FIRST AMENDMENT TO AGREEMENT NO. 13-3188
BETWEEN THE CITY OF LOS ANGELES
AND
ACCUVANT, INC.

THIS FIRST AMENDMENT to Agreement No. 13-3188 is made and entered into by and between the CITY OF LOS ANGELES, a municipal corporation ("City"), acting by and through its Board of Harbor Commissioners ("Board"), and ACCUVANT, INC. ("Consultant") as follows:

1. Section III, subsection B, "EFFECTIVE DATE AND TERM OF AGREEMENT" is hereby amended by increasing the term of this Agreement from a period of "no later than one (1) year" from the date of execution to a period of "no later than two (2) years" from the date of execution. The term of this Agreement will thus expire on December 12, 2015, unless terminated earlier under the provisions of Section III or Section IV of this Agreement.

2. Section V. "COMPENSATION AND PAYMENT", Subsection B is hereby deleted in its entirety and replaced with the following:

> "B. The maximum payable under this Agreement, including reimbursable expenses (see Exhibit B), shall be Four Million One Hundred Forty-Nine Thousand Eight Hundred Thirteen Dollars and Twenty Cents ($4,149,813.20) for Phase I and II."

3. Exhibit A. "SCOPE OF WORK" is hereby amended by adding the attached "EXHIBIT A: SCOPE OF WORK PHASE II" as pages 9 – 25 of Exhibit A.

4. Exhibit B. "COMPENSATION RATES AND FEES" is hereby amended by including the attached "Exhibit B: Compensation Rates and Fees Phase II" as page 2 of Exhibit B.

Except as amended herein, all remaining terms and conditions of Agreement No. 13-3188 shall remain in full force and effect.

////

////

////

////

IN WITNESS THEREOF, the parties hereto have executed this First Amendment to Agreement No. 13-3188 on the date to the left of their signatures.

THE CITY OF LOS ANGELES, by its Board of Harbor Commissioners

Dated: _____, 2014

By: _____
Executive Director

Attest: _____
Board Secretary

ACCUVANT, INC.

Dated: May 9, 2014

By: Pat Farrelly

Patrick Farrelly, Director of Legal Affairs
(Print/type name and title)

Attest: Jennifer Dewar

Jennifer Dewar, Director of Operations
(Print/type name and title)

APPROVED AS TO FORM AND LEGALITY

May 13, 2014

MICHAEL N. FEUER, City Attorney
JANNA B. SIDLEY, General Counsel

By: JTD for
JOHN T. DRISCOLL, Deputy

JTD/HJS:jpr
05/08/14
Attachments

Account #	54310 & 59994	W.O. #	25260
Ctr/Div #	1179	Job Fac. #	635-00
Proj/Prog #	624		

Act 54310
Act 59994

Budget FY:	Amount:
14/15	$ 900,000
14/15	$ 1,100,000
TOTAL:	$ 2,000,000

For Acct/Budget Div. Use Only:
Verified by: Julie Yano
Verified Funds Available: Maria Gregorio
Date Approved: 5/13/14

EXHIBIT A: SCOPE OF WORK PHASE II

Project Description

The Consultant shall provide the following:

1. Hardware, Software, Supplies, Installation and Integration Services to Enhance the Cyber Security Operation Center Capabilities

1.1 Cyber Security Operations Center Audio/Video System Build Out

Tasks and Deliverables

1.1.1 Video Display Wall

- 6 LED-based 55" full HD resolution (1920 x 1080) large-format 24/7-rated ultra narrow bezel (5.5mm) panels arranged in a 2-high by 3-wide matrix and hung on large fusion scissor wall mounts. This creates an overall resolution of 5,760 x 2,160 for a total of nearly 12.5 million pixels.
- Windows 7-based Mauell Nexus 550 display wall controller (w/ upgraded configuration + remote racking).
- Display Wall Controller software
- DVI cabling
- Miscellaneous cabling and mounting hardware

1.1.2 Audio System

- A programmable Digital Signal Processing (DSP) system that allows for the control of individual sources as well as room audio from each operator desk.
- A programmable controller for the DSP system that will be located at each desk position and one (1) along the wall at TBD location.
- Each Operator Position will be supplied with low profile hi-fidelity desktop speaker designed to go under the monitors.
- 8 ohm 4 channel Amplifier to be used with room speakers
- 2 Surface mount speakers to used with amplifier
- Miscellaneous cabling and mounting hardware included

1.1.3 Remote Graphics Unit (RGU) System and Extended Warranty

- Four- Head RGU Hardware
- PC Host Adapters
- Remote KVM software
- Extended Warranty for 55" LED-based full HD ultra-narrow bezel LCD panels for two (2) additional years, combined with the included Video Manufacturer three (3) year warranty will provide five (5) years of coverage of warranty coverage
- Mauell Nexus 550 DWC Extended Warranty for four (4) years, combined with the included Mauell one (1) year warranty will provide five (5) years of warranty coverage

1.2 SOC Collaboration and Enhancement Solution

Consultant shall provide the following:

- Videoconferencing solution that is compliant with H.323, H.320 and Session Initiation Protocol (SIP) and is designed to work with the existing flat-panel, Wall-mounted video wall, and for both audio and video communications.
- Supply and install 6 solar shades and 6 blackout shades for SOC facility security.
- Supply equipment and installation services for SOC facility enhancement.

2. Provide Professional Services and Ongoing Support to Improve Cyber Security

2.1 System Support and Maintenance Extension Services

Consultant shall provide 24 months extension of system warranty support and maintenance for the following products and services:

Part Number	Description
SA-S4H-P-CONE1	S4S HeadUnit Pkt Concentrator EnMnt1M
SA-S4H-P-DECE1	Series4S HeadUnit Pkt Decoder EnMnt1M
SA-S4H-ASE1	Series4S HeadUnit-Analytics Svr 10 Enhanced Maintenance 1 MO
SA-HPD12H1E1	High Perf DirAttch Capacity EnMnt1M
SA-HDD32-LPE1	32TB VHiDenDAC4PktDec EnMnt1M
NWA200-N-8iE1	NetWitness 1MO Mnt NWA200-N-8iE1 Enhanced

SMC-10GE-FE1	SMC-10GE-F Enhanced Maint 1 Mo.
NW LIVE-E-1MO	NetWitness 1YR Enhanced NetWitness Live
NW LIVE-B-1MO	1MO NETWITNESS LIVE BASIC
THR-1500-P-MNT	MNT THREAT 0-1500 PERP BASIC PER MONTH PRICING
ODA-1500-P-MNT	ODA 0-1500 Perp Basic Maint
BLP-1M-PB	Basic support per month

ProSecure Services

ProSecure Consulting is a partnership that is custom tailored by clients to meet their specific needs on an ongoing basis. Based on conversations with Port of Los Angeles, the initial effort to be performed under this agreement is targeted to include (but is not limited to) the following:

- ArcSight Tuning and implementation
- Version upgrades for security Solutions
- Security policy and procedure review and development
- Deployment and integration of new security solutions

Despite the focus of the initial effort on the tasks outlined above, the services that can be leveraged under the ProSecure Consulting agreement can span a variety of Accuvant services practice areas, including:

- Enterprise Risk – helping organizations build and manage information security and risk management programs
- Incident Response & Malware – responding with forensics and reverse engineering skills to tackle business critical incidents
- Technology Services – helping with deploying and integrating technologies successfully within client existing environments
- GRC – helping set up, use and manage your GRC tools and automating policy management audits
- Provide one thousand hours of consultation and support for existing and newly implemented security solutions including but not limited to the following technologies:
  - Intrusion Prevention Technologies
  - Security Incident and Event Management
  - Malware Analysis Technologies
  - Firewalling Technologies
  - Vulnerability Management

Enterprise Staffing

Port of Los Angeles has requested assistance in the initial implementation and running of the Security Operations Center. This requirement requires a skilled resource be allocated to assist as an individual contributor within the SOC. This requirement requires at least an individual with the following qualifications:

- Handles escalated incidents from helpdesk/deskside and end users
- Able to reliably monitor and analyze specified data sources
- Able to interpret common attacks and exploits, including:
- Spear phishing
  - Drive-by compromises
  - Malware infection
  - Exploit kit exposure
- Able to consistently follow incident monitoring processes and procedures
- Technically proficient with interpreting the output of all monitored security tools, including:
  - Antivirus
  - IDS
  - SIEM
  - Mail filters
  - Proxy Deliverables
- Able to demonstrate mastery of Tier 1 Monitoring Analyst and Tier 2 Incident Handler responsibilities
- Able to plan and coordinate response activities during an enterprise-wide breach
- Technically proficient with the analysis of:
  - Network data (pcap, netflow)
  - Host data (live analysis, volatile data, prefetch, memory)
  - Authentication data and logs (LDAP, Active Directory)
- Able to document and communicate incident status updates, for non-technical personnel
- Able to create consistent and complete incident reports
- Responsible for monitoring escalated event alerts
- Ability to place blocks in firewalls & content filters
- Provide four thousand hours of on-site support and knowledge transfer

2.2 Security Program Alignment and Threat Intelligence

The execution of these tasks will support the Port of Los Angeles alignment with the recently released NIST Cyber Security Framework. The tasks include the following:

Task 1: Security program and operations alignment with NIST framework

Checkpoint assessment of Port of Los Angeles' Security Operations Program with correlation of findings to the NIST Cyber Security Framework.

Deliverables:

- Documented Current State and Prioritized list Identify Gaps
- Rate current State Maturity Model
- Align Maturity to NIST Cyber Security Framework
- Develop Recommendations for Improvement

Task 2: Threat intelligence

Develop a threat intelligence operation to include the following:

- Develop a process to consume shared threat intelligence data
- Create a repository to store threat intelligence data
- Developed a process to update its security tools with gained threat intelligence data
- Develop a process to historically look for IOC's

The following deliverables will be included in this engagement:

Tasks	Deliverables
1. Security program and operations alignment with NIST framework	1 Document Current State and Identify Gaps 2 Rate Current State Maturity Model 3 Align Maturity to NIST Cyber Security Framework 4 Recommendations for Improvement
2. Threat Intelligence	1. Threat Intelligence Methodology to include: • IOC Historical Look Up Process • Security Tool Updates with Threat Intel Data Process

	• Shared threat intelligence data consumption 2. Threat Intelligence Repository

2.3 Enterprise Security Assessment

Accuvant has developed a phased assessment approach that is extremely effective for testing and improving the security of enterprise IT assets derived from years of experience and following key guidelines developed by groups such as NSA, OISSG, OWASP, WASC, OSSTMM, CLASP and MSDN. The methodology executed for this engagement will focus on black-box penetration testing of the Port of Los Angeles perimeter environment. Throughout the technical testing phases, Accuvant assessors will attempt to catalog, then penetrate or circumvent existing security mechanisms by using software tools and exploit scripts that are similar to those used by attackers.

Pre-Engagement Phase

Kick-Off Call

This pre-engagement call allows Accuvant consultants to gather the detailed information about the client's environment necessary to perform the project. Accuvant consultants will drive this discussion by going through a pre-engagement checklist with client personnel. The primary goals are to confirm the scope of work has been accurately captured in the project proposal and to identify any significant obstacles to completion prior to beginning the engagement.

Remote Network Testing Phase

Asset Testing

- Information Gathering - Accuvant will perform comprehensive information gathering, data mining procedures and device discovery review both in the public domain and targeting the subnet ranges supplied by Port of Los Angeles.
- Asset Identification – Accuvant will perform a scan to identify testing targets based on common open TCP ports across the provided external subnets.
- Vulnerability Discovery - Accuvant will perform detailed security analysis and vulnerability scanning using a comprehensive suite of commercial and open source tools targeting externally visible devices.

- Confirmation & Manual Testing - All identified vulnerabilities will be reviewed and validated to eliminate false positives. Manual testing procedures will also be executed to identify flaws not easily identifiable with automated tools and coordinated exploitation of targeted issues will be performed to demonstrate impact and allow for further vulnerability exploitation testing exercises (if desired).

Focused Penetration Testing

Use of common attack methodologies and manual exploitation attempts to try and circumvent existing security mechanisms protecting the systems exposed to the Internet.

Web applications identified during Asset Identification and Asset Testing activities will be confirmed with the client before any manual testing of application injection points is performed. This exercise is not intended as a comprehensive application vulnerability Smoke Test as it will focus primarily on compromising the application's host system.

Web Application Testing Phase

Web Application Security Smoke Test

- Targeted Scanning – Targeted web application scanning to discover vulnerabilities present within the application. The scans will be performed using a set of qualified web application testing tools and focus on a single user role. The selected user role should represent the largest user population or highest risk. Scanning configuration will be based on the OWASP Top 10 vulnerability list.
- Application Walkthrough – The application will be manually walked with the scanning tools and monitored during the scan for errors. This effort ensures that the tools are performing properly and that if there are areas within the application that would benefit from manual testing that they are considered by the assessor.
- Review & Manual Confirmation – Previously identified vulnerabilities are reviewed and validated to ensure that scanning tool false positives are acknowledged and removed.

Wireless Testing Phase

Identification & Analysis

- Access Point Discovery - Accuvant will identify, enumerate and analyze authorized wireless infrastructure and un-authorized Access Points. Once enumerated, this activity will provide

an analysis of the traffic that is visible to users within the wireless environment based on the initial access obtained.

- RF Signal Range Testing – Using information gathered during the discovery component, as well as leveraging multiple cards, software, and antenna, an analysis will be performed on the wireless signal strength and availability outside the physical confines of the acceptable coverage area.

Architecture Review

- Configuration Review – Review of sample AP and client configurations looking for common configuration errors and deviations from security best practices. This review will provide valuable insight into potential technical and non-technical deficiencies that can compromise the security of the wireless architecture.
- Wireless Architecture and Policy Review - Gather information about the current capabilities of the wireless network architecture and perform a gap analysis between industry best practices/pertinent controls, as well as and the organizations current posture and wireless policies (if applicable).

Penetration Testing & Exploitation

- Penetration Testing – This component of the assessment process is to determine if the security measures can be bypassed or circumvented. Accuvant will attempt to exploit weaknesses and/or crack the encryption to gain access to corporate resources via the wireless network. A wide range of commercial and public scanning and exploit tools (e.g. Aircrack, Kismet, Asleap, Karmetasploit, Ettercap, CoWPaAtty) are used to ensure comprehensive results and to mirror the types of probing that wireless environments receive every day.
- Controlled Exploitation – Following the penetration testing and subsequent access obtained (if any), this component will provide an analysis of the security of the assets that are accessible once attached to each of the wireless networks being examined.

<u>Onsite Network Testing Phase</u>

Asset Testing

- Asset Identification – Accuvant will perform a scan to identify testing targets based on common open TCP ports across the provided internal subnets.

- Servers – Accuvant will perform detailed vulnerability discovery and scanning using a comprehensive suite of commercial and open source tools targeting server-based systems.
- Workstations – In addition to the comprehensive security testing executed on the server based systems in the environment, this phase will execute thorough vulnerability scanning, confirmation and manual testing techniques targeting a representative sampling of a minimum of 10% of the workstations present in each environment to be tested. For the purposes of this assessment, this effort is expected to encompass a sampling of the total workstations.
- IP Enabled Devices – In addition to the server and workstation testing, Accuvant will perform vulnerability scanning across additional IP-enabled devices (e.g. printers, phones, cameras, network device management) within the address ranges specified.
- Confirmation & Manual Testing - All identified vulnerabilities will be reviewed and validated to eliminate false positives. Manual testing procedures will also be executed to identify flaws not easily identifiable with automated tools and coordinated and controlled exploitation of targeted issues will be performed to demonstrate impact and allow for further vulnerability exploitation exercises (if desired).
- Authenticated Scanning – Where the standard vulnerability testing, confirmation and exploitation targets vulnerabilities and configuration errors as seen by the majority of the environment users, this phase will perform additional scanning on those systems using 'Administrator' level credentials in order to provide a comprehensive analysis of missing patches, potential vulnerabilities and configuration-errors that may deviate from best-practices or Port of Los Angeles standards and control requirements.

Focused Penetration Testing

Use of common attack methodologies and manual exploitation attempts to try and circumvent existing security mechanisms protecting the systems accessible on the internal network.

Social Testing Phase

User Email Phishing

This social engineering scenario will leverage a targeted phishing email scheme to take advantage of the environment users in order to gain access to sensitive information or targeted data. All exercises will be closely coordinated with client personnel prior to execution.

User Pre-Text Calling

This social engineering scenario will leverage telephone communication to take advantage of the environment users in order to gain access to sensitive information or targeted data. All exercises will be closely coordinated with client personnel prior to execution.

Architecture & Configuration Review Phase

Architecture & Design Review

An analysis of the documented network infrastructure, the Architecture and Design Review identifies gaps in security controls through interviews with key information asset owners and security staff coupled with an evaluation of the relevant network diagrams.

Findings Gap Analysis

Gather Input & Documentation

A document collection sheet will be distributed in order to collect relevant policies, standards and procedures for review. The findings from the technical testing will also be collected and reviewed relative to the baseline established.

Determine Findings Gap

Accuvant consultants will assess the information gathered against ISO controls, and Internal Security Policies, as well as industry best practices, and then align the list of vulnerabilities in each of the controls areas.

Security Coverage Gap Analysis

Using the information gathered, Accuvant will perform a gap analysis and about the current capabilities of Port of Los Angeles's existing security environment, processes, controls and network architecture and utilize the findings as part of the security roadmap.

Security Program Review Tracking Matrix

A completed tracking matrix will be provided, showing current state of compliance, comments and recommendations. This tracking matrix is interactive and can be updated by Port of Los Angeles as improvements are made in the security program. The matrix has automated charts and graphs to show remediation progress.

Follow-Up Remediation Testing

Remote Remediation Validation

Following any required remediation, a single re-test of pertinent findings will be performed remotely to ensure the changes implemented are effective. The original deliverable will be updated to note the outcome of the re-test.

Note: Retesting will be performed within 30 days after the completion of primary testing and final delivery of findings documentation.

Deliverables:

Status Reports

Accuvant's assessors deliver daily or weekly status reports to our primary client contact detailing activities, what is planned for the following day or week, as well as any issues which have arisen that may delay the on-time completion of the engagement.

All communication is secured utilizing industry accepted encryption software to ensure critical information is not compromised.

Technical Findings Document

A single document detailing the technical findings and recommendations regarding any identified weaknesses in the environment. The document will also articulate the work performed, list the tools used and link to all relevant raw data captured during the engagement. The final report will be created using Accuvant's standard format and presented to Port of Los Angeles as a PDF within two weeks of the conclusion of the overall effort.

Vulnerability Tracking Spreadsheet

A spreadsheet will accompany the comprehensive report. The spreadsheet will contain the findings for each phase of the assessment. The spreadsheet format will facilitate sorting findings by IP address, vulnerability title and description, severity rating, software patch versions if applicable, etc.

Executive Summary

A single executive summary will be produced at the conclusion of the assessment summarizing the objectives of the engagement, work performed, findings and remediation strategy.

Customer Summary

A single customer facing document summarizing the effort and methodology that was executed and provides assurance that the customer organization actively performs their due diligence with regards to third-party validation of information security controls (relative to those phases included in the given assessment project). The document will be created using Accuvant's standard format and presented to Port of Los Angeles as a PDF.

2.4 Cyber Security Framework implementation

Consultant shall provide the consulting services to assist Harbor Department to implement ISO 27001 based Information Security Management System (ISMS) best practices.

This service includes but not limited to the following activities:

- Establish ISMS policy, objectives, processes and systems and procedures relevant to managing risk and improving information security
- Recommend actionable steps to implement and operate the ISMS policy, controls, processes and systems and procedures
- Co-ordinate with security team to define the scope and boundaries of the ISMS
- Develop criteria for accepting risks and identify the acceptable levels of risk
- Prepare a Statement of Applicability (SOA)
- Prepare a statement of exclusion of any control objectives and controls in SOA with the justification for their exclusion
- Assist with completing documentation, procedures required by ISO 27001
- Work with Port of Los Angeles security team to engage external certification agency for certification audit

<u>Deliverables:</u>

Develop Compliance Roadmap

- Maturity or current level of implementation of control

- Risk level associated with absence of control
- Resources required to implement
- Logical progression of activities
- Statement of Applicability (SOA)

Project Report

- Executive Summary
- Detailed Findings
- Compliance Roadmap

Formal Presentation

3. Training and Knowledge Transfer

The Port of Los Angeles is implementing a Security Operations Center and as per Phase II of the project it is required to provide information security training, best practices, and certifications in-line with industry best practices. These certifications will include but not limited to industry best practice training in reference to Cyber Security Hacking techniques, Defensive techniques, training in reference to products deployed in the environment and information security standards and process methodologies will be included in the training. Provide staff development in relation to daily operational cyber security methodologies. The training is to facilitate the adherence to the new information security regulations and standards such as NIST, ISO 27001/2, and COBIT.

The trainings will be provided to Port of Los Angeles information security staff. Accuvant shall provide the training vouchers and/or proof of registration. Accuvant will co-ordinate with the Port's project manager for the scheduling and availability of the staff.

Deliverables:

Training Topics include but not limited to Certification and knowledge transfer of the following topics:

- Firewalls, Intrusion Prevention, Network Access Control
- Security Incident and Event Management, Incident Handling, Forensics
- Standards, Policy, Governance, Risk, Compliance
- Penetration Testing, Validation of Security Controls, Vulnerability Management

4. Supply and Install Hardware and Software Required to Address New and Emerging Cyber Security Threats

The Consultant shall provide the following products. A digital forensic solution and accessories. Hardware and software to address data governance, compliance and classification. A system to support packet capture, deep packet analysis and security analysis.

Deliverables:

3 Forensic Laptop and Accessories • 15 inch MacBook Pro with Retina Display • 2.6GHz Quad--_core Intel Core i7, Turbo Boost up to 3.8GHz • 16GB 1600MHz DDR3L SDRAM • 1TB PCIe--_based Flash Storage • Parallels Desktop Switch to Mac Edition 9, Apple USB • SuperDrive, Mini DisplayPort to DVI Adapter, • Apple Thunderbolt to Gigabit Ethernet AdapterWindows for MacBooks, Microsoft Office Suite, Visio, Adobe Acrobat Professional, parallel vm
1 HP LaserJet Pro 400 M451dn Workgroup
4 HP 460W CS Plat PL Ht Plg Pwr Supply Kit
1 Data governance, compliance and classification system
1 Systems support packet capture and deep packet analysis, Security analysis

5. As Needed Security Products and Services

Provide Port of Los Angeles as-needed products or services. The total cost for the deliverable shall not exceed $559.

Services are provided on an as-needed basis and per each Work Authorization as directed by the client. The minimum duration for each Work Authorization is one day (8 hours) for onsite or one half-day (4 hours) for offsite (within Standard Rates), with time being billed at the hourly rate associated with the services scoped for the project.

To obtain professional services: Contact your Accuvant sales account team for scoping an individual project. Details regarding timing, scope, and effort required, will be captured in a Work Authorization and submitted to Port of Los Angeles for approval. The final amount of that Work Authorization will be deducted from the overall contract value and the delivery process will be kicked off. In the event of an explicit conflict or inconsistency between a Work Authorization Scheduling clause and this SOW, the Work Authorization will control.

Scheduling onsite services (meaning Accuvant personnel working onsite at the client premises) typically requires two weeks advance notice from the client, although resource availability may allow for much shorter (and occasionally longer) response times, especially in emergency situations for forensics or malware services.

Offsite assistance conducted either over the phone and/or online can typically be scheduled within a twenty-four hour notice subject to resource availability.

Project Assumptions

The ability to complete this engagement in an efficient and timely manner is critical to Accuvant. The assumptions listed below set forth the expectations of the working relationship between Port of Los Angeles and Accuvant.

Accuvant

- Our consultants consider all Port of Los Angeles information and documentation as sensitive and confidential and will handle appropriately
- Our consultants recognize the value of knowledge transfer and will encourage Port of Los Angeles to participate in all appropriate aspects of the project
- Our consultants and/or project managers will notify Port of Los Angeles of any items that may be delayed as soon as possible in order to determine ways to manage any impact (i.e., cost, timeframes, modifications, etc.)
- All Accuvant consultants supporting this engagement have undergone a set of background checks that include: Social Security Number Verification, Social Security Fraud Detect, Basic Employment Verification, Education Verification, 7-year All Residences Felony County Criminal Search, 7-year All Residences Misdemeanor Criminal Search, Federal Criminal Records Search, National Criminal Records Index, U.S. and Foreign Government and International Organizations Terrorist Watch and Sanctions List, Employment Credit Report and Professional Credential Verification.

- Accuvant shall have no responsibility for other contractors or third parties engaged on the project unless expressly agreed to in writing

Port of Los Angeles

- Provides a single point of contact within Port of Los Angeles's organization to help Accuvant consultants coordinate access to the required project materials and personnel
- Provides a safe working environment, including a workspace, telephone and network (and Internet) access for the purpose of time entry, email and project-related efforts
- Provides any necessary building, parking and/or machine room badges/passes to Accuvant consultants

Terms

All work will be performed subject to the terms and conditions listed in contract agreement 13-3188 between Accuvant and Port of Los Angeles.

EXHIBIT B - Compensation Rates and Fees Phase II

SOW	Description	Cost
1.1	Cyber Security Operations Center Audio/Video system build out	$159,750.00
1.2	SOC Collaboration and enhancement solution	$65,250.00
2.1	System support and maintenance extension services	$828,204.00
2.2	Security Program Alignment and Threat Intelligence	$200,250.00
2.3	Enterprise Security Assessment	$65,000.00
2.4	Cyber Security Framework implementation	$248,000.00
3	Training and Knowledge Transfer	$243,295.00
4	Supply and install hardware and software required to address new and emerging cyber security threats	$189,692.00
5	As Needed Security Products and Services	$559.00
	Total Costs	$2,000,000.00