Attachment C

# COUNTYOF ORANGE
# OFFICE OF INFORMATION TECHNOLOGY

# SUBORDINATE AGREEMENT
# MA-017-17011533
# BETWEEN
# THE COUNTY OF ORANGE
# AND
# TEVORA BUSINESS SOLUTIONS, INC.
# FOR
# CYBER SECURITY ASSESSMENT SERVICES

# SUBORDINATE AGREEMENT NO. MA-017-17011533
# BETWEEN
# THE COUNTY OF ORANGE
# AND
# TEVORA BUSINESS SOLUTIONS, INC.
# FOR CYBER SECURITY ASSESSMENT & AUDIT SERVICES

This Subordinate Agreement No. MA-017-17011533 for Cyber Security Assessment Services, hereinafter referred to as “Subordinate Agreement”, is made and entered into as of the date fully executed by and between the County of Orange, a political subdivision of the State of California, hereinafter referred to as “County”, acting through the County Executive Office/Orange County Information Technology (“OCIT”), and Tevora Business Solutions, Inc., with a place of business at 1 Spectrum Pointe Drive, Suite 200, Lake Forest, CA 92630 hereinafter referred to as “Contractor”, with County and Contractor sometimes referred to individually as “Party” or collectively as “Parties”.

This Subordinate Agreement is comprised of this document and the following Attachments, which are attached hereto and incorporated herein by reference:

## ATTACHMENTS

Attachment A: Scope of Work
Attachment B: Compensation and Payment
Attachment C: Regional Cooperative Agreement # RCA-017-17010018

## RECITALS

***WHEREAS***, on April 11, 2017, County, acting through County Executive Office/Orange County Information Technology (“OCIT”), and Contractor executed Regional Cooperative Agreement RCA-017-17010018, hereinafter referred to as “RCA”, for Cyber Security Assessment & Audit Services, effective for the period April 11, 2017 through April 10, 2020; and

***WHEREAS,*** Article 4 entitled, “Cooperative Agreement”, of the RCA allows other California local or state governmental entities to utilize the RCA with the same provisions and pricing; and

***WHEREAS***, County, acting through OCIT, and Contractor now desire to enter into this Subordinate Agreement for Cyber Security Assessment & Audit Services pursuant to the terms, conditions and pricing of the RCA, which is attached hereto and incorporated herein by reference as Attachment C.

**NOW THEREFORE**, the Parties mutually agree as follows:

1. **Scope of Work:** This Subordinate Agreement and its Attachments A, B, and C specifies the contractual terms and conditions by which County will procure Cyber Security Assessment & Audit Services from Contractor. The details of the services to be provided by Contractor are further outlined in Attachment A, entitled “Scope of Work”, attached hereto and incorporated herein by reference.

2. **Term of Subordinate Agreement:** The term of this Subordinate Agreement shall commence upon full execution of the Subordinate Agreement by both Parties, and shall be effective through April 11, 2017 through April 10, 2018, unless otherwise terminated by the County pursuant to the termination provisions of the RCA or renewed by a duly executed written amendment between the Parties according to RCA Article C. Any renewal of this Subordinate Agreement may require approval by the County of Orange Board of Supervisors. County is not obligated to provide a reason should it elect not to renew this Subordinate Agreement.

3. **Compensation & Payment:** Contractor agrees to provide Cyber Security Assessment Services in accordance with the terms and conditions of the RCA, including its attachments, and in line

with the pricing set forth in Subordinate Agreement Attachment B entitled, "Compensation and Payment", as they now exist or may hereafter be amended.

4. **Not to Exceed Limit:** The total amount of this Subordinate Agreement shall not exceed **$97,280.00**. The County shall have no obligation to pay any sum in excess of this amount unless authorized by written amendment signed by both Parties.

5. **Notices:** Any and all notices, requests demands and other communications contemplated, called for, permitted or required to be given hereunder shall be in writing, except through the course of the Parties project managers' routine exchange of information and cooperation during the terms of the work and services provided. Any written communications shall be deemed to have been duly given upon 1) actual in-person delivery, if delivery is by direct hand, 2) upon delivery on the actual day of receipt or no greater than four (4) calendar days after being mailed by US certified or registered mail, return receipt requested, postage prepaid, whichever occurs first, or 3) upon delivery via electronic mail with confirmation receipt from recipient. If notice is by US certified or registered mail, the date of mailing shall count as the first day. All communications shall be addressed to the appropriate party at the address stated herein or such other address as the Parties hereto may designate by written notice from time to time in the manner aforesaid.

Contractor:
Tevora Business Solutions, Inc.
Attn: Cindy Curley
1 Spectrum Pointe Drive, Suite 200
Lake Forest, CA 92630
Phone: 858-361-7743
Email: CCurley@tevora.com

County Program:
OCIT
Attn: Wilson Crider, County Designated Representative
1501 E. St. Andrew Pl., 1st Floor
Santa Ana, CA 92705
Phone: 714-567-6285
Email: Wilson.Crider@ceoit.ocgov.com

County Contracts & Purchasing:
OCIT/Contracts & Purchasing
Attn: Duyen Lac, DPA
1501 E. St. Andrew Pl., 2nd Floor
Santa Ana, CA 92705
Phone: 714-567-7443
Email: Duyen.Lac@ceoit.ocgov.com

## SIGNATURE PAGE

In WITNESS WHEREOF, the Parties hereto have executed this Subordinate Agreement on the dates shown opposite their respective signatures below:

**TEVORA BUSINESS SOLUTIONS, INC.***

*If the Contractor is a corporation, signatures of two specific corporate officers are required as further set forth.

The first corporate officer signature must be one of the following: 1) the Chairman of the Board; 2) the President; 3) any Vice President.

In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution demonstrating the legal authority of the signature to bind the company.

The second corporate officer signature must be one of the following: 1) Secretary; 2) Assistant Secretary; 3) Chief Financial Officer; 4) Assistant Treasurer.

Steve Stumpfe
Print Name

V.P. of Sales
Title

Signature

April 11, 2017
Date

Nazy Fouladirad
Print Name

President
Title

Signature

April 11, 2017
Date

*****************************************************************************

COUNTY OF ORANGE, a political subdivision of the State of California

Duyen Lac
Print Name

Deputy Purchasing Agent
Title

Signature

April 11, 2017
Date

# ATTACHMENT A
# SCOPE OF WORK

## A. SCOPE OF SERVICES:

Contractor shall provide all labor, materials, tools, equipment and travel necessary to perform Cyber Security Assessment Services as further outlined in this Subordinate Agreement.

## B. CONTRACTOR RESPONSIBILITIES:

Contractor shall provide:

1. Service Description: Contractor will provide the following services to County:

   DHS Cyber Resilience Procedure Review

   On-Site Validation of Physical Security Controls

   Vulnerability Assessment

   Software Application Security Assessment

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 County's Designated Representative.

| Service | Estimated Effort |
|---|---|
| 1) DHS Cyber Resilience Procedure Review | 3.5-4 weeks |
| 2) On-Site Validation of Physical Security Controls | 3-4 days |
| 3) Vulnerability Assessment | 1.5-2 weeks |
| 4) Vulnerability Assessment Remediation Validation | 1 day |
| 5) Software Application Security Assessment | 2.5 weeks |
| 6) Software Application Security Assessment Remediation Validation | 1 day |

3. Service Locations, Hours and Travel:

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

   ii) Contractor and County anticipate that the professional services will be provided from both Contractor offices and County offices. Project work to be performed at the County 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.

## C. PARTIES' OBLIGATIONS:

1. Contractor' s Obligations:

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

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

2. County's Obligations:

   i) County 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. Contractor cannot be held responsible for analysis of applications, systems, and networks to which Contractor has not been given access to.

   ii) County 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) County will give Contractor a minimum of three (3) weeks' notice for onsite resource scheduling requests.

## D. PROJECT APPROACH AND DELIVERABLES:

1. DHS Cyber Resilience Procedure Review

   This portion of the project will focus on reviewing the current policies and the associated security procedures according to DHS Cyber Resilience requirements. Recommendations for controls and modifications will be provided for policy and procedure updates. Activities will include:

   - Interviews with key stakeholders and subject matter experts to capture any Information Security, IT and relevant business requirements, as needed
   - Identify the scope of the DHS Cyber Resilience Review Self-Assessment (CRR Self-Assessment) with stakeholders
   - Review the DHS Cyber Resilience Self-Assessment criteria to determine the current state of policies and procedures against the DHS Cyber Resilience
   - Ensure content includes applicable security requirements for DHS Cyber Resilience, including:
     - Asset Management
     - Controls Management
     - Configuration and Change Management
     - Vulnerability Management
     - Incident Management
     - Service Continuity Management
     - Risk Management
     - External Dependencies Management
     - Training and Awareness
     - Situational Awareness
   - Review of specific policies including:
     - Security Policy Framework (Governing document)
     - Risk Management and Assessment
     - Business Continuity Plan
     - Acceptable Use Policy
     - Data Classification
     - Malware Protection
     - Laptop and Workstation Security
     - Configuration Management
     - Vulnerability Management

  - Secure Disposal of Data and Media
  - Security Incident Response Plan and Notification
  - Vendor and Third-Party Management
  - HR Security
  - Onboarding and Termination
  - Access Control and Monitoring
  - Training and Awareness
  - Secure Coding
  - Mobile Device Management
  - Network Security

- Definition of the formal management review process for policies, processes and controls; including identification of policy owner, and the impact of any changes to existing or new federal, legal, privacy and standards requirements

- Identification of gaps in the current policies and procedures

Key Project Considerations

- Interviews with County's managed service providers, Atos Governmental IT Outsourcing, LLC (network) and Science Applications International Corporation (servers) will be in scope for this DHS Cyber Resilience Procedure Review

**Deliverable:**

DHS Cyber Resilience Self-Assessment Criteria Report: Generate a report based on the scope determined and information provided by stakeholders. The report will include any gaps with requirements, an overall score and score per domain area.

| Service | Deliverable | County | Contractor |
|---|---|---|---|
| DHS Cyber Resilience Procedure Review | DHS Cyber Resilience Self-Assessment Criteria Report | Assist | Primary |

2. On-Site Validation of Physical Security Controls

This portion of the project will focus on conducting a physical penetration test at 3 locations to identify vulnerabilities associated with staff's ability to follow documented policies and procedures, and security best practices. A physical penetration test focuses primarily on the human element of security, and secondarily on physical security mechanisms in place to protect personnel and assets. Attempts will be made to exploit any potential staff and current physical security weaknesses. Activities will include:

- Objectives based physical penetration testing to include:
  - Accessing building and offices
  - Sensitive data access
  - Exfiltration of sensitive data
  - Setup of rogue access point(s)
  - Setup of rogue terminal(s)
  - Document physical security weaknesses

- Bypassing physical security mechanisms (i.e. locks, gates, cameras, and security guards) to gain access without causing property damage

Key Project Considerations:

- Contractor will attempt to gain physical access to three (3) buildings and will not be limited to any rooms or offices within the building to achieve their objective(s)

  **Deliverables:**

  Physical Security Penetration Test 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 social engineering and physical security exploit examples and detailed remediation recommendations.

| Service | Deliverables | County | Contractor |
|---|---|---|---|
| On-Site Validation of Physical Security Controls | Physical Security Penetration Test Report | Assist | Primary |

3. Vulnerability Assessment

This portion of the project will focus on conducting a vulnerability assessment to determine if current network security controls are vulnerable to actionable attacks from a malicious intruder that has gained access to the network either physically or virtually. This level of testing validates corporate security policy and development standards by identifying the resiliency of the internal network against determined intruders. Activities will include:

- Up to 40 Servers, 1 Operating System, 800 Workstations running Windows, 20 Network Devices, 1 mainframe, 1 Enterprise Firewall, and 1 database will be considered in scope for this vulnerability assessment
- Internal vulnerability testing from the County's office, or datacenter, covering production servers and network devices 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:**

  Vulnerability Assessment 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

Vulnerability Assessment Report Addendum: Contractor will validate remediation of any findings the County requests be validated and update the Vulnerability Assessment Test Report verifying that all findings have been remediated

| Service | Deliverable | County | Contractor |
|---|---|---|---|
| Vulnerability Assessment | Vulnerability Assessment Report<br>Vulnerability Assessment Report Addendum | Assist | Primary |

4. Software Application Security Assessment

This project will focus on conducting a security assessment for vulnerabilities that could lead to unauthorized access of the application or the supporting environments. Contractor will use a combination of tools, utilities and methodologies to review the various potential points of security failure. Activities will include:

- One (1) application will be considered in scope for testing:
  - OC Expediter
- Web application penetration testing from Contractor's offices to simulate an untrusted network attack to include:
  - Credentialed and non-credentialed testing of
    - Web servers
    - Application servers
    - Database server
    - Middleware or support infrastructure
    - Firewall, switches and routers that are used to segment and route application traffic
  - Manual and automated testing and use of commercial and open source tools
- Objectives based testing of all OWASP Top Ten vulnerabilities for web applications to include:
  - Injection
  - Broken Authentication and Session Management
  - Cross-Site Scripting (XSS)
  - Insecure Direct Object References
  - Security Misconfiguration
  - Sensitive Data Exposure
  - Missing Function Level Access Control
  - Cross-Site Request Forgery (CSRF)
  - Using Components with Known Vulnerabilities
  - Un-validated Redirects and Forwards
- Scanning for and identification of well-known server, code engine, and database vulnerabilities
- Identification of, and attempting to compromise, any server and administration flaws
- Analysis of basic functionality of the user interface, normal application behavior, and the overall application architecture for potential security vulnerabilities

- Analysis of data communications between the application and databases or other back-end systems wherever possible
- Manual analysis of all input facilities for unexpected behavior such as SQL injection, arbitrary command execution, and unauthorized data access
- Analysis of user and group account authentication and authorization controls to determine if they can be bypassed
- Identification of information leakage across the application's boundaries, including the capability to enumerate other users' data and "show code" weaknesses that reveal internal \ application logic
- Identification of where error handling is insufficient or reveals too much sensitive information
- Detection of opportunities to write to the host file system or execute uploaded files
- Identification of product sample files, application debugging information, developer accounts or other legacy functionality that allows inappropriate access
- Attempting to determine if fraudulent transactions can be performed
- Attempting to view unauthorized data, especially data that should be confidential
- Examination of County-side cached files, temporary files, and other information that can yield sensitive information or be altered and re-submitted
- Analysis of encoded and encrypted tokens, such as cookies, for weakness or the ability to reverse engineer

Key Project Considerations:

- The OC Expediter application is in Client's Microsoft Azure environment
- Client to provide third-party "right-to-test" proof prior to testing

**Deliverables:**

Software Application Security Assessment Report: A report that includes an executive summary on findings, documentation of the County's existing security posture, and provides exploit codes examples and remediation recommendations

Software Application Security Assessment Report Addendum: Contractor will validate remediation of all assessment findings deemed necessary by the County and update the Software Application Security Assessment Report verifying that all findings have been remediated.

| Service | Deliverables | County | Contractor |
|---|---|---|---|
| Software Application Security Assessment | Web Application Penetration Test Report<br>Web Application Penetration Test Report Addendum | Assist | Primary |

## E. TERM:

Vulnerability Assessment and Software Application Security Assessment validation testing and addendum reports will be available for a one (1) year term. The one-year term will be effective from the date of acceptance of the Vulnerability Assessment Report and Software Application Security Assessment report.

## F. PROJECT MANAGEMENT:

1. Parties' Roles

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

i) Contractor 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 County 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) County 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

2. 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 County'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

3. Issue Resolution

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

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

ii) If #1 does not resolve the issue, the Contractor Project Lead will work with the County 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.

## ATTACHMENT B
## COMPENSATION & PAYMENT

I. **COMPENSATION:** This is a fee for service Contract between County and Contractor for services defined in Attachment A - Scope of Work.

Contractor agrees to accept the specified compensation as set forth in this Subordinate Agreement as full remuneration for performing all services and furnishing all staffing and materials required, for any reasonably unforeseen difficulties which may arise or be encountered in the execution of the services until acceptance, for risks connected with the services, and for performance by Contractor of all its duties and obligations hereunder. The total amount of this Subordinate Agreement shall not exceed **$97,280.00**. The County shall have no obligation to pay any sum in excess of this amount unless authorized by written amendment signed by both Parties.

Contractor shall bill County for services rendered according to the rates listed below.

| Service Description | Deliverable(s) | Cost |
|---|---|---|
| 1) DHS Cyber Resilience Procedure Review | • DHS Cyber Resilience Self-Assessment Criteria Report | $33,200.00 |
| 2) On-Site Validation of Physical Security Controls | • Physical Penetration Test Report | $12,100.00 |
| 3) Vulnerability Assessment | • Vulnerability Assessment Report | $18,700.00 |
| 4) Vulnerability Assessment Remediation Validation | • Vulnerability Assessment Report Addendum | $1,640.00 |
| 5) Software Application Security Assessment | • Software Application Security Assessment Report | $30,000.00 |
| 6) Software Application Security Assessment Remediation Validation | • Software Application Security Assessment Report Addendum | $1,640.00 |
| | **Total:** | **$97,280.00** |

II. **Payment Terms:** Invoices are to be submitted in arrears, after services have been completed. Payment will be net forty-five (45) days after receipt of an invoice in a format acceptable to the County of Orange. Invoices shall be verified and approved by the County and subject to routine processing requirements. The responsibility for providing an acceptable invoice to the County for payment rests with the Contractor. Incomplete or incorrect invoices are not acceptable and will be returned to the Contractor for correction.

Billing shall cover goods and services not previously invoiced. The Contractor shall reimburse the County of Orange for any monies paid to the Contractor for good or services not provided or when goods and services do not meet the Contract requirements.

Payments made by the County shall not preclude the right of the County from thereafter disputing any goods or services involved or billed under this Contract and shall not be construed as acceptance of any part of the goods or services.

III. **Invoice Instructions:** Each invoice must be on Contractor’s letterhead and have a unique number and shall include the following information:

a. Contractor’s name and address
b. Contractor’s remittance address
c. County Subordinate Agreement #MA-017-17011533
d. Contractor’s Federal I.D. number
e. Date of Order/Service date(s)
f. Product/service description, quantity, prices
g. Total invoice amount

Invoices are to be forwarded to:

County of Orange
OCIT/Budget & Finance Division
Attention: Accounts Payable
1501 E. St. Andrew Place, Suite 200
Santa Ana, CA 92705

# ATTACHMENT C
# REGIONAL COOPERATIVE AGREEMENT RCA-017-17010018