general fund.

OTHER AGENCY INVOLVEMENT:

ALTERNATIVES TO STAFF RECOMMENDATIONS:
The Board could choose to not approve the agreement with Tevora Business Solutions Inc., however this is not recommended and will continue our non-compliance with Federal and State mandates which could result in reputational and financial harm when audited by these governmental bodies.

ATTACHMENTS:
Agreement for Services (3 originals)

STATEMENT OF WORK

2017 HIPAA and Penetration Test Services

This Statement of Work ("**SOW**") is entered into by and between Tevora Business Solutions, Inc. ("**Tevora**") and Humboldt County ("**Client**") on March 7, 2018 ("**SOW Effective Date**") Regional Cooperative Agreement RCA-017-17010018, attached hereto and incorporated herein by reference, between the parties dated as of April 11, 2017 ("**Agreement**").

1. Services

1.1 Service Description: Tevora will provide the following services to Client ("**Services**"):

HIPAA Security Risk Assessment

External Penetration Testing

External Penetration Test Remediation

Vulnerability Scanning

1.2 Timeline

The initial high-level timeline for the service(s) is reflected in the table below. Some of the work may be completed concurrently. This timeline reflects total effort in man days/weeks. The actual project completion time frame is dependent on timely decisions, remediation and approvals, when appropriate, by Client's management/Project Sponsor.

Service(s)	Estimated Effort
1) HIPAA Security Risk Assessment	5.5 weeks
2) External Penetration Testing	1 week
3) External Penetration Testing Remediation	1 day
4) Vulnerability Scanning	2 days

1.3 Service Locations, Hours and Travel:

i) Main client service operations are out of four (4) domestic locations in Eureka, CA.

ii) Tevora and Client anticipate that the professional services will be provided from both Tevora offices and Client offices. Project work to be performed at the Client facility(s) shall be performed during normal business hours: Monday through Thursday 8:00AM to 5:00PM and Friday 8:00AM to 1:00PM local time, excluding holidays.

iii) Where possible, work will be performed offsite to reduce travel expenses.

2. Parties' Obligations

2.1 Tevora' s Obligations:

i) Prior to commencement of any services, Tevora will provide Client notice of all personnel that Tevora intends to use in its performance of the Services, and Client will have the right to approve or disapprove which proposed individuals are staffed for such services. Additionally, any changes to Tevora staff assignment must be agreed upon by Client prior to changes taking effect.

ii) Whenever possible, Tevora will use previously created material to reduce effort.

2.2 Client's Obligations:

i) Client will provide adequate access to systems and personnel as required to perform the project objectives. This includes all network diagrams, documentation, policies, systems, network access, support staff, administrative staff and executive staff needed to complete the objectives of this SOW. Tevora cannot be held responsible for analysis of applications, systems, and networks to which Tevora has not been given access to.

ii) Client will provide necessary workspace and equipment to conduct onsite work, including (but not limited to) desk space, telephone, printer access, Project Management Tools access and conference room access as needed.

iii) Client will give Tevora a minimum of three (3) weeks' notice for onsite resource scheduling requests

3. Project Approach and Deliverables

3.1. HIPAA Security Risk Assessment

This project will focus on conducting a HIPAA risk assessment against all Client IT and Security systems and processes to identify the risks that may impact the security or objectives of the organization. The risk assessment will leverage the NIST 800-30 framework and HydraRisk Model for risk decisioning. Activities will include:

- Identification of project stakeholders, key client programs and business units to be included in the risk assessment process
- Interviews with key stakeholders and staff within IT and Information Security, and other business areas, to identify any objectives that may impact security and handling of ePHI (electronic personal health information) and PII (Personally Identifiable Information)
- Identification of the following:
    - All legal, regulatory and standard requirements applicable to the business
    - Outsourced security tools (up to 3) to be included in the risk assessment process
    - Internally managed security tools (up to 10) to be included in the risk assessment process
- Identification of strategic business objectives that may impact the environment. Which may include the following:
    - Cloud usage and/or transition
    - Mobile expansion
    - Cyber Security trends and standards (NIST CyberSecurity Framework)

  - Data sharing or market research
  - Data loss prevention for ePHI and PII
  - Technical changes
- Identification and classification of key assets within the Client's environment
- Evaluation of asset categories for common threats and vulnerabilities, organized into three primary areas:
  - Environmental
  - Technical
  - Human
- Identification and evaluation of process risks affecting organizations, including:
  - Emerging security trends that may affect the Client's environment
  - Service provider risk management and due diligence
  - Data movement throughout the organization
  - Access and authentication controls based on roles and function within the organization
  - Preventative and detective alerts and monitoring for security analytics
  - Incident management process, procedures and awareness
  - Effectiveness of the security awareness and training program
  - Security measurements and metrics reported and reviewed by management
  - Risk-based approach within Change Management and Control
- Review of existing security policies and documentation
- Review of the following security concepts to include:
  - Security Management
  - Security Responsibilities
  - Perimeter Security Controls
  - Network Segmentation and Architecture
  - Wireless Security
  - Workforce Clearance/Termination Procedures
  - Authorization and Supervision of Access to PII and IP
  - Log-in Monitoring
  - Password Management
  - Security Incidents
  - Malware Protection
  - Security Awareness Training
  - Risk Management and Analysis
  - Vulnerability Assessment
  - Contingency Planning
  - Data Backup and Retention
  - Disaster Recovery Plan
  - Emergency Mode Operation Plan
  - Testing and Revision Procedures
  - Applications and Data Critical Analysis
  - Facility Access Controls
  - Facility Security Plan
  - Workstation Use/Security Policies and Practices
  - Policies and Procedures for Device and Media Controls (Disposal/Reuse/Accountability)

  - Technical Policies to manage PII and PCI access (User ID, Emergency Access, Auto Log-off, Encryption)
  - Secure Transmission (Integrity and Encryption)
  - Breach Notification Plan/Procedures
- Identification, measurement and evaluation of risk based on Client's strategy and objectives
- Measurement of identified risks based on NIST principles
- Root cause categorization of identified risks
- Creation of recommended risk treatment to accommodate scalability and re-use across other systems

Deliverables:

HIPAA Assessment Report: a report that outlines the identified risks that may impact the security and organizational objectives of the Client's systems/data

Service	Deliverable	Client	Tevora
HIPAA Risk Assessment	HIPAA Risk Assessment Report	Assist	Primary

3.2. External Penetration Test

This portion of the project will focus on conducting an external network penetration test to determine the resiliency of the network perimeter against existing threats from remote Internet attackers. This is done by modeling all potential technical attack vectors with the goal of breaching the perimeter security and gaining unauthorized access to sensitive data. In addition to traditional direct attacks at the network, operating system and application level, certain Client-side tests will be conducted to determine the effectiveness of virus/malware screening systems, and e-mail proxies. Activities will include:

- Up to 50 network devices will be considered in scope for this external pen test
- External penetration testing from Tevora's offices to simulate an untrusted network attack to include:
  - Credentialed and non-credentialed testing
  - Manual and automated testing and use of commercial and open source tools
  - Use of information captured in the previous tasks to validate vulnerabilities, test exploitation, and measure effectiveness of controls
  - Creative techniques to include business logic analysis and manual exploit creation
- Objectives based testing designed to identify and validate high risk vulnerabilities to include:
  - Privilege Escalation
  - Sensitive Data Access
  - Data exfiltration

Deliverable:

External Penetration Test Report: This report will include an executive summary of findings, documentation of all testing results, and classification of findings using the

HydraRisk classification model. The report will also include exploit code examples and detailed remediation recommendations

External Penetration Test Report Addendum: Tevora will validate remediation of all external penetration test findings and update the External Penetration Test Report verifying that all findings have been remediated

Service	Deliverable	Client	Tevora
External Penetration Test	External Penetration Test Report External Penetration Test Report Addendum	Assist	Primary

3.3. Vulnerability Scanning

This portion of the project will focus on conducting a vulnerability scan. Activities will include:

- Enumeration of all services running on all in-scope IP addresses
- Vulnerability scanning and assessment of all identified services
- Up to one thousand (1,000) nodes will be considered in scope for this scan

Deliverable:

- Vulnerability Scan Report
  Host, port, and vulnerability level detail report organized by IP address

Service	Deliverable	Client	Tevora
Vulnerability Scanning	Vulnerability Scan Report	Assist	Primary

4. Pricing, Expenses and Requirements for Project Commencement

4.1 Pricing

This SOW is for work to be done on a fixed fee basis not to exceed $67,910 including expenses as outlined below.

Service	Deliverable(s)	Cost
1. HIPAA Security Risk Assessment (213 hours @ $230 per hour RCA 18.3)	• HIPAA Risk Assessment Report	$48,990
2. External Penetration Test (RCA 11.1)	• External Penetration Test Report	$12,000
3. External Penetration Test Remediation (RCA 11.4)	• External Penetration Test Report Addendum	$1,640
4. Vulnerability Scanning (16 hours @ $205 per hour RCA 18.2)	• Vulnerability Scan Report	$3,280
	Sub Total:	**$65,910**
	Estimated Expenses:	**$2,000**

Total:	**$67,910**

Pricing in this SOW is based on the following parameters. Tevora reserves the right to change pricing if there are any variations in scope.

Number of locations in-scope: 4

Number of disaster recovery locations: 1 AWS

Number of systems (i.e. Servers) and network devices: 65

Number of core applications: 40

Third-party IT services: AWS, Exchange Online, Citrix (Persimmony), Dell SecureWorks (IDS)

4.2 Expenses

i) This SOW authorizes up to USD $2,000 for reimbursed travel expenses to be calculated on an actual basis.

ii) All out of pocket expenses, including but not limited to travel and lodging, will be billed on a monthly basis.

iii) Each reimbursable expense will be supported by satisfactory documentation and be in accordance with Client's Reimbursement Policy

4.3 Requirements for Project Commencement

i) Payment for work performed under this SOW will be billed upon Client acceptance of individual deliverables 1 through 4 in Section 4.1 of this SOW. Payment on invoices will be due within 45 days of receipt (net 45).

ii) Any fees for third party licenses or services (e.g., software licenses, etc.) not specifically referenced in this SOW are NOT included in these costs and will be paid in advance if required to commence work. Client will pay vendors directly for any such costs, although Tevora can assist in procurement as required.

5. Term

Remediation Assistance hours will be available for a one (1) year term. The one-year term will be effective from the SOW Effective Date.

6. Project Management

6.1 Parties' Roles

Tevora and Client resources will work as a single team to produce timely and efficient deliverables, consisting of the following roles:

i) Tevora Roles

Project Lead

- Responsible for all deliverables
- Escalation point for all project issues
- Works with Project Sponsor to define vision, objectives, and delivery timelines
- Guides project team in the overall methodology and execution of project activities

Technical Lead

- Leads and executes all strategic and tactical objectives for the project
- Interfaces with project stakeholders
- Main contributor for all deliverable documentation
- Provides support to the Client team as needed

Project Manager

- Develops and maintains project plan and coordinates all parties
- Allocates resources, sets milestones, and identifies the critical project path
- Conducts regular meetings and provides updates on major milestone progress, budgets, and issue resolution

ii) Client Roles

Project Sponsor

- Working with Business Sponsors, sets overall vision, maintains authority over and responsibility for project, provides direction related to key decisions, addresses escalated issues, and ensures IT ownership
- Provide project closure approval

Project Lead

- Ensures IT engagement and secures key IT, compliance, and business resources
- Provides direction related to key project decisions, addresses escalated issues
- Sign-off on deliverables for all activities
- Review testing results
- Validate project communications

6.1 Project Communication

Project communication will occur through the following methods:

i) Weekly status meetings (for projects longer than 3 weeks)

ii) Weekly status updates into Client's EPM (Enterprise Project Management) system. If none is available updates will be sent via email.

iii) Ad-hoc status reports as requested

iv) Email or phone updates on particular issues as needed

6.2 Issue Resolution

Any project issues will be resolved through the following escalation sequence:

i) Tevora Technical Lead, and Client Project Sponsor will attempt to resolve issue internally with the project team

ii) If #1 does not resolve the issue, the Tevora Project Lead will work with the Client Project Sponsor for resolution

iii) If #2 does not resolve the issue, an Issue Resolution Meeting will be conducted with impacted project personnel and subsequent meetings will occur until the issue is resolved.

7. Acceptance of Deliverables

All deliverables are subject to acceptance as set forth in the Agreement. Acceptance of deliverables for this SOW will be documented by Client using the Tevora signoff forms. Upon completion of the deliverable, Tevora will provide Client with the applicable signoff form for signature.

8. Nuclear Free Humboldt County Ordinance Compliance

Tevora certifies by its signature below that it is not a Nuclear Weapons Contractor, in that Tevora is not knowingly or intentionally engaged in the research, development, production or testing of nuclear warheads, nuclear weapons systems or nuclear weapons components as defined by the Nuclear Free Humboldt County Ordinance. TEVORA agrees to notify Client immediately if it becomes a Nuclear Weapons Contractor as defined above. Client may immediately terminate this Agreement if it determines that the foregoing certification is false or if Tevora subsequently becomes a Nuclear Weapons Contractor.

[signature page follows]

SIGNATURES

HUMBOLDT COUNTY

("CLIENT")

By: _____
Authorized Signature

Name: Ryan Sundberg

Title: Chair, Humboldt County Board of Supervisors

Date: 4/3/18

Address: 825 5th St. Room 111
Eureka, Ca 95501

TEVORA BUSINESS SOLUTIONS, INC

("TEVORA")

By: _____
Authorized Signature

Name: Steve Stumpfl

Title: Executive Vice President, Sales

Date: 3/7/2018

By: _____
Authorized Signature

Name: Nazy Fouladirad

Title: CFO

Date: 3/8/18

Address: 1 Spectrum Point, Suite 200
Lake Forest, CA 92630

INSURANCE AND INDEMNIFICATION REQUIREMENTS APPROVED:

By: _____

Risk Analyst

Date: 3/19/18