

Region 4 Education Service Center (ESC)

Contract # R200804

for

*Cyber Security Solutions and Associated
Services*

ThunderCat Technology, LLC

Effective: October 1, 2020

The following documents comprise the executed contract between Region 4 Education Service Center and ThunderCat Technology, LLC, effective October 1, 2020:

- I. Appendix A: Vendor Contract
- II. Offer and Contract Signature Form
- III. Supplier's Response to the RFP, incorporated by reference

Tab 1: Contract and Offer And
Contract Signature Form
(Appendix A)

APPENDIX A

CONTRACT

This Contract ("Contract") is made as of August 25, 2020 by and between ThunderCat Technology, LLC ("Contractor") and Region 4 Education Service Center ("Region 4 ESC") for the purchase of Cyber Security Solutions and Associated Products & Services ("the products and services").

RECITALS

WHEREAS, Region 4 ESC issued Request for Proposals Number RFP 20-08 for Cybersecurity solutions ("RFP"), to which Contractor provided a response ("Proposal"); and

WHEREAS, Region 4 ESC selected Contractor's Proposal and wishes to engage Contractor in providing the services/materials described in the RFP and Proposal;

WHEREAS, both parties agree and understand the following pages will constitute the Contract between the Contractor and Region 4 ESC, having its principal place of business at 7145 West Tidwell Road, Houston, TX 77092.

WHEREAS, Contractor included, in writing, any required exceptions or deviations from these terms, conditions, and specifications; and it is further understood that, if agreed to by Region 4 ESC, said exceptions or deviations are incorporated into the Contract.

WHEREAS, this Contract consists of the provisions set forth below, including provisions of all attachments referenced herein. In the event of a conflict between the provisions set forth below and those contained in any attachment, the provisions set forth below shall control.

WHEREAS, the Contract will provide that any state and local governmental entities, public and private primary, secondary and higher education entities, non-profit entities, and agencies for the public benefit ("Public Agencies") may purchase products and services at prices indicated in the Contract upon the Public Agency's registration with OMNIA Partners.

- 1) Term of agreement. The term of the Contract is for a period of three (3) years unless terminated, canceled or extended as otherwise provided herein. Region 4 ESC shall have the right to renew the Contract for two (2) additional one-year periods or portions thereof. Region 4 ESC shall review the Contract prior to the renewal date and notify the Contractor of Region 4 ESC's intent renew the Contract. Contractor may elect not to renew by providing three hundred sixty-five days' (365) notice to Region 4 ESC. Notwithstanding the expiration of the initial term or any subsequent term or all renewal options, Region 4 ESC and Contractor may mutually agree to extend the term of this Agreement. Contractor acknowledges and understands Region 4 ESC is under no obligation whatsoever to extend the term of this Agreement.
- 2) Scope: Contractor shall perform all duties, responsibilities and obligations, set forth in this agreement, and described in the RFP, incorporated herein by reference as though fully set forth herein.
- 3) Form of Contract. The form of Contract shall be the RFP, the Offeror's proposal and Best and Final Offer(s).

- 4) Order of Precedence. In the event of a conflict in the provisions of the Contract as accepted by Region 4 ESC, the following order of precedence shall prevail:
 - i. This Contract
 - ii. Offeror's Best and Final Offer
 - iii. Offeror's proposal
 - iv. RFP and any addenda
- 5) Commencement of Work. The Contractor is cautioned not to commence any billable work or provide any material or service under this Contract until Contractor receives a purchase order for such work or is otherwise directed to do so in writing by Region 4 ESC.
- 6) Entire Agreement (Parol evidence). The Contract, as specified above, represents the final written expression of agreement. All agreements are contained herein and no other agreements or representations that materially alter it are acceptable.
- 7) Assignment of Contract. No assignment of Contract may be made without the prior written approval of Region 4 ESC. Contractor is required to notify Region 4 ESC when any material change in operations is made (i.e. bankruptcy, change of ownership, merger, etc.).
- 8) Novation. If Contractor sells or transfers all assets or the entire portion of the assets used to perform this Contract, a successor in interest must guarantee to perform all obligations under this Contract. Region 4 ESC reserves the right to accept or reject any new party. A change of name agreement will not change the contractual obligations of Contractor.
- 9) Contract Alterations. No alterations to the terms of this Contract shall be valid or binding unless authorized and signed by Region 4 ESC.
- 10) Adding Authorized Distributors/Dealers. Contractor is prohibited from authorizing additional distributors or dealers, other than those identified at the time of submitting their proposal, to sell under the Contract without notification and prior written approval from Region 4 ESC. Contractor must notify Region 4 ESC each time it wishes to add an authorized distributor or dealer. Purchase orders and payment can only be made to the Contractor unless otherwise approved by Region 4 ESC. Pricing provided to members by added distributors or dealers must also be less than or equal to the Contractor's pricing.
- 11) TERMINATION OF CONTRACT
 - a) Cancellation for Non-Performance or Contractor Deficiency. Region 4 ESC may terminate the Contract if purchase volume is determined to be low volume in any 12-month period. Region 4 ESC reserves the right to cancel the whole or any part of this Contract due to failure by Contractor to carry out any obligation, term or condition of the contract. Region 4 ESC may issue a written deficiency notice to Contractor for acting or failing to act in any of the following:
 - i. Providing material that does not meet the specifications of the Contract;
 - ii. Providing work or material was not awarded under the Contract;
 - iii. Failing to adequately perform the services set forth in the scope of work and specifications;
 - iv. Failing to complete required work or furnish required materials within a reasonable amount of time;

- v. Failing to make progress in performance of the Contract or giving Region 4 ESC reason to believe Contractor will not or cannot perform the requirements of the Contract; or
- vi. Performing work or providing services under the Contract prior to receiving an authorized purchase order.

Upon receipt of a written deficiency notice, Contractor shall have ten (10) days to provide a satisfactory response to Region 4 ESC. Failure to adequately address all issues of concern may result in Contract cancellation. Upon cancellation under this paragraph, all goods, materials, work, documents, data and reports prepared by Contractor under the Contract shall immediately become the property of Region 4 ESC.

- b) Termination for Cause. If, for any reason, Contractor fails to fulfill its obligation in a timely manner, or Contractor violates any of the covenants, agreements, or stipulations of this Contract Region 4 ESC reserves the right to terminate the Contract immediately and pursue all other applicable remedies afforded by law. Such termination shall be effective by delivery of notice, to the Contractor, specifying the effective date of termination. In such event, all documents, data, studies, surveys, drawings, maps, models and reports prepared by Contractor will become the property of the Region 4 ESC. If such event does occur, Contractor will be entitled to receive just and equitable compensation for the satisfactory work completed on such documents.
- c) Delivery/Service Failures. Failure to deliver goods or services within the time specified, or within a reasonable time period as interpreted by the purchasing agent or failure to make replacements or corrections of rejected articles/services when so requested shall constitute grounds for the Contract to be terminated. In the event Region 4 ESC must purchase in an open market, Contractor agrees to reimburse Region 4 ESC, within a reasonable time period, for all expenses incurred.
- d) Force Majeure. If by reason of Force Majeure, either party hereto shall be rendered wholly or in part to carry out its obligations under this Agreement then such party shall give notice and full particulars of Force Majeure in writing to the other party within a reasonable time after occurrence of the event or cause relied upon, and the obligation of the party giving such notice, so far as it is affected by such Force Majeure, shall be suspended during the continuance of the inability then claimed, except as hereinafter provided, but for no longer period, and such party shall endeavor to remove or overcome such inability with all reasonable dispatch.

The term Force Majeure as employed herein, shall mean acts of God, strikes, lockouts, or other industrial disturbances, act of public enemy, orders of any kind of government of the United States or the State of Texas or any civil or military authority; insurrections; riots; epidemics; landslides; lighting; earthquake; fires; hurricanes; storms; floods; washouts; droughts; arrests; restraint of government and people; civil disturbances; explosions, breakage or accidents to machinery, pipelines or canals, or other causes not reasonably within the control of the party claiming such inability. It is understood and agreed that the settlement of strikes and lockouts shall be entirely within the discretion of the party having the difficulty, and that the above requirement that any Force Majeure shall be remedied with all reasonable dispatch shall not require the settlement of strikes and lockouts by acceding to the demands of the opposing party or parties when such settlement is unfavorable in the judgment of the party having the difficulty.

- e) Standard Cancellation. Region 4 ESC may cancel this Contract in whole or in part by providing written notice. The cancellation will take effect 30 business days after the other party receives the notice of cancellation. After the 30th business day all work will cease following completion of final purchase order.

- 12) Licenses. Contractor shall maintain in current status all federal, state and local licenses, bonds and permits required for the operation of the business conducted by Contractor. Contractor

shall remain fully informed of and in compliance with all ordinances and regulations pertaining to the lawful provision of services under the Contract. Region 4 ESC reserves the right to stop work and/or cancel the Contract if Contractor's license(s) expire, lapse, are suspended or terminated.

- 13) Survival Clause. All applicable software license agreements, warranties or service agreements that are entered into between Contractor and Region 4 ESC under the terms and conditions of the Contract shall survive the expiration or termination of the Contract. All Purchase Orders issued and accepted by Contractor shall survive expiration or termination of the Contract.
- 14) Delivery. Conforming product shall be shipped within 7 days of receipt of Purchase Order. If delivery is not or cannot be made within this time period, the Contractor must receive authorization for the delayed delivery. The order may be canceled if the estimated shipping time is not acceptable. All deliveries shall be freight prepaid, F.O.B. Destination and shall be included in all pricing offered unless otherwise clearly stated in writing.
- 15) Inspection & Acceptance. If defective or incorrect material is delivered, Region 4 ESC may make the determination to return the material to the Contractor at no cost to Region 4 ESC. The Contractor agrees to pay all shipping costs for the return shipment. Contractor shall be responsible for arranging the return of the defective or incorrect material.
- 16) Payments. Payment shall be made after satisfactory performance, in accordance with all provisions thereof, and upon receipt of a properly completed invoice.
- 17) Price Adjustments. Should it become necessary or proper during the term of this Contract to make any change in design or any alterations that will increase price, Region 4 ESC must be notified immediately. Price increases must be approved by Region 4 ESC and no payment for additional materials or services, beyond the amount stipulated in the Contract shall be paid without prior approval. All price increases must be supported by manufacturer documentation, or a formal cost justification letter. Contractor must honor previous prices for thirty (30) days after approval and written notification from Region 4 ESC. It is the Contractor's responsibility to keep all pricing up to date and on file with Region 4 ESC. All price changes must be provided to Region 4 ESC, using the same format as was provided and accepted in the Contractor's proposal.

Price reductions may be offered at any time during Contract. Special, time-limited reductions are permissible under the following conditions: 1) reduction is available to all users equally; 2) reduction is for a specific period, normally not less than thirty (30) days; and 3) original price is not exceeded after the time-limit. Contractor shall offer Region 4 ESC any published price reduction during the Contract term.

- 18) Audit Rights. Contractor shall, at its sole expense, maintain appropriate due diligence of all purchases made by Region 4 ESC and any entity that utilizes this Contract. Region 4 ESC reserves the right to audit the accounting for a period of three (3) years from the time such purchases are made. This audit right shall survive termination of this Agreement for a period of one (1) year from the effective date of termination. Region 4 ESC shall have the authority to conduct random audits of Contractor's pricing at Region 4 ESC's sole cost and expense. Notwithstanding the foregoing, in the event that Region 4 ESC is made aware of any pricing being offered that is materially inconsistent with the pricing under this agreement, Region 4 ESC shall have the ability to conduct an extensive audit of Contractor's pricing at Contractor's

sole cost and expense. Region 4 ESC may conduct the audit internally or may engage a third-party auditing firm. In the event of an audit, the requested materials shall be provided in the format and at the location designated by Region 4 ESC.

- 19) Discontinued Products. If a product or model is discontinued by the manufacturer, Contractor may substitute a new product or model if the replacement product meets or exceeds the specifications and performance of the discontinued model and if the discount is the same or greater than the discontinued model.
- 20) New Products/Services. New products and/or services that meet the scope of work may be added to the Contract. Pricing shall be equivalent to the percentage discount for other products. Contractor may replace or add product lines if the line is replacing or supplementing products, is equal or superior to the original products, is discounted similarly or greater than the original discount, and if the products meet the requirements of the Contract. No products and/or services may be added to avoid competitive procurement requirements. Region 4 ESC may require additions to be submitted with documentation from Members demonstrating an interest in, or a potential requirement for, the new product or service. Region 4 ESC may reject any additions without cause.
- 21) Options. Optional equipment for products under Contract may be added to the Contract at the time they become available under the following conditions: 1) the option is priced at a discount similar to other options; 2) the option is an enhancement to the unit that improves performance or reliability.
- 22) Warranty Conditions. All supplies, equipment and services shall include manufacturer's minimum standard warranty and one (1) year labor warranty unless otherwise agreed to in writing.
- 23) Site Cleanup. Contractor shall clean up and remove all debris and rubbish resulting from their work as required or directed. Upon completion of the work, the premises shall be left in good repair and an orderly, neat, clean, safe and unobstructed condition.
- 24) Site Preparation. Contractor shall not begin a project for which the site has not been prepared, unless Contractor does the preparation work at no cost, or until Region 4 ESC includes the cost of site preparation in a purchase order. Site preparation includes, but is not limited to: moving furniture, installing wiring for networks or power, and similar pre-installation requirements.
- 25) Registered Sex Offender Restrictions. For work to be performed at schools, Contractor agrees no employee or employee of a subcontractor who has been adjudicated to be a registered sex offender will perform work at any time when students are or are reasonably expected to be present. Contractor agrees a violation of this condition shall be considered a material breach and may result in the cancellation of the purchase order at Region 4 ESC's discretion. Contractor must identify any additional costs associated with compliance of this term. If no costs are specified, compliance with this term will be provided at no additional charge.
- 26) Safety measures. Contractor shall take all reasonable precautions for the safety of employees on the worksite and shall erect and properly maintain all necessary safeguards for protection of workers and the public. Contractor shall post warning signs against all hazards created by its operation and work in progress. Proper precautions shall be taken pursuant to state law

and standard practices to protect workers, general public and existing structures from injury or damage.

- 27) Smoking. Persons working under the Contract shall adhere to local smoking policies. Smoking will only be permitted in posted areas or off premises.
- 28) Stored materials. Upon prior written agreement between the Contractor and Region 4 ESC, payment may be made for materials not incorporated in the work but delivered and suitably stored at the site or some other location, for installation at a later date. An inventory of the stored materials must be provided to Region 4 ESC prior to payment. Such materials must be stored and protected in a secure location and be insured for their full value by the Contractor against loss and damage. Contractor agrees to provide proof of coverage and additionally insured upon request. Additionally, if stored offsite, the materials must also be clearly identified as property of Region 4 ESC and be separated from other materials. Region 4 ESC must be allowed reasonable opportunity to inspect and take inventory of stored materials, on or offsite, as necessary. Until final acceptance by Region 4 ESC, it shall be the Contractor's responsibility to protect all materials and equipment. Contractor warrants and guarantees that title for all work, materials and equipment shall pass to Region 4 ESC upon final acceptance.
- 29) Funding Out Clause. A Contract for the acquisition, including lease, of real or personal property is a commitment of Region 4 ESC's current revenue only. Region 4 ESC retains the right to terminate the Contract at the expiration of each budget period during the term of the Contract and is conditioned on a best effort attempt by Region 4 ESC to obtain appropriate funds for payment of the contract.
- 30) Indemnity. Contractor shall protect, indemnify, and hold harmless both Region 4 ESC and its administrators, employees and agents against all claims, damages, losses and expenses arising out of or resulting from the actions of the Contractor, Contractor employees or subcontractors in the preparation of the solicitation and the later execution of the Contract. Any litigation involving either Region 4 ESC, its administrators and employees and agents will be in Harris County, Texas.
- 31) Marketing. Contractor agrees to allow Region 4 ESC to use their name and logo within website, marketing materials and advertisement. Any use of Region 4 ESC name and logo or any form of publicity, inclusive of press releases, regarding this Contract by Contractor must have prior approval from Region 4 ESC.
- 32) Certificates of Insurance. Certificates of insurance shall be delivered to the Region 4 ESC prior to commencement of work. The Contractor shall give Region 4 ESC a minimum of ten (10) days' notice prior to any modifications or cancellation of policies. The Contractor shall require all subcontractors performing any work to maintain coverage as specified.
- 33) Legal Obligations. It is Contractor's responsibility to be aware of and comply with all local, state, and federal laws governing the sale of products/services and shall comply with all laws while fulfilling the Contract. Applicable laws and regulation must be followed even if not specifically identified herein.

OFFER AND CONTRACT SIGNATURE FORM

The undersigned hereby offers and, if awarded, agrees to furnish goods and/or services in strict compliance with the terms, specifications and conditions at the prices proposed within response unless noted in writing.

Company Name ThunderCat Technology, LLC

Address 1925 Isaac Newton Square, Suite 180

City/State/Zip Reston, VA 20190

Telephone No. 703-674-0216

Email Address contracts@thundercatttech.com

Printed Name Jean Kim

Title Contracts

Authorized signature 

Accepted by Region 4 ESC:

Contract No. R200804

Initial Contract Term October 1, 2020 to September 30, 2023


Region 4 ESC Authorized Board Member

8/25/2020
Date

Margaret S. Bass
Print Name


Region 4 ESC Authorized Board Member

8/25/2020
Date

Linda Tinnerman
Print Name

Tab 1a: Terms and Conditions Acceptance Form
(Appendix B)

Tab 2: Products/Pricing

Omnia Cyber Contract OEMs

OEM	Partner Link
Analyst Platform	https://analystplatform.com/
AttackIQ	https://attackiq.com/
Bricata	https://bricata.com/
Carbon Black	https://www.carbonblack.com/
Centrify	https://www.centrify.com/
CheckMarx	https://www.checkmarx.com/
Cisco	https://www.cisco.com/
CiscoDuo	https://duo.com/partners/technology-partners/select-partners/cisco
Cofense	https://cofense.com/
Cohesity	https://www.cohesity.com/
Contrast	https://www.contrastsecurity.com/
CoreLight	https://www.corelight.com/
CrowdStrike	https://www.crowdstrike.com/
CyberArk	https://www.cyberark.com/
Dark Owl	https://www.darkowl.com/
Demisto	https://www.demisto.com/
Digital Shadows	https://www.digitalsadows.com/
Elastic	https://www.elastic.co/
Exabeam	https://www.exabeam.com/
Exiger	https://www.exiger.com/
ExtraHop	https://www.extrahop.com/
F5	https://www.f5.com/
Fidelis	https://www.fidelissecurity.com/
FireEye	https://www.fireeye.com/
Flashpoint	https://www.flashpoint-intel.com/
Forescout	https://www.forescout.com/
Fortify	https://www.microfocus.com/en-us/solutions/application-security
Google	https://cloud.google.com/solutions/security
Interos	https://www.interos.ai/
Juniper	https://www.juniper.net/us/en/
KnowBe4	https://www.knowbe4.com/
Lookout	https://www.lookout.com/
McAfee	https://www.mcafee.com/en-us/index.html
Micro Focus	https://www.microfocus.com/en-us/home
OPSWAT	https://www.opswat.com/
Palo Alto	https://www.paloaltonetworks.com/
Phantom	https://www.splunk.com/en_us/software/splunk-security-orchestration-and-automation.html
Proofpoint	https://www.proofpoint.com/us
PulseSecure	https://www.pulsesecure.net/
RedHat	https://www.redhat.com/en
RedSeal	https://www.redseal.net/
RSA	https://www.rsa.com/
Sayari	https://sayari.com/
SecureAuth	https://www.secureauth.com/
ServiceNow	https://www.servicenow.com/
solarwinds	https://www.solarwinds.com/
Splunk	https://www.splunk.com/
Swimlane	https://swimlane.com/
Symantec	https://securitycloud.symantec.com/cc/#/landing
Tanium	https://www.tanium.com/
Tenable	https://www.tenable.com/
Thycotic	https://thycotic.com/
Titus	https://titus.com/
Veeam	https://www.veeam.com/
Veritas	https://www.veritas.com/
Zerto	https://www.zerto.com/

Managed Security Service Providers	Partner Link
SecureWorks	https://www.secureworks.com/
Arctic Wolf	https://arcticwolf.com/
Red Canary	https://redcanary.com/
Symantec	https://securitycloud.symantec.com/cc/#/landing

Analyst Platform:

Illuminate is commercially available software that solves fundamental issues within defensive cyber operations. The Illuminate software automates tedious, time-consuming, repetitive activities, improves situational awareness, and makes cyber analysts more efficient and more effective. Illuminate increases your understanding of cyber threats and enable you to create effective rules to strengthen the defensive posture of your networks without having to replace your existing cybersecurity investments.

Illuminate provides significant cost savings through efficiency gains. Within a few clicks of the mouse anyone can quickly identify actionable intelligence, understand what happened, who the targets are, who the threat actors are, what malware is used, what vulnerabilities are exploited, prescribe mitigation actions, validate actions occurred, and share critical information with mission partners. Illuminate provides analysts with customizable dashboards that provide insights into trends and changes in adversarial activity over time. Modernizing information sharing, Illuminate implements machine-to-machine interactions and supports STIX and TAXII data exchange standards. Additionally, Illuminate automatically converts any ingested report regardless if it is structured or unstructured to STIX which can then be exported.

The proposed solution is to deploy Analyst Platform's Illuminate software as a commercially available and supported solution that exceeds the VA's technical and operational requirements. Illuminate will enable VA to maintain awareness of Indicators of Threat (IoT)/ Indicators of Compromise (IoC), and identify if the IoT/IoC is a new or known threat; detect IoT/IoCs; correlate ingested data, conduct analysis, and provide understanding of threat activity and impacts to the target/victim; and to enable effective mitigation and host cleanup, ensuring maximum information sharing and analysis assistance.

The core technology of the solution, Illuminate, is designed and built to support the understanding of evolving patterns in nation-state actors and trends in targeting. It can respond to knowledge of the latest malware, and work indicator by indicator in defensive or other tasks and assist the workflow needed by cyber analysts to see data in a single pane of glass. Its unique position and functional set make it ideal for large scale usage because it integrates with, not overtakes, existing systems and finds higher value for customers in sharing data bi-directionally with existing on-network tools. Illuminate correlates the threat actors and malware families to indicators, and "pushes" the indicators and associated threat information into commercial SIEMs, commercial data platforms, and custom-built analysis clusters to enrich the events with contextual threat information.

AttackIQ:

In cybersecurity, AttackIQ was created to watch our watchers. It's a penetration testing tool, but one that is configured to operate from the inside, with the primary goal of identifying flaws, misconfigurations and outright shortcomings in all other cybersecurity defenses. It can be used to pit various defenses against one another to see which works best for an environment, to discover areas where existing defenses unnecessarily overlap, or to identify bad configurations that are preventing security tools from properly operating. The main AttackIQ management console either sits in the cloud or can be installed locally on premises if an organization wishes. In addition to the main console, which is used to configure and deploy tests against protected assets as well as collecting those results, users will need to deploy agents. There are agents available for all forms of Windows and Mac OS systems, plus most flavors of Linux. Deploying those agents involves a fairly simple wizard-supported process to ensure that the right agents get to the correct assets. There are actually two types of agents: static and dynamic. The static agents install onto an asset and remain there forever. They are perfect for critical assets that always need to be protected. The dynamic agents can be installed on systems for specific tests and then can be removed or moved to other systems. One such use would be to periodically test non-critical assets, such as antivirus protections on endpoints. Most deployments end up being about 80 percent static agents and 20 percent dynamic, according to AttackIQ officials. Pricing for AttackIQ is tiered subscription model based on the number of agents used. Once the agents are in place, users can choose from an existing library of 1,260 attack scenarios, all of which are highly configurable based on the unique environment where they are deployed. AttackIQ is constantly expanding its scenario library. Each scenario can be modified using a very easy-to-use wizard that ensures proper deployment, or if users feel comfortable doing so, the Python code they are written in can be edited directly. Users can additionally use the wizards to create their own scenarios with the existing toolset. And because AttackIQ is designed to run in working production environments, all attacks associated with a test have been defanged so they won't cause any damage. AttackIQ can also be configured to interface with any network security information and event management system (SIEM). This can be helpful if defenses are set to report potentially suspicious behavior to a SIEM instead of taking any direct action. In that case, AttackIQ launches the scenario and then queries the SIEM to see if its specific attack behavior was reported at that time. Thereafter, the report from AttackIQ is identical to others. It shows whether an asset passed the test and why, and also what is to blame for any failures. Not only will AttackIQ identify weak spots or flaws in existing defenses, but it will also find areas where misconfigurations or installation mistakes are preventing good cybersecurity tools from operating properly. In this era of incredibly complex networking where everything is a unique environment, AttackIQ can help ensure that the best defenses are in place and that they are operating at maximum efficiency.

Breeden, John. (2019). Review: AttackIQ watches the watchers. CSO: From IDG [online], 8 January 2019.

https://d307wsvyo0odb1.cloudfront.net/media/filer_public/5c/3a/5c3a0f28-0924-4503-82d4-ab930a8cfeec/attackia_cso_product_review_01_08_19.pdf?v=0312d7b6c70b53fb1504aee3695177d7423579e
(Accessed 7 April 2020)

Bricata:

Bricata is the leader in comprehensive network protection. The Bricata solution provides unparalleled network visibility, full-spectrum threat detection, threat hunting and post-detection response capabilities in an intuitive, tightly integrated and self-managing system. Its automated detection, productive GUIs, and expert system workflows make it easy-to-use for novices, while granular control of its engines, access to rich network metadata and PCAPs, and true threat hunting capabilities give experts the power and control they demand. Bricata has been proven to speed incident resolution by up to eight times by reliably detecting threats and providing the context necessary to get to the truth quickly and act.

Cyber threats are complex and ever-evolving and require a range of detection and protection technologies to fully protect your network. Bricata seamlessly integrates a full range of advanced threat protection technologies onto a single platform to improve ease-of-use, increase productivity, reduce time to containment, and minimize operating costs. If you can't see it, you can't protect it. Bricata's comprehensive threat protection provides organizations with deep insight into network devices, applications, users, operating systems, files, and more, for full contextual awareness in real-time. Bricata can make incident response over 800% faster, providing the context necessary to get to the truth quickly and act. Our solution provides the performance and flexibility organizations require to adapt and respond to ever-changing threats and adversary behaviors. Our commitment to open data exchange offers easy integration and configuration with other security systems while substantially reducing total cost of ownership. Bricata lets you see everything that transpires on your network via high-fidelity metadata and SmartPCAP.

"In the last 12 months, the company has released a [new version of its platform](#), added key [new executives](#) to its leadership team, strengthened partnerships, and earned industry analyst recognition for its innovation in [network traffic analysis](#) and [intrusion detection and prevention systems](#). I look forward to continuing to work with the Bricata team as they further develop the state-of-the-art in network protection." John Becker - Executive Board Chair

Carbon Black:

Carbon Black has been a leader in endpoint security for years. We've created whole new categories and continue to pioneer others. Carbon Black offers more than an endpoint security and operations platform; it supports a robust community made up of customers, partners, and industry experts that engage daily to collaborate and combat today's threat landscape. Their collective knowledge is shared through active forum discussions, product tips and training, and curated watchlists and threat intel.

Over the years Carbon Black has become one of the endpoint partners of choice when it comes to integrating and sharing data with SOC automation, incident management, and IT operations solutions. Our vast community of developers shares and actively collaborates on their work, reducing the cost of any organization desiring a more automated, interconnected security stack.

The Carbon Black Threat Analysis Unit (TAU) is focused on the next wave of attacks. Their job is to keep you safe by understanding how to detect and prevent attacks that bypass traditional, file-centric, prevention strategies. They are focused on techniques that were once the domain of advanced hackers, and are now moving downstream into the commodity attack market.

More than 5,600 global customers, including approximately one-third of the Fortune 100, trust Carbon Black to keep their organizations safe. Our diverse customer base includes Silicon Valley leaders in internet search, social media, transportation, and hospitality, as well as leaders across finance, manufacturing, retail, and government. With an eye on empowering every security team and protecting every endpoint, we stand true to our founding vision: To create a world safe from cyberattacks.

Centrify:

For more than a decade, Centrify has been leading the way in redefining the Fabric of Privileged Access Management. As traditional network perimeters dissolve, organizations must discard the old model of “trust but verify” which relied on well-defined boundaries. Zero Trust mandates a “never trust, always verify, enforce least privilege” approach to privileged access, from inside or outside the network.

Organizations may consider approaching Privileged Access Management (PAM) by solely implementing password vaults, leaving gaps that can easily be exploited. Centrify Zero Trust Privilege combines password vaulting with brokering of identities, multi-factor authentication enforcement and “just enough” privilege, all while securing remote access and monitoring of all privileged sessions.

Centrify is redefining the legacy approach to Privileged Access Management (PAM) by delivering cloud-ready [Zero Trust Privilege](#) to secure access to infrastructure, DevOps, cloud, containers, Big Data and other modern enterprise [use cases](#).

[Centrify Zero Trust Privilege](#) helps customers grant least privilege access based on verifying who is requesting access, the context of the request, and the risk of the access environment. By implementing least privilege access, Centrify minimizes the attack surface, improves audit and compliance visibility, and reduces risk, complexity and costs for the modern, hybrid enterprise.

[Over half of the Fortune 100](#), the world’s largest financial institutions, intelligence agencies, and critical infrastructure companies, all trust Centrify to stop the leading cause of breaches — privileged credential abuse.

Checkmarx:

The Checkmarx Software Security Platform provides a centralized foundation for operating your suite of software security solutions for Static Application Security Testing (SAST), Interactive Application Security Testing (IAST), Software Composition Analysis (SCA), and application security training and skills development. Built to address every organization's needs, the Checkmarx Software Security Platform provides the full scope of options: including private cloud and on-premises solutions. Allowing a range of implementation options ensures customers can start securing their code immediately, rather than going through long processes of adapting their infrastructure to a single implementation method. The Checkmarx Software Security Platform transforms the standard for secure application development, providing one powerful resource with industry-leading capabilities, including:

[Checkmarx Static Application Security Testing \(CxSAST\)](#)

CxSAST is an enterprise-grade, flexible, and accurate static analysis solution capable of identifying hundreds of security vulnerabilities and weaknesses in custom code; supporting over 22 coding and scripting languages and frameworks, with zero configuration necessary to scan any language.

[Checkmarx Open Source Analysis \(CxOSA\)](#)

CxOSA is a powerful software composition analysis solution focused on enabling development and security teams to mitigate security risks present in open source software and third-party libraries within their codebase. Users can identify and prioritize open source vulnerabilities, generate an inventory of open source components and dependencies in use, and evaluate the risk of open source license non-compliance.

[Checkmarx Interactive Application Security Testing \(CxIAST\)](#)

CxIAST fills the critical software security gap by leveraging existing functional testing activities to automate the detection of vulnerabilities on running applications. CxIAST is the industry's first IAST solution that fully integrates with a Static Application Security Testing solution and offers query language, allowing for greater vulnerability coverage and higher accuracy.

[Checkmarx AppSec Awareness Solution \(CxCodeBashing\)](#)

Checkmarx Codebashing cultivates a culture of software security that empowers developers to take security into their own hands and be comfortable doing so. Leverage just-in-time training to educate developers on specific challenges they are facing, without diverting them from accomplishing their main task – writing secure code quickly

Cisco:

Security is a grind. You are working to build the future and battling to keep it secure. The demands are significant. You need a workforce protected anywhere, on any device--a digitized workplace where every part of your infrastructure is safe, and workloads are secured wherever they are running, 24/7. Meanwhile, cyber threats are constantly evolving, getting smarter and more sophisticated. What's the answer? Cisco is reimagining what's possible with Cisco SecureX, a cybersecurity platform that simplifies your security. As a leading security provider, protecting 100 percent of the Fortune 100, no one is better equipped. We can help you cover your entire infrastructure with best-of-breed products on an integrated, open platform. With unrivaled threat intelligence and an industry-leading zero trust approach, Cisco helps you attain effective security to face tomorrow's evolving threats.

Cisco's range of security products includes:

- Advanced Malware Protection
- Cloud Security
- Email Security
- Endpoint Security
- Multi-Factor Authentication
- Next-Generation Firewalls
- Network Visibility and Segmentation
- Next-Generation Intrusion Prevention Systems
- Security Management
- Threat Reponse
- VPM Security Clients
- Web Security

Cisco Duo:

Duo and Cisco collaborate on range of use cases to bring strong user and device verification and mutual exchange of security context. The Duo-Cisco joint solution enables customers to deploy zero-trust security measures both inside and outside the corporate network.

Duo's integration with Cisco ASA VPN provides strong user authentication and device security hygiene check and visibility. This integrated solution provides security admins the ability to enforce consistent user and device based access policy for VPN access and thereby reduce risk for data breaches and meet compliance requirements.

Cisco Umbrella (previously OpenDNS) is a cloud security platform that provides the security at DNS layer. Umbrella identifies malicious domains, IPs, detects anomalies and predicts emerging threats. It often provides first line of defence against the threats originating from internet and therefore protecting logins into Umbrella is critical to maintain integrity of security infrastructure. Duo is integrated with Umbrella to provide strong user authentication, device security hygiene check and visibility thereby ensuring access to Umbrella is not compromised.

Duo's integration with Cisco WebEx offers a variety of methods for adding two-factor authentication and flexible security policies to WebEx SSO logins. Duo layers strong authentication and a flexible policy engine on top of WebEx logins using the Security Assertion Markup Language (SAML) 2.0 authentication standard. Duo authenticates your users using existing on-premises or cloud-based directory credentials and prompts for two-factor authentication before permitting access to WebEx.

The background of this partnership is Duo's support to Cisco itself:

Rolling out a new technology to 120,000 users globally can often take organizations multiple years. The Cisco IT team was determined to complete its Duo rollout in a much shorter period of time. The small project team consisted of two people, and they knew they had to be efficient and strategic in their approach.

The team took key steps to implement a robust program with Duo:

To not pull attention too far to one area, the team had two active workstreams: technical implementation and change management for users.

They focused on communicating the importance of MFA and why they were rolling out Duo. Cisco also used it as an opportunity to reinforce the importance of security in people's personal lives and integrating MFA where possible into banking and other online accounts.

Duo replaced an existing MFA solution and the team was concerned users might get frustrated with the change and be slow to enroll. The team integrated it into the company's Office 365 rollout to present a compelling user experience.

Pairing Duo with an easier way to access key work resources from any location positioned security as a user experience improvement and not a barrier.

The team enabled robust self-service resources for enrollment and support - making the process painless for users.

Evaluating device health to ensure every device attempting to access an application is secure and up-to-date. Attributes can include screenlocks, operating system version, encryption status, whether it is corporate-owned or not, and more.

Fully enabling secure BYOD by putting applicationspecific access controls and policies in place to grant access based on device health, type of device, location and sensitivity of the application.

With Duo's help, the Cisco team implemented a rather large change in a short period of time. And because Duo was easy for end users to adopt, it created minimal burden on IT staff. Cisco achieved its goal of securing a diverse workforce and environment in a way that improved employee flexibility and productivity.

Enabled zero trust for the international workforce:

Every user, device and access attempt is continuously validated.

Employees and contractors worldwide have secure access to applications.

Employees have the flexibility to securely work from anywhere at any time to meet customer needs.

Implemented a security solution that was easy to administer and use:

An implementation team of two rolled out Duo to 120,000 users in less than six months.

70% of users enrolled with Duo within 48 hours of receiving an invitation.

Only 1% of users opened helpdesk tickets and needed support.

The implementation team received positive user feedback - users embrace Duo and appreciate the ease of use and security it provides.

As the largest security vendor on the planet, Cisco became a proving ground for their products:

Demonstrated how Duo can be rolled out at enterprise scale easily and quickly.

Ensure that the over 400,000 access devices being used are healthy and up to date.

Duo policies secure 5 million access attempts each month.

Create a zero-trust framework that goes beyond MFA:

Cisco protects 3,000 applications with Duo - ensuring the right users and devices can securely access the right applications.

Duo notifies users if a device is at-risk and allows self-remediation.

Visibility into who and what is on the network gives the security team the speed and agility to respond quickly to threats.

Duo's forward-looking features enable cutting-edge approaches to ever-evolving security challenges.

Cofense:

To stop rapidly evolving phishing attacks, you need more than a layered defense. You need the right layers. Our bundled solutions equip your teams to find, report, respond to, and neutralize phishing threats by fusing human intelligence and advanced technology. When users act as human sensors, they supply valuable intelligence to security operations teams, giving them the visibility to neutralize threats faster. According to Mandiant, average attacker dwell time (the time between compromise and detection) is 78 days. Cofense enables you to identify and mitigate active phishing attacks in less than 20 minutes.

Cofense tailors bundling configurations that take into account:

- Awareness - Condition users to recognize phishing
- Detection - Enable SOC analysts to find 'bad' faster
- Defense - Understand and neutralize real threats.

Cohesity:

Cohesity eliminates mass data fragmentation by providing a single web-scale data management platform to manage the vast majority of an organization's data—backups, file shares, object stores, and data used for dev/test and analytics. Cohesity tailors their products around three principles. The first is simplicity. They do this by controlling data management workloads through a single UI with simple policies. The second principle is speed. They meet business SLAs with machine driven operational intelligence. Third is flexibility. They respond to evolving business needs from core to edge to cloud.

With this in mind, Cohesity offers a portfolio of products:

Data Protect: DataProtect delivers comprehensive data protection with policy-based management for all workloads, anywhere—virtual and physical, databases, NAS, cloud environments, and business-critical applications.

Data Platform: Designed with Google-like principles, DataPlatform is a web-scale solution that solves mass data fragmentation by consolidating workloads on a single software-defined platform.

DataPlatform Cloud Edition: Extend data mobility across your data center and public clouds. DataPlatform Cloud Edition allows you to span a hybrid cloud environment to support your evolving data requirements.

Data Platform Virtual Edition: Bring the benefits of core data center protection and productivity workflows—including backup, recovery, archiving, dev/test, and analytics—to remote and branch office locations.

Helios: Monitor and manage your global environment in real time with this intelligent dashboard. Utilizing cutting edge algorithms, Helios proactively assesses IT needs and automates data management resources.

Analytics Workbench: A data analytics solution available within DataPlatform, Analytics Workbench allows businesses to analyze and extract detailed information directly without migrating data to an application server.

Contrast:

Most companies build or buy software applications to run their business. Unfortunately, application code exposes critical vulnerabilities to hackers. Contrast solves this complex problem with a bold new secure technology platform that transforms application security by making software self-protecting. Intelligent Contrast agents are injected into the code, instrumenting applications with thousands of smart, agile sensors that detect and correct vulnerabilities before deployment, and protect the software applications in operation. No legacy security tool can protect every application. But a tenacious army of intelligent Contrast sensors can. The Contrast technology platform is a fundamentally new way to protect a company from threats, giving our customers visibility and accuracy that verges on clairvoyance. Because Contrast technology works hand-in-glove with agile and DevOps teams, it transforms every software application in a company's portfolio from a weak spot into a strong point to decisively repel attacks. Because Contrast technology runs at the speed of business, it transforms everyone responsible for software into defenders of the company, protectors of company data, and guardians of customers' personal information. Because we focus on the security of their apps, Contrast is an indispensable partner so our customers can focus on running their business.

Their portfolio of products are:

Contrast Assess: Contrast Assess is a revolutionary application security testing solution that infuses software with vulnerability assessment capabilities so that security flaws are automatically identified.

Contrast OSS: Contrast OSS delivers automated open source risk management by embedding security and compliance checks in applications throughout the development process while performing continuous monitoring in production. Contrast is the only solution that can identify vulnerable components, determine if they are actually used by the application and prevent exploitation at runtime.

Contrast Protect: By being within the application itself, Contrast gives visibility into the application like never before and provides actionable and timely application layer threat intelligence across the entire application.

Contrast Security Agents: Java, .NET, NODE.JS, Ruby, Python

Contrast CE: Contrast CE is a free and full-strength application security platform that provides "always on" IAST, RASP, and SCA for Java applications, .NET Core (and .NET Framework coming soon), and APIs. Contrast isn't a scanner or firewall, instead it works from inside the running application -- like an AppDynamics or NewRelic for security. This approach is easier, faster, and more accurate than legacy AppSec tools.

Corelight:

Corelight helps defend some of the most risk-averse government agencies globally, safeguarding high-value assets with a master record of network events. A foundational, data-driven security tool for leading SOCs, Corelight transforms raw traffic into rich logs with [Zeek](#) / [Bro](#). Combined with custom insights and extracted files, Corelight accelerates hunting and response and magnifies signal in your security analytics. Their three sets of products are Sensor Appliances, Cloud Sensor and Virtual Sensor:

Sensor Appliances:

Corelight AP 3000 Sensor

- 25 Gbps+ monitored traffic*
- 1U rack mounted appliance
- 15 minute out-of-band deployment

Corelight AP 1001 Sensor

- Up to 10 Gbps monitored traffic
- 1U rack mounted appliance
- 15 minute out-of-band deployment

Corelight AP 200 Sensor

- Up to 2 Gbps monitored traffic
- 1U half-depth rack mounted appliance
- 15 minute out-of-band deployment

Cloud Sensor:

- Deploys in AWS or Azure
- Ingests traffic via native traffic mirrors (AWS only) or agent-based solutions
- Rapid deployment

Corelight Virtual Sensor:

- Requires VMware ESXi 6.0 or above or Hyper-V on Windows Server 2016
- Up to 2 Gbps per instance
- Capacity licensed (independent of instances)
- 15 minute out-of-band deployment

Crowdstrike:

The Crowdstrike difference is defined as: World-class Intelligence, 24/7 Threat Hunting and providing Fully Managed Service. By World-class Intelligence, Crowdstrike is referring to cloud data that is enriched with threat intelligence to provide a **full picture of attacks** and the context needed to pivot to a proactive security posture. That capability is called 'Falcon X.' Falcon OverWatch proactively searches for threats on our customers behalf. An elite team of **threat hunters works 24/7** to catch what other solutions miss. Fully Managed Service goes by the name 'Falcon Complete.' This bridges resident experience gaps with a cost-effective way to address them. Experts will configure and operate while offering true remote remediation.

These products are cloud native, AI-powered and deploys a single agent that is fully operational on Day One.

CyberArk:

CyberArk is the undisputed leader in the Privileged Access Management market. Working with a market leader gives our customers the advantage of a proven leadership team, the industry's broadest global presence and the largest and most diverse customers. Privileged access management was born from the collaborative effort of CyberArk's founders and customers. Since then, the same team continues to introduce new products, define the market and lead with innovations, proven methodologies and thoughtful customer service. CyberArk is known as the market share leader and #1 vendor in the privileged access management space. It is used by 5300+ customers in 90 countries with over 50% of the Fortune 500 and over 35% of the Global 2000. CyberArk breaks down their offering into the following products:

CORE PRIVILEGED ACCESS SECURITY

Continuously discover and manage privileged accounts and credentials, record and monitor privileged sessions and remediate risky activities across on-premises, cloud and hybrid environments. Enable least privilege on both Windows and *NIX servers and detect and mitigate threats on domain controllers. The API-first approach enables full task automation and enhances functionality.

ALERO™

Enable secure remote vendor access to the most sensitive IT assets managed by CyberArk, without the need for VPNs, agents or passwords. Alero combines Zero Trust access, biometric multi-factor authentication, just-in-time provisioning and visibility into one single SaaS solution for providing remote vendors secure access to the CyberArk Core Privilege Access Security Solution.

APPLICATION ACCESS MANAGER

Control, manage and audit non-human privileged access for applications, including commercial off-the-shelf, in-house developed applications and applications developed using DevOps tools and methodologies -- across on premises, hybrid, cloud and containerized environments.

ENDPOINT PRIVILEGE MANAGER

Enforce least privilege, control applications, and prevent credential theft on Windows and Mac desktops and Windows servers to contain attacks and stop lateral movement.

CYBERARK PRIVILEGE CLOUD

Satisfy fundamental privileged access security requirements by utilizing CyberArk's expertise to manage the underlying infrastructure. With CyberArk Privilege Cloud, organizations can empower security and IT operations to focus on high-level tasks critical to the organization's security posture.

DarkOwl:

DarkOwl enables customers to search, monitor, and investigate content from current and historical darknet sites from the comfort of their browser. The four pillars of their approach are: Search, Streamline, Score and Monitor:

Search

Search the world's largest dataset of darknet content safely from your browser with DarkOwl Vision's User Interface. Use keywords, search pods, filters, and our own Lexicon reference tool to find what matters most.

Streamline

Integrate DarkOwl's data directly into your platform with our Vision API. Whether it is your own internal threat team enhancing their threat intelligence, or your customer-facing platform, our API makes our data easy to access in your native environment.

Score

Calculate the risk score of any organization based on the extent of their darknet footprint with all-new DARKINT Scores. For the cyber risk management industry, this is the data point you've been missing.

Monitor

Set up monitors on DarkOwl Vision and receive alerts if breached data appears on the darknet. Monitor your own organization's internal data, or your customer's personal information.

This is accomplished through four products:

Darknet data: Accessing the darknet directly requires you to download and utilize a number of specific technologies and precautionary tools (such as Tor and VPNs). Darknet sites are transient, with the average site coming up and down within 48 hours. Threat intelligence teams spend copious amounts of time tracking down darknet pages via directory sites, as there is no search engine for the darknet itself. Darknet sites are unpredictable and hard to keep track of, making effective use of the darknet as part of your information security program a difficult challenge. With DarkOwl, users can browse, monitor, and search near real-time content from darknet pages - without having to go onto darknets like Tor directly.

Vision UI: The user can investigate threat actors, search for bitcoin wallets and addresses, assess darknet brand exposure, identify threats on darknet forums, monitor for leaked credentials, see inside authenticated chatrooms, track vendors on marketplaces and access historical darknet accounts.

Vision API: Makes it easier to access darknet content without leaving current environment.

DARKINT Scores calculate how exposed an organization is on the darknet.

Demisto:

Demisto is a Palo Alto Networks Company that builds COPS (Collaborative Open Playbook Standard) for both automated and process-oriented operations. In addition to playbooks, they offer thousands of automations and hundreds of integrations on open-source. The release of Demisto v5.0 is packed with new features suggested to us by you, you, and even you there, throwing popcorn from the back row. Our community of customers, partners, and independent users are the reason we exist, and we're thrilled that you're a part of our journey. Demisto v5.0's new features help:

Personalize case layouts with a reimagined user interface

Gain indicator visibility with new threat intelligence capabilities

Achieve horizontal scalability with database scaling

The Cortex XSOAR version offers:

Unlimited Automations

Unlimited Incident History

Unlimited Threat Intelligence Feeds

Native Threat Intel with AutoFocus

Full Enterprise Reports Package

24/7 Customer Support

Multi-Tenancy

The Community Edition version offers:

166 Daily Automation Commands

Rolling 30-Day Incident History

5 Active Feeds/100 Indicators Per Feed

Not Included

Incident Closure Report

Slack DFIR Community

Single Tenant On!

Digital Shadows:

Digital Shadows offers a product called Searchlight™. SearchLight protects against external threats, continually identifying where your assets are exposed, providing sufficient context to understand the risk, and options for remediation. Searchlight™ is defined as offering: Phishing Protection, Dark Web Monitoring, Account Takeover Prevention, Threat Intelligence, Data Leakage Detection and Digital Footprint Monitoring.

The four areas where they excel are:

WIDER COVERAGE: The most comprehensive coverage across the open, deep, and dark web

DEEPER CONTEXT: Immediate context to enrich alerts and enable better decisionmaking faster

MORE RELEVANCY: By tailoring SearchLight from the outset, only relevant alerts affecting business and brand are sent

EXPERT SUPPORT: As a member of the team, they provide context, remediation options, and assistance with takedowns

Elastic:

The products in the [Elastic Stack](#) are designed to be used together and releases are synchronized to simplify the installation and upgrade process. The new release streamlines automated threat detection with the launch of a new SIEM detection engine and a curated set of detection rules aligned to the MITRE ATT&CK™ knowledge base, brings performance improvements to Elasticsearch, makes supervised machine learning more turnkey with inference-on-ingest features, and deepens cloud observability and security with the launch of new data integrations. And that's just a small slice of all that's new and exciting in this release.

The full stack consists of:

[Beats 7.6](#)

[APM Server 7.6](#)

[Elasticsearch 7.6](#)

[Elasticsearch Hadoop 7.6](#)

[Kibana 7.6](#)

[Logstash 7.6](#)

Exabeam:

The Exabeam Security Management Platform is a modern SIEM that helps security teams work smarter. Organizations can take advantage of its big data architecture, advanced analytics, and automation capabilities. Their SIEM is noted for four attributes:

Collect unlimited log data

The Exabeam security data lake combines a modern big data infrastructure and predictable user-based pricing so you can collect and quickly search all of your data sources in a central repository without making compromises due to lack of scalability or budget.

Detect and investigate complex and insider threat attacks

Exabeam's user and entity behavior analytics (UEBA) solution detects anomalous behavior and suspect lateral movements within your organization while machine-built timelines further reduce the time and specialization required to detect attacker tactics, techniques, and procedures.

Automate and orchestrate incident response

Exabeam's incident response solution allows analysts of all levels to combine out-of-the-box integrations with popular security solutions to automate response playbooks and replace manual, error prone processes to ensure timely, consistent results and improve response times.

Flexible deployment options

In addition to being deployed on-premises, the Exabeam Security Management Platform can be deployed on cloud infrastructure, as software-as-a-service or through a managed security service provider, to help CIOs and CISOs transition to the cloud.

Exiger:

Exiger was formed by a group of leading authorities on financial crimes compliance to solve some of the most complex problems confronting business today. The firm arms financial institutions and multinational corporations with the practical expertise and tools they need to prevent breaches in compliance, respond to risk intelligence, remediate gaps and monitor ongoing business activities. Exiger helps financial institutions, multinational corporations, and governmental agencies pursue their strategic goals with the confidence that regulatory change will not alter their course. In addition to its Monitorship work, Exiger guides a wide range of clients around the world through the process of managing the worst-case scenario compliance challenges and implementing the programs they need to prevent them in the future.

Their configuration for Due Diligence Investigation is called DDIQ. DDIQ is rolled into the Insight 3PM framework where its automated due diligence is coupled with Risk Assessments, Risk Modeling, Third-party segmentation, monitoring, ERP integration and population assessment. In addition they also staff Subject Matter Experts that can provide routine or surge support as the situation dictates.

ExtraHop:

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Their breakthrough approach analyzes all network interactions and applies cloud-scale machine learning for complete visibility, real-time detection, and intelligent response. Using this approach, they help the world's leading enterprises rise above the noise of alerts, organizational silos, and runaway technology. Whether it is investigating attacks, ensuring the availability of critical applications, or securing the investment in cloud, ExtraHop helps by detecting threats up to 95 percent faster and respond 60 percent more efficiently.

They do this through three products:

Reveal(X): Network Detection and Response

Reveal(X) Cloud: Detection and Response for AWS

Reveal(X) for IT Ops: Application and Network Performance

These three products define the type of solution sought:

SECURITY OPERATIONS

Threat Detection and Response

Secure Decryption

Enterprise IoT Security

Hygiene and Compliance

CLOUD-NATIVE SECURITY

Security for AWS

Security for Azure

Security for Google Cloud Platform

Cloud Migration

NETWORK PERFORMANCE

Security & Availability for Remote Access

NOC/SOC Integration

Remote Site Visibility

Triage & Troubleshooting

APPLICATION ANALYTICS

Commercial Application Visibility

Customer Experience Monitoring

Application Upgrade & Cloud Migration

F5: F5 Networks, Inc. is a transnational company that specializes in application services and application delivery networking (ADN). F5 technologies focus on the delivery, security, performance, and availability of web applications, including the availability of computing, storage, and network resources.

APPLICATION SERVICES:

Traffic Management
Infrastructure Security
Automation, Management, and Visibility

DEPLOYMENT OPTIONS:

Cloud Services (aaS)
Cloud Software
Hardware
Managed Services

NGINX APPLICATION PLATFORM

Their Service Portfolio includes:

Support Professional
Services
Training
Certification
Resources

Fidelis:

Fidelis Cybersecurity exceeds expectations because the cybersecurity products and their associated professional services are the solution of choice currently used worldwide. What makes Fidelis special is that it is outward looking from a vigilance perspective while at the same time meets industry-specific regulatory controls such as PCI, HIPPA, PHI, PII, and SOX to ensure that the enterprise is secure and compliant.

Coupled with this baseline are a portfolio of products to choose from:

- Fidelis Elevate™: Detects, hunts and responds to threats
- Fidelis Network: Detects threats and prevents data loss with Network Traffic Analysis
- Fidelis Endpoint: Speeds investigations with Endpoint Detection and Response
- Fidelis Deception: Reduces dwell time with dynamic Deception technology

This portfolio addresses a number of solutions:

- Asset inventory
- Cloud security
- Data Loss Prevention
- Email security
- Endpoint Detection and Response (EDR)
- Endpoint protection
- Holistic visibility
- Network traffic analysis
- Threat detection
- Managed Detection and Response (MDR)
- Office 365 Security
- Threat Hunting
- Incident Response

FireEye:

FireEye is an industry leader in security:

700+ frontline/intelligence experts

32 languages

23 countries

Over 2 decades of experience and more than 1 million hours per year on the frontlines of cyber attacks

380+ red team engagements per year and more than 60k hours

800+ incident response engagements per year

1 Million+ unique malware samples per day

They do this through a number of Enterprise Security platforms:

Helix Security Platform

Verodin Security Instrumentation

Network Security and Forensics

Endpoint Security

Email Security

Detection On Demand

They also provide five types of services:

Assess

Transform

Defend

Respond

Train

Flashpoint:

Flashpoint is the globally trusted leader in risk intelligence for organizations that demand the fastest, most comprehensive coverage of threatening activity on the internet. Fueled by a combination of sophisticated technology, advanced data collections, and human-powered analysis, Flashpoint tailors its offerings to customer requirements. From bolstering cyber and physical security, to detecting fraud and insider threats, Flashpoint partners with customers across the private and public sectors to help them rapidly identify threats and mitigate their most critical security risks.

Products and Services include:

- Intelligence Platform
- Compromised Credential Monitoring
- Threat Response & Readiness
- Flashpoint API

They also have additional support packages, using talent that addresses:

- Cyber threats
- Corporate and physical security
- Fraud
- Insider threat
- Vulnerability management

Forescout:

Forescout Technologies is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environments and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, real-time discovery and classification of every IP-connected device, as well as continuous posture assessment.

These products are: eyeSight, eyeSegment, eyeControl, eyeExtend, eyeManage, SilentDefense, CounterACT and ROI Calculator

Each platform addresses six areas:

Device Visibility: Continuously discovers, classifies and assesses every IP-connected device that touches the extended enterprise network to unify security management.

Asset Management: Automate inventories and maintains accurate asset details across IT and OT networks.

Device Compliance: Continuously assess devices, monitor them and enforce security policies to reduce compliance risk.

Network Access Control: Applies unified NAC policies across heterogeneous campus, data center, cloud and OT environments—with or without 802.1X.

Network Segmentation: Simplifies segmentation planning and automate ACL/VLAN assignment to reduce your attack surface.

Incident Response: Automates threat detection, prioritization and containment to accelerate incident response and mitigate risks.

Fortify:

Fortify offers end-to-end application security solutions with the flexibility of testing on-premises and on-demand to scale and cover the entire software development lifecycle. Their automated application security helps developers and AppSec pros eliminate vulnerabilities and build secure software.

They do this through:

- 1) Finding vulnerabilities directly in the developer's IDE with real-time security analysis or save time with machine learning-powered auditing.
- 2) Assembling a team of experts who deliver optimization, results review, and false positive removal as part of their global 24/7 support. Choices are on-premises, as a service or hybrid.
- 3) CI/CD integration in order to make security scans a part of the build/release process. This enables full automation and workflow support. Defect management integrations provides transparent remediation for security issues.
- 4) Automation and scaling: Expands with centralized scanning capabilities that support mature AppSec programs running 1000s of scans per day. Automates security in the CI/CD pipeline with the tools already in use.

Other available products are:

- Fortify on Demand (FoD): Application Security as a Service (AppSEC SaaS)
- Fortify Static Code Analyzer: Static Application Security Testing (SAST)
- Fortify Webspect: Dynamic Application Security Testing (DAST)
- Fortify Application Defender: Runtime Application Self-Protection
- Fortify Software Security Center: Integrates and automates application security testing

Google:

Their offering called Chronicle offers the following:

Security Analytics and operations
Application security
BeyondCorp Remote Access

They clarify the three as:

Analyze risks at the speed of search

Ingest, index, correlate, and use new telemetry, in seconds. Analyze massive amounts of historical security data to gain visibility and insights. With Chronicle, you can combine intelligence about threats both in the wild and inside your network to speed investigations.

Protect users with up-to-date intel

Google Cloud's user protection technology is proven through Google's years of experience keeping people safe online. But protecting your users today also requires our constantly updated lists of unsafe web resources to identify phishing and deceptive sites as well as sites that host malware or unwanted software.

Rely on Google's global infrastructure

Protect your users, data, and applications, using the same secure-by-design infrastructure, built-in protection, and global network that Google relies on.

Fully scalable security analytics

Built on core Google infrastructure, our security analytics solutions give you an elastic container for [storing huge volumes](#) of enterprise security telemetry.

Up-to-date intelligence

Our [user protection services](#) include data on more than a million unsafe URLs and stay current by examining billions of URLs each day.

Rapid deployment

Cloud-based security means new analytics and protection services can be spun up in hours or even minutes.

Interos:

With a team of analysts, Interos researched and assessed individual suppliers, providing customers complete supply chain maps, identifying risks and alerting businesses to areas that required attention. Keeping pace with the growing complexity of global supply chains required finding a faster way to keep pace with the complex risk-influencing events that occur every day. In 2015 the company took a massive leap forward, embracing the power of emerging technology and beginning development of an automated platform that would provide multi-tier, multi-factor risk scoring on a continuous basis. Today their knowledge graph contains and analyzes information on over 50 million relationships, making it the world's largest company database. Using this technology coupled with natural language processing, and machine learning, Interos ingests over 85,000 information feeds, processing 250 million risk events per month. Interos instantly visualizes the most complex multi-tier, 3rd party relationships updating and alerting to changes in risk along five factors— financial, geographic, compliance, cyber and strategic.

The offering provides:

Graphs of ecosystems include: Networks, geographic concentration, radial and hierarchical
Sanction controls: This includes filtering suppliers by country, risk factor, industry and tier so you can get to the information that matters most to you, fast. Risk factors include: Financial, Operations, Governance, Geographic and Cyber

High Risk Outlier Protection: Machine Learning parses 85,000 data sources for a real-time view and customized alerts of your highest risk suppliers.

Risk Insights: Provides risk scores for an individual company across all 5 risk factors: ESG Concerns, Trade Compliance and Political Exposure.

Juniper:

Juniper follows three business model approaches: Enterprise, Cloud Provider and Service Provider. These are further defined by a number of specific areas: 5G Networking, Automation, Data Center, Metro Fabric, Remote Work, Security, Segment Routing and SD-WAN/SD-LAN.

Products:

Identity & Policy Control
Network Edge Services
Network Operating System
Packet Optical
Routers
SDN, Management & Operations
Security
Switches
Wired & Wireless Access
End of Life Management

Services:

Advisory
Implementation
Maintenance
Managed Services
Onsite Technical Services
Remote Operational Services
Testing as a Service

As an OEM, Juniper has one of the most comprehensive training and certification programs in the industry.

KnowBe4:

KnowBe4 is recognized by Gartner's as the highest and furthest overall in the **2019 Magic Quadrant for the Security Awareness Computer-Based Training (CBT) market**. This is the third consecutive year KnowBe4 has been recognized as a Leader in this report. Led by legendary hacker Kevin Mitnick, their offerings fall into the following categories:

- 1) Kevin Mitnick Security Awareness Training
- 2) KnowBe4 Enterprise Security Awareness Training Program with modules dedicated to:

- Credit Card Security
- CEO Fraud
- Common Threats
- Passwords
- Financial Institution Physical Security
- GDPR (EU Data Rights)
- GLBA Security Awareness Training (Financial Institutions)
- Handling Sensitive Information
- Mobile Device Security
- PCI Compliance Simplified
- Ransomware for Hospitals
- Safe Web Browsing
- Social Engineering Red Flags
- The Danger Zone (Responding to social engineering attacks)
- Your Role, Internet Security and You
- Email Spoofing
- USB Attack

Lookout:

The Lookout Security Platform consists of:

Security Protections:

- Mobile Threat Defense
- Phishing Protection
- Web Access Controls

Security & IT Operations:

- Data Protection Integrations
- Mobile Vulnerability Management
- Mobile App Reputation
- Security Event Forensics

Intelligence:

- Malware Analysis
- Threat Intelligence

Application Development:

- In-App Protection

Their services cover:

Lookout App Security Assessment - Lookout App Security Assessment offers a comprehensive, white-glove app analysis by Lookout's elite mobile security research team, paired with app insights from Lookout's corpus of over 70 million analyzed apps. Lookout reviews all dimensions of app risk including code construction, permissions, behavior, malware, network traffic, vulnerabilities, and prevalence.

Lookout Threat Advisory - Lookout Threat Advisory provides cutting-edge mobile threat intelligence from Lookout's global sensor network of millions of mobile devices and insights from Lookout's top mobile security researchers. Customers get access to monthly threats reports and analyst inquiry calls, quarterly webcasts, and also get early access to novel Lookout threat research.

McAfee:

Products

[Endpoint Security](#)

[Cloud Access Security Broker \(CASB\)](#)

[Endpoint Detection & Response](#)

[Data Loss Prevention](#)

[ePolicy Orchestrator](#)

[Mobile Security](#)

[SaaS Security Management](#)

[SIEM](#)

[Network Security Platform](#)

[Web Gateway](#)

Of the featured solutions, Endpoint Protection is the most straightforward. The other two, Cloud Security and their MVISION offering begs further clarification. MVISION Cloud can provide complete visibility into an organization's SaaS, PaaS, and IaaS usage. Discovered SaaS and PaaS services in-use are matched against the MVISION Cloud Registry and reported accordingly in one of the 30+ service type categories or one of the 120+ sub-categories. For example, Salesforce.com SaaS service usage would be discovered and categorized as CRM, while the force.com PaaS platform usage would be discovered separately and categorized as a Development service. IaaS services are handled a little differently as many public cloud service providers choose to host on IaaS platforms. For example, Dropbox hosts its SaaS service on Amazon AWS. Also, many organizations may choose to migrate and build their own bespoke cloud apps on IaaS platforms. To address this and provide complete visibility into IaaS usage, MVISION Cloud performs the following:

If the web request (Dst Host, URL or Dst IP) does not match an existing SaaS or PaaS service from the MVISION Cloud Registry, MVISION Cloud attempts to match the Dst IP to one of 20+ known IaaS providers. If the Dst IP matches one of the 20+ known IaaS providers, MVISION Cloud initiates a TLS handshake session with the destination service to retrieve the SSL certificate. The SSL certificate is examined and MVISION Cloud attempts to match the customer's domain names against the certificate. If a match is found, the service is automatically added to the MVISION Cloud Registry as one of the customer's own custom apps and its usage is reported on accordingly. Some of the 20+ IaaS providers MVISION Cloud tracks include but are not limited to: Amazon AWS, Microsoft Azure,

Micro Focus:

Micro Focus delivers on the promise of smart digital transformation. By delivering solutions that bridge the existing and the new, Micro Focus allows customers to sidestep the risky and time-consuming prospect of digitally transforming from scratch. This helps make IT work harder and allows the organization to run and transform at the same time.

Their portfolio includes:

[Analytics and big data](#)

[Application development, test, and delivery](#)

[COBOL](#)

[Collaboration solutions](#)

[Information management and governance](#)

[Business continuity](#)

[IT operations management](#)

[Mainframe](#)

[Security](#)

Their support and services are primarily consultant-oriented around:

Analytics and Big Data

Cyber Security

DevOps

IT4IT Value Chain Consulting

Application Delivery Management

Mobile Application Lifecycle

Hybrid Cloud Management and Brokerage

Data Center Automation

Operations Management

Service Management

Global Product Authentication

OPSWAT:

OPSWAT solutions are based on a Zero Trust framework that applies [Deep Content Disarm and Reconstruction \(CDR\) technology](#) to scan and sanitize all files and ensures the integrity of devices via its [Access Control Certification](#) program. For more than a decade, OPSWAT technology has been white labeled to power NAC, SDP, SSL VPN, and secure device access for Cisco, Palo Alto Networks, Pulse Secure and other leading network vendors. The OPSWAT [MetaAccess](#) product line also integrates with leading SDP solutions such as Symantec Secure Access Cloud and others, providing critical infrastructure customers with easy-to-use secure cloud and network access.

These technologies would be used to execute:

[Deep Content Disarm and Reconstruction \(Deep CDR\)](#)

[Multiscanning](#)

[File-Based Vulnerability Assessment](#)

[Proactive Data Loss Prevention \(Proactive DLP\)](#)

[Threat Intelligence Platform](#)

[Endpoint Compliance](#)

[Endpoint Vulnerability Assessment](#)

[Endpoint Malware Detection](#)

[Endpoint Application Removal](#)

[Data Protection](#)

These solutions focus in areas related to:

Cross-Domain Solutions

Secure Device Access

Network Access Control

File Upload Security

Malware Analysis

Email Security

They also provide developer tools:

[MetaDefender](#)

[CoreMetaDefenderCloud API](#)

[MetaAccess API](#)

[OESIS Framework SDK](#)

[Threat Intelligence Feed](#)

They also provide training and an extensive resource depository.

Palo Alto:

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Their mission is to be the cybersecurity partner of choice, protecting our digital way of life. They do this by helping address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, they are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices.

Their products are broken down into three categories:

Secure the Enterprise:

STRATA prevents attacks with the industry-leading network security suite, which enables organizations to embrace network transformation while consistently securing users, applications, and data, no matter where they reside. STRATA has three offerings: [Next Generation Firewall](#), [Security subscriptions](#) and [Panorama](#)

Secure the Cloud:

Prisma Cloud offers the industry's broadest security and compliance coverage—for applications, data, and the entire cloud native technology stack—throughout the development lifecycle and across multi- and hybrid cloud environments. Prisma Cloud offers: [Prisma Cloud](#), [Prisma Access \(SASE\)](#), [Prisma SaaS](#) and [VM-Series](#).

Secure the Future:

Cortex is the industry's most comprehensive product suite for security operations empowering enterprises with the best-in-class detection, investigation, automation and response capabilities. These products are: [Cortex XDR](#), [Cortex XSOAR](#), [Cortex Data Lake](#) and [AutoFocus](#).

Phantom:

Phantom is a purpose-built, community-powered **security automation**, and **orchestration platform**. The company's mission is to close the **security gap** by enabling enterprise **security operations** to be smarter, faster, and stronger. Having been acquired by Splunk (Noted in a separate tab), Splunk Phantom provides security orchestration, automation and response (SOAR) capabilities that allow analysts to improve efficiency and shorten incident response times. Organizations are able to improve security and better manage risk by integrating teams, processes and tools together. With Phantom, security teams can automate tasks, orchestrate workflows and support a broad range of SOC functions including event and case management, collaboration and reporting. They do this by:

Orchestrating Security Infrastructure Using Phantom Apps

Phantom's flexible app model supports hundreds of tools and thousands of unique APIs, enabling you to connect and coordinate complex workflows across your team and tools. Powerful abstraction allows you to focus on what you want to accomplish, while the platform translates that into tool-specific actions.

Automating Security Actions using Phantom Playbooks

Phantom enables you to work smarter by executing a series of actions — from detonating files to quarantining devices — across your security infrastructure in seconds, versus hours or more if performed manually. Codify your workflows into automated playbooks using our visual editor (no coding required) or the integrated Python development environment.

Collaborating and Responding to Security Incidents Fast

Drive efficient communications across your team with integrated collaboration tools. Use Phantom event and case management to rapidly triage events in an automated, semi-automated, or manual fashion. Confirmed events can be aggregated and escalated to cases within Phantom, which enable efficient tracking and monitoring of case status and progress. Measure and report on all SecOps activity through the platform to provide human oversight and auditing

Phantom on Mobile App

Security orchestration, automation, and response from your mobile device. Work smarter, respond faster, and strengthen defenses — now from anywhere at anytime. No need to open your laptop. Orchestrate security operations from the palm of your hand. Respond faster than ever before, because it's reachable from anywhere. Run playbooks, triage events, and collaborate with colleagues — all on-the-go.

Proofpoint:

Proofpoint is a unique cybersecurity company in that their products and services focus on the human actor in an organization. Their approach is to stop email and cloud-based threats, including malware, credential phishing and email fraud. Their goals are to: Stop impostors from spoofing, Block the entire spectrum of email threats, including malware, phishing and email fraud and Resolve threats more quickly and effectively.

They offer:

- General security awareness training and targeted training for users most at risk
- Conducts phishing simulation based on real-world attack techniques
- Isolates users' personal web and email activity from the corporate network Ecosystem protection Secure the digital channels you don't own. Block impostor attacks and malicious content that use trusted and lookalike email and web domains, social media, the dark web, and more.
- Prevents email domain spoofing through DMARC authentication
- Identifies and take down lookalike websites and social media accounts
- Stop fraudulent email before it reaches users' inbox Information protection
- Protects most sensitive data and complies with ever-evolving regulations—without the headaches and costs of legacy data protection tools.

Proofpoint helps by:

- Collecting, archiving, supervising and managing protected data sent via email through transparent, automated encryption
- Understanding where your most sensitive data lives and manage it in a compliant, legally defensible manner
- Preventing data exposure and inappropriate access to data in cloud apps controlling who—and what apps—have access to it
- Collecting, archiving, supervising and monitoring sensitive data in a compliant and legally defensible manner without the cost and hassle of traditional compliance tools.
- Meet regulatory, legal, and corporate compliance requirements quickly and accurately
- Manage the cost and complexity of staying in compliance at scale
- Get greater insight into archived data for greater control and decision-making power

Pulse Secure:

Pulse One provides central policy management that enables secure access for all endpoints and mobile devices to corporate applications that may be located on-premise or in the cloud. The color coded dashboard allows IT managers to easily check their organization's security status. Their portfolio of products are broken down as follows:

Pulse Access Suite

[Zero Trust Access Overview](#)

[Pulse Access Suite Editions](#)

[Pulse One Manager](#)

[Pulse Secure Appliance](#)

Software Defined Perimeter

[SDP Overview](#)

[Pulse SDP](#)

Secure Remote Access

[VPN Overview](#)

[Pulse Connect Secure \(VPN\)](#)

[Pulse Cloud Secure](#)

[In Case of Emergency \(ICE\)](#)

[Secure Access Emergency Readiness](#)

Network Visibility, NAC, IoT Security

[NAC Overview](#)

[Pulse Profiler](#)

[Pulse Policy Secure \(NAC\)](#)

Application Delivery Controller

[Virtual ADC Overview](#)

[Virtual Traffic Manager](#)

[Virtual Services Director](#)

[Virtual Web Application Firewall](#)

Unified Endpoint Management

[Pulse Workspace](#)

[Pulse Client](#)

Their support includes 24/7 assistance. The Gold Package is the norm while the Platinum package is for 250+ users.

RedHat:

For over 25 years, RedHat has revolutionized the operating system with [Red Hat® Enterprise Linux®](#). Now, they boast a broader [portfolio](#), including hybrid cloud infrastructure, middleware, agile integration, cloud-native application development, and management and automation solutions. They segment their offerings around: Infrastructure, Integration, Cloud, App Development, Automation & Management.

They do this through:

Platforms:

[Red Hat Enterprise Linux](#)

[Red Hat JBoss Enterprise Application Platform](#)

[Red Hat OpenStack Platform](#)

[Red Hat Virtualization](#)

Middleware:

[Red Hat Runtimes](#)

[Red Hat Integration](#)

[Red Hat Process Automation](#)

[Red Hat Middleware Portfolio](#)

Cloud computing:

[Red Hat Cloud Suite](#)

[Red Hat Hyperconverged Infrastructure](#)

[Red Hat OpenShift](#)

[Red Hat OpenStack Platform](#)

[Red Hat Quay](#)

Application development:

[Red Hat CodeReady Studio](#)

[Red Hat CodeReady Workspaces](#)

[Red Hat JBoss Enterprise Application Platform](#)

[Red Hat OpenShift](#)

[Red Hat Middleware Portfolio](#)

Storage:

Red Hat OpenShift Container Storage

Red Hat Ceph Storage

Red Hat Hyperconverged Infrastructure

RedSeal:

RedSeal provides a cyber terrain analytics platform by which every organization can be confident that it understands what's on the network, how it's connected and the associated risks. The primary input for your network model comes from configuration files RedSeal takes in from switches, routers, firewalls and load balancers. RedSeal integrates with your public cloud and private cloud managers to include all your network environments in the network model. Then RedSeal's cyber terrain analytics platform imports host and vulnerability data from vulnerability scanners and other sources. This network modeling is done without agents, span ports or taps and without being in line with production traffic or consuming net flow data. With this information, RedSeal uses its patented algorithms to calculate an accurate model of your network and how data can move through it. You can liken this to the roads on a map. RedSeal can show you how (or if) data can move from any point to another with network modeling. Next, in network modeling, RedSeal overlays the host and endpoint information, along with identified vulnerabilities.

They target their offerings towards:

- Compliance
- Cyber Insurance
- Executive Solutions
- Incident Response
- Vulnerability Management

They support customers through:

- Professional Services
- Customer Support
- Training

RSA:

RSA manages digital risk with a range of capabilities and expertise including integrated risk management, threat detection and response, identity and access management, and fraud prevention. RSA® Business-Driven Security™ solutions addresses critical risks that organizations across sectors are encountering as they weave digital technologies deeper into their businesses. Broken down into products and services, RSA offers:

Products:

[Identity and Access Management](#)

[Integrated Risk Management](#)

[Omnichannel Fraud Prevention](#)

[Threat Detection and Response](#)

Services:

[Advisory and Assessment](#)

[Implementation and Optimization](#)

[Incident Response and Cyber Defense](#)

[Technical Support](#)

[Training](#)

Sayari:

Sayari is a data provider and commercial intelligence platform, serving financial institutions, legal and advisory service providers, multinationals, journalists, and governments. Thousands of analysts and investigators in over 35 countries rely on their products to safely conduct cross-border trade, research front-page news stories, confidentially enter new markets, and prevent financial crimes such as corruption and money laundering. To visualize the data, the 'Sayari Graph' is the first purpose-built tool for navigating complex global corporate ownership and commercial relationships. This provides a complete picture of customers, vendors, and third-parties, while maintaining provenance back to primary source documents. This Graph can be delivered as a cloud application with an intuitive user interface, REST API, data subscription, or on-premise.

If you are familiar with relationship graphs, these are possible when fed by:

Normalized Global Public Records Data: Their proprietary pipelines collect, extract, enrich, match, and analyze high-value public information from over 150 countries.

Multilingual Search Across Jurisdictions & Attributes: Sayari Graph enables users to search records from around the world with the freedom to select specific data attributes or free text search.

Original Source Documentation Provided for Every Relationship & Attribute: Official public records are essential to understanding the ownership and control links tied to potential clients, vendors, or targets of an investigation.

Navigate & Visualize Cross-Border Corporate Hierarchy, UBO & Subsidiary Structures: Sayari Graph enables users to quickly navigate complex, cross-border corporate structures with network visualizations powered by custom graph-based matching and entity resolution models, built on a foundation of investigative and regional domain expertise.

Data Refreshes & Timeline View of Corporate Entities: Sayari provides time-stamped copies of records after every data refresh cycle so users can rewind ownership history and assess historical changes.

SecureAuth:

SecureAuth, the secure identity company, is used by leading organizations to secure workforce and customer identities everywhere: hybrid, on-prem, and the cloud. With the SecureAuth® Identity Platform, organizations can secure access for everyone and everything that connects to their business. SecureAuth helps reduce threat surface, enable user adoption and meet business demands by delivering a frictionless user experience that drives engagement and productivity. SecureAuth provides the most flexible and adaptable identity and access management solution available to help you prevent identity-related breaches. They categorize their offerings as follows:

IDENTITY PLATFORM: The SecureAuth® Identity Platform provides the flexibility required to meet the security and usability requirements for your diverse population of identities — workforce and customer.

Intelligent Identity Cloud: The SecureAuth Intelligent Identity Cloud delivers out of the box functionality that enables highly flexible and highly secure experiences for every identity, without the need for cumbersome implementations and integrations with third party services.

Adaptive Authentication: Adaptive authentication provides additional security without impacting usability. That's because risk checks automatically take place without users even being aware. Multi-factor authentication is only required if risks are detected.

Multi-Factor Authentication: Through the use of multiple risk checks, SecureAuth only forces a multi-factor authentication (MFA) step if risk is identified. Of the 617 million authentications processed last year, 90% did not require an MFA step.

Single Sign-On: Enterprise single sign-on (SSO) provides a seamless experience by enabling workforce and customer identities to provide credentials once and gain access to many applications and systems. Adaptive and multi-factor authentication ensure only the right users at the right time.

User Self-Service: Ensure users stay productive wherever they are by empowering users to self-service:

- Password resets
- Account lock-outs
- Profile updates
- Device enrollments

ServiceNow:

ServiceNow specializes in revolutionizing workflow improvement through IT. They do this through the following product offerings on a single, unified, digital platform:

- [IT Service Management](#)
- [IT Operations Management](#)
- [IT Business Management](#)
- [IT Asset Management](#)
- [DevOps](#)
- [Security Operations](#)
- [Governance, Risk, and Compliance](#)

The goal of this platform is to:

- [Automate work for everyone](#): Empower anyone to automate, extend, and build digital workflow apps across the enterprise with a single, unified platform.
- [Deliver seamless experiences](#): Achieve new levels of user productivity and satisfaction with intuitive mobile experiences that are as easy to use as common consumer apps.
- [Connect your enterprise](#): Rapidly unite people and processes with intuitive, cross-enterprise integrations for ServiceNow solutions and external services.
- [Work intelligently](#): Seamlessly embed AI and analytics in every app. Predict issues, make smarter business decisions, and help people get work done easier and faster.

Solarwinds:

Solarwinds is a leading provider of powerful and affordable IT infrastructure management software. Their products give organizations worldwide, regardless of type, size or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-premises, in the cloud, or in hybrid models.

Products:

- Network Management
- Systems Management
- Database Management
- IT Security
- IT Service Management
- Application Management
- Managed Service Providers Solutions:

[IT Security Solutions](#)

[Enterprise Solutions](#)

[IT Operations Solutions](#)

[Network Solutions](#)

[Database Management](#)

[IT Service Desk Solutions](#)

[Infrastructure Management](#)

[IT Help Desk](#)

[Application Performance Solutions](#)

[IT Asset Solutions](#)

[ITSM Solutions](#)

[ITIL Solutions](#)

[Office 365 Solutions](#)

[Azure Cloud Solutions](#)

[Active Directory](#)

[Cisco Solutions](#)

[Employee Experience Solutions](#)

[Scalability Solutions](#)

[SolarWinds Orion Platform](#)

[SolarWinds Customer Success](#)

[MSP Solutions](#)

[Compliance Solutions](#)

Splunk:

Their claim is that customers choose Splunk to: Act faster and accelerate innovation, Amplify the data's impact, and the ability to scale without the noted stress that goes with it. Part of their brand equity is the community they have grown around themselves. They also have a well-developed ecosystems of partners and developers to constantly improve the user experience, This culminates in robust Service, Support and Training packages that places them on par with the largest OEMs in the industry.

Their product configuration focuses on the following:

IT Operations: Predict and prevent problems with one unified monitoring experience. Monitoring could be infrastructure monitoring, application monitoring as well as business and IT service monitoring.

Event Management: Splunk uses AI powered by machine learning to reduce noise by clustering events. Their newest innovation is called VictorOps. VictorOps is a SaaS-based collaborative incident response system that connects alerts to the people that can solve them. Together, Splunk ITSI and VictorOps decrease downtime and reduce alert fatigue by helping on-call teams quickly act on the most relevant and important events from Splunk ITSI. VictorOps integrates seamlessly with the tools you already use, enabling cross-team collaboration across web and mobile interfaces. After incident resolution, teams have all the data they need to conduct blameless post-incident reviews and improve their processes moving forward.

DevOps: For IT teams adopting DevOps, Splunk software helps improve velocity, quality and the business impact of app delivery. Unlike other solutions that focus on discrete release components, Splunk provides real-time insights across all stages of the delivery lifecycle.

Infrastructure Monitoring: Splunk App for Infrastructure (SAI) unifies and correlates logs and metrics, providing an integrated experience for monitoring, troubleshooting, and alerting. Help to prevent outages, ensure uptime and maintain performance.

Predictive Analysis: Splunk ITSI uses machine learning to predict and prevent imminent outages up to help 30 minutes before so your team can prevent it from ever happening. Gain access to both a high-level view of service health and performance while also being able to dive deeper into investigations to find the root cause of a problem faster.

Swimlane:

Swimlane is a leader in security orchestration, automation and response (SOAR). By automating time-intensive, manual processes and operational workflows and delivering powerful, consolidated analytics, real-time dashboards and reporting from across your security infrastructure, Swimlane maximizes the [incident response capabilities](#) of over-burdened and understaffed security operations. Swimlane was founded to deliver scalable, innovative and flexible security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages. Swimlane is at the forefront of the growing market for [security automation and orchestration](#) solutions that automate and organize security processes in repeatable ways to get the most out of available resources and accelerate incident response. Swimlane offers a broad array of features aimed at helping organizations to address both simple and complex security activities, from prioritizing alerts to remediating threats and improving performance across the entire operation.

Swimlane's specialty is Security Orchestration, Automation and Response (SOAR). They do this through Security automation, orchestration and response speeds up the incident response process by replacing repetitive, manual tasks with automated workflows. Manual incident response processes, insufficient workflows and difficulty hiring security personnel leave security operations teams struggling to keep up with the growing volume of alerts. SOAR combines automated data gathering, security automation, case management and analytics to provide organizations the ability to easily implement sophisticated defense-in-depth capabilities based on internal and external data sources.

Swimlane's SOAR platform helps organizations manage the growing volume of alerts more efficiently by automating time-consuming incident response processes. The solution collects security alert data from virtually any security platform with minimal effort and then automatically responds to alerts using [automated workflows and playbooks](#).

To augment their SOAR offering, Swimlane has an support, service, training and certification infrastructure built around the product.

Symantec:

Symantec has been a leader in IT security for some time. Now a division of Broadcom (

they have three product categories:

Endpoint Security: For prevention, detection, and response using advanced, multi-layered defenses for all devices and operating systems - now cloud delivered with an intelligent, AI-driven security console and a single agent. Their approach is to prevent attacks, reduce attack surface, prevent breaches, remediate and respond to advanced threats.

Information Security: Safeguards the most confidential data through secure access and keeps employees productive, wherever they are. They do this through data protection, SaaS and corporate assets protection, storage protection, authentication, compliance and monitoring hybrid cloud workload infrastructure.

Web Security: Stops inbound and outbound threats targeting end users, information, and key infrastructure.

Tanium:

Tanium offers a unified endpoint management offering whose security platform closes IT gaps. Tanium provides two solution packages: Unified Endpoint Management and Unified Endpoint Security. This approach reduces complexity, improves efficiency and closes the gaps between operations and security.

UNIFIED ENDPOINT MANAGEMENT (UEM)

Asset Discovery and Inventory

Patch Management

Software Management

Configuration Management

Performance Monitoring

UNIFIED ENDPOINT SECURITY (UES)

Asset Discovery and Inventory

Data Risk and Privacy

Endpoint Detection and Response

Vulnerability and Configuration Management

The Tanium Platform is broken down into the following products:

IT Operations:

Tanium Asset: *Hardware and software inventory and usage tracking.*

Tanium Deploy: *Operating system and application installation, update and removal.*

Tanium Discover: *Unmanaged hardware and software discovery.*

Tanium Map: *Application component, dependency and relationship mapping.*

Tanium Patch: *Operating system and application patch management.*

Tanium Performance: *End user experience management.*

Risk and Security:

Tanium Comply: *Vulnerability management and configuration compliance.*

Tanium Integrity Monitor: *Operating system, application and log file monitoring for compliance.*

Tanium Protect: *Native operating system security controls management.*

Tanium Reveal: *Sensitive data discovery and management.*

Tenable:

Started with Tenable.io, the world's first Cyber Exposure platform. Tenable's goal is to arm Security with the visibility to see their entire cyber attack surface at all times (from IT to Cloud to IoT to OT) and arms the CISO, C-suite and Board of Directors with the insight to focus on the issues which matter most and make better strategic decisions.

Their list of products are as follows:

tenable.io: Accurately identify, investigate and prioritize vulnerabilities. Tenable.io® Container Security seamlessly and securely enables DevOps processes by providing visibility into the security of container images – including vulnerabilities, malware and policy violations – through integration with the build process. Managed in the Cloud. Tenable's PCI ASV solution, a Tenable.io workbench, leverages Tenable.io Vulnerability Management scanning to streamline the ASV process, including running scans, resolving disputes and preparing compliant scan reports as required by PCI 11.2.2. Tenable.io® Web Application Scanning safely, accurately and automatically scans your web applications, providing deep visibility into vulnerabilities and valuable context to prioritize remediation.

tenable.sc: Same as io above but managed On-Prem

Tenable Lumin: Provides advanced visualization, analytics and measurement solution, to understand and reduce Cyber Exposure. Lumin transforms vulnerability data into meaningful insights to help manage cyber risk across the entire organization.

Nessus: A variety of tools that explore vulnerability. This was the beginning product of all that followed. Nessus was built from the ground-up with a deep understanding of how security practitioners work. Every feature in Nessus is designed to make vulnerability assessment simple, easy and intuitive. The result: less time and effort to assess, prioritize, and remediate issues.

tenable.ot: IT and OT infrastructures are rapidly converging. The days of air-gapped systems are gone. Industrial and critical infrastructure organizations are adopting IoT devices at an unprecedented rate. As these environments converge and expand, the attack surface and attack vectors do, too. That means potential blind spots across converged IT/OT infrastructure that leads to unacceptable risk.

Thycotic:

Their speciality is Privileged Access Management (PAM).

Their categories of products encompassing Privileged Access and Password Management are:

[Secret Server](#)

[Account Lifecycle Manager](#)

[Privileged Behavior Analytics](#)

[Password Reset Server](#)

[DevOps Secrets Vault](#)

[Connection Manage](#)

For Least Privilege and Application Control, they offer:

[Privilege Manager](#)

[Unix Protection](#)

Their services are broken down into:

[Secret Server Packages](#)

[Privilege Manager Packages](#)

[Custom Services](#)

[Partner with our professional services team or one of our partners](#)

[Professional Services Support Packages Overview](#)

Their training is primarily an E-Learning Center offered remotely. These courses are designed to boost the skills of IT administrators, systems administrators, and security professionals responsible for using and maintaining Secret Server, Privileged Behavior Analytics and Privilege Manager. Courseware involves:

The Basics – How to configure groups, roles, permissions, folders, dashboards, and everything else you need to get started.

Access & Approval Workflows – Configure access to privileged accounts with best practice protections.

Automatic Password Changing & Discovery – Learn how Secret Server can automate your privileged account security to meet compliance and protect your organization against backdoor accounts.

Advanced Reporting, Monitoring, & Alerts – See how you can use out of the box monitoring, or customize to meet your security & compliance policies.

Technology Integrations – Find out how you can add security and automation to vulnerability scanning, SIEM

Titus:

Titus is a global leader in delivering solutions that helps organizations meet their data identification, classification, and protection needs. The company's products enable organizations to discover, classify, protect, analyze and share information. Used in over 120 countries, customers trust Titus to keep their data compliant and secure, including some of the largest financial institutions, manufacturing companies, Government and militaries across the G-7 and Australia as well as Fortune 2000 companies.

Designed to take the complexity out of data management and becoming cumbersome on productivity, Titus configures their suite into the following:

Titus Classification Suite: Data classification is the foundation of data security. Add rich context to on-prem and cloud data with the leading data classification solution.

Titus Illuminate: Scan and analyze unstructured data at rest and apply appropriate identification attributes to help you understand what sensitive data is stored in your systems.

Titus Accelerator: Powered by Machine Learning, Titus Accelerator detects personally identifiable information (PII) at creation in email and files and prevent inadvertent disclosures.

Veeam:

Veeam® is the leader in backup solutions that deliver Cloud Data Management™. Veeam provides a single platform for modernizing backup, accelerating hybrid cloud and securing your data. They pride themselves on solutions that are simple to install and run yet flexible enough to fit into any environment.

For Public Sector clients, they offer:

Veeam Availability Suite: [Veeam® Availability Suite™](#) is Veeam's flagship solution that makes data management simple, flexible and reliable. It combines the industry-leading backup, restore and replication capabilities of Veeam Backup & Replication™ with the advanced monitoring and analytics of Veeam ONE™.

Veeam Backup & Replication: [Veeam Backup & Replication](#) delivers Availability for ALL your cloud, virtual and physical workloads. Through a simple-by-design management console, you can easily achieve fast, flexible and reliable backup, recovery and replication for all your applications and data.

Veeam Agent for Microsoft Windows: [Veeam Agent for Microsoft Windows](#) is a key component of Veeam Backup & Replication. It provides a comprehensive backup and recovery solution for Windows-based servers, workstations, and cloud instances.

Veeam Agent for Linux: [Veeam Agent for Linux](#), part of Veeam Backup & Replication, is a comprehensive backup and recovery solution for Linux-based workstations, cloud instances, and servers, that helps organizations protect diverse environments.

Veeam ONE: [Veeam ONE](#), part of Veeam Availability Suite, provides comprehensive monitoring and analytics for backup, virtual and physical environments including proactive alerts, capacity planning and chargeback, and Intelligent automation and diagnostics.

Veeam Backup for Nutanix AHV: Get Availability for all applications and data hosted on the [Nutanix Acropolis Hypervisor \(AHV\)](#), offering a highly available, hyper-converged infrastructure solution that delivers resilient scale-out capability.

Veeam Backup for AWS: Get AWS-native backup that's cost-effective and secure. Easily recover from any cloud data loss scenario – whether due to outages, accidental deletion, malware and more – in minutes

Veeam Agents for IBM AIX and Oracle Solaris: [Veeam Agents for IBM AIX and Oracle Solaris](#) offer a single, comprehensive data protection platform to protect all data, applications and systems that exist in enterprise environments.

Veeam Availability Orchestrator: [Veeam Availability Orchestrator](#) delivers a recovery orchestration engine for replicas and backups, purpose-built for today's DR needs. Plan, prove and execute your DR strategy in as little as one-click.

Veeam Backup for Office 365: Eliminate the risk of losing access and control over your [Office 365 data](#), including Exchange Online, SharePoint Online and OneDrive for Business, with the ability to store it anywhere — on premises or in cloud object storage.

Veeam Management pack for System Center: [Veeam Management Pack™ \(MP\)](#) for System Center is the most comprehensive and intuitive System Center extension for app-to-metal management of VMware vSphere, Microsoft Hyper-V and Veeam Backup & Replication.

Veritas:

Veritas specializes in a number of areas such as Ransomware, Software-Defined Storage, Workload Management and Cloud environments. What makes them unique is that their solutions focus on information, not infrastructure. Their comprehensive approach to multi-cloud data management provides protection, availability and insight everywhere the client's information travels. These solutions include:

[Multi-Cloud](#)

[GDPR](#)

[Data Visibility](#)

[Data Protection](#)

[Data and Workload Portability](#)

[Storage Optimization](#)

[Business Continuity](#)

[Digital Compliance](#)

[Healthcare](#)

[Government](#)

[Education](#)

Their products are broken down into three areas:

[Availability](#) : [InfoScale](#) , [Resiliency Platform](#)

[Protection](#) : [NetBackup](#) , [NetBackup Appliances](#) , [Backup Exec](#) , [CloudPoint](#) , [SaaS Backup](#) , [Desktop and Laptop](#)

[Option](#) , [Access](#) , [Access Appliance](#) , [Flex Appliance](#) , [System Recovery](#) , [Predictive Insights](#)

[Insights](#) : [APTARE IT Analytics](#) , [Information Studio](#) , [Enterprise Vault](#) , [Enterprise Vault.cloud](#) , [eDiscovery Platform](#) ,

[Data Insight](#)

Zerto:

A world of uninterrupted technology is a world where organizations across all industries can thrive without downtime or disruptions for their customers. From 24/7 continuous patient care in hospitals, to interruption-free airline travel, to keeping ecommerce systems running without a hitch, the path to this always-available world starts with IT resilience. Zerto helps our 7000+ customers realize this vision through our IT Resilience Platform™, an all-in-one converged disaster recovery and backup platform that enables digital transformation, reduces downtime and data loss, and helps businesses move workloads seamlessly across clouds or datacenters. With Zerto, a world of truly uninterrupted technology is within reach.

Pinarilly, they offer one Platform for Disaster Recovery, Backup & Cloud Mobility. This 'all-in-one' IT Resilience Platform converges Disaster Recovery, Backup and Cloud Mobility in one simple, scalable solution. Zerto asserts that these attributes define their product:

- 1) Reduces cost and complexity of application migrations and data protection with Zerto's unique platform utilizing Continuous Data Protection.
- 2) Orchestration built into the platform enables full automation of recovery and migration processes.
- 3) Analytics that provide 24/7 infrastructure visibility and control, even across clouds.

Function	Category	Subcategory	Vendors
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	Cisco ISE, ForeScout, Pulse Secure, Solarwinds, Tanium, Service Now, Microfocus
		ID.AM-2: Software platforms and applications within the organization are inventoried	
		ID.AM-3: Organizational communication and data flows are mapped	
		ID.AM-4: External information systems are catalogued	
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1: The organization's role in the supply chain is identified and communicated	Exiger, Interos, Sayari
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	
		ID.BE-5: Resilience requirements to support delivery of critical services are established	
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established	ServiceNow, RSA Archer, RedSeal
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	
		ID.GV-4: Governance and risk management processes address cybersecurity risks	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	Flashpoint, Digital Shadows, Dark Owl, RedSeal, AttackIQ, Tenable, Recorded Future
ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources			
ID.RA-3: Threats, both internal and external, are identified and documented			
ID.RA-4: Potential business impacts and likelihoods are identified			
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk			
ID.RA-6: Risk responses are identified and prioritized			
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	Contrast, CheckMarx, MicroFocus Fortify	
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed		
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis		

<p>Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.</p>	<p>PR.AC-1: Identities and credentials are managed for authorized devices and users</p>	<p>Pulse Secure, Cisco Duo, SecureAuth, CyberArk, Thycotic, Centrify</p>
	<p>PR.AC-2: Physical access to assets is managed and protected</p>	
	<p>PR.AC-3: Remote access is managed</p>	
	<p>PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties</p>	
	<p>PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate</p>	
<p>Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>	<p>PR.AT-1: All users are informed and trained</p>	<p>Proofpoint, Cofense, KnowB4</p>
	<p>PR.AT-2: Privileged users understand roles & responsibilities</p>	
	<p>PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities</p>	
	<p>PR.AT-4: Senior executives understand roles & responsibilities</p>	
	<p>PR.AT-5: Physical and information security personnel understand roles & responsibilities</p>	
<p>Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.</p>	<p>PR.DS-1: Data-at-rest is protected</p>	<p>Broadcom (EDLP, Encryption), McAfee (EDLP, Encryption), Fidelis (NDLP), Titus, Thales</p>
	<p>PR.DS-2: Data-in-transit is protected</p>	
	<p>PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition</p>	
	<p>PR.DS-4: Adequate capacity to ensure availability is maintained</p>	

PROTECT (PR)

PR.DS-5: Protections against data leaks are implemented

PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity

PR.DS-7: The development and testing environment(s) are separate from the production environment

PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained

PR.IP-2: A System Development Life Cycle to manage systems is implemented

PR.IP-3: Configuration change control processes are in place

PR.IP-4: Backups of information are conducted, maintained, and tested periodically

Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met

PR.IP-6: Data is destroyed according to policy

PR.IP-7: Protection processes are continuously improved

PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties

PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

PR.IP-10: Response and recovery plans are tested

PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)

PR.IP-12: A vulnerability management plan is developed and implemented

Veritas, Cohesity, Solarwinds, MicroFocus, Veam, Zerto, Tenable, Tanium

Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools

PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

	<p>Protective Technology (PR,PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	<p>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</p>	<p>OPSWAT (removable media), Crowdstrike, McAfee EPP, Broadcom EPP, Carbon Black, Fireeye HX, Fireeye MVX, Juniper SRX, Palo Alto, Cisco, Infoblox</p>
		<p>PR.PT-2: Removable media is protected and its use restricted according to policy</p>	
		<p>PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality</p>	
		<p>PR.PT-4: Communications and control networks are protected</p>	

DETECT (DE)	<p>Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.</p>	<p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed</p>	<p>ExtraHop, Bricata, Cisco FirePower, Corelight, McAfee Network Security, F5, Palo Alto, Lookout. zScaler</p>
		<p>DE.AE-2: Detected events are analyzed to understand attack targets and methods</p>	
		<p>DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors</p>	
		<p>DE.AE-4: Impact of events is determined</p>	
		<p>DE.AE-5: Incident alert thresholds are established</p>	
	<p>Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.</p>	<p>DE.CM-1: The network is monitored to detect potential cybersecurity events</p>	<p>Splunk, Elastic, Fireeye Helix, Exabeam, Google Backstory, Analyst Platform, Crowdstrike, Carbon Black, Tenable, Gigamon, Trustwave</p>
		<p>DE.CM-2: The physical environment is monitored to detect potential cybersecurity events</p>	
		<p>DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events</p>	
		<p>DE.CM-4: Malicious code is detected</p>	
		<p>DE.CM-5: Unauthorized mobile code is detected</p>	
		<p>DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events</p>	
		<p>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed</p>	
		<p>DE.CM-8: Vulnerability scans are performed</p>	
	<p>Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events</p>	<p>DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability</p>	<p>Demisto, Swimlane, Phantom, Redhat Ansible</p>
		<p>DE.DP-2: Detection activities comply with all applicable requirements</p>	
<p>DE.DP-3: Detection processes are tested</p>			
<p>DE.DP-4: Event detection information is communicated to appropriate parties</p>			
<p>DE.DP-5: Detection processes are continuously improved</p>			

RESPOND (RS)	<p>Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.</p>	<p>RS.RP-1: Response plan is executed during or after an event</p>	
	<p>Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.</p>	<p>RS.CO-1: Personnel know their roles and order of operations when a response is needed</p>	<p>ServiceNow, Demisto, Phantom, Swimlane</p>
		<p>RS.CO-2: Events are reported consistent with established criteria</p>	
		<p>RS.CO-3: Information is shared consistent with response plans</p>	
		<p>RS.CO-4: Coordination with stakeholders occurs consistent with response plans</p>	
		<p>RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness</p>	
	<p>Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.</p>	<p>RS.AN-1: Notifications from detection systems are investigated</p>	<p>Demisto, Swimlane, Phantom, ServiceNow, Fireeye PX, ExtraHop,</p>
		<p>RS.AN-2: The impact of the incident is understood</p>	
		<p>RS.AN-3: Forensics are performed</p>	
		<p>RS.AN-4: Incidents are categorized consistent with response plans</p>	
	<p>Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.</p>	<p>RS.MI-1: Incidents are contained</p>	
		<p>RS.MI-2: Incidents are mitigated</p>	
		<p>RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks</p>	
<p>Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</p>	<p>RS.IM-1: Response plans incorporate lessons learned</p>		
	<p>RS.IM-2: Response strategies are updated</p>		

RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	
		RC.IM-2: Recovery strategies are updated	
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed	
		RC.CO-2: Reputation after an event is repaired	
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	

Tab 3: Performance Capability

1.0 Supplier Response (Section 3.0)

1.1 Company (Section 3.1)

A. Brief History and Description

ThunderCat Technology, LLC, is an ISO 9001:2015, Value Added Reseller (VAR) and Service-Disabled Veteran Owned Small Business (100% Combat-related Disability) with numerous industry awards and exceptional evaluations for Government contracts. In the IT industry, ThunderCat has won CRN Tech Elite 250 (seven times), INC5000 (five years in a row), Forbes Most Promising Small Businesses, Washington Technology Fast 50, Washington Technology Top 100, Solution Provider 500, CRN Fast Growth 100, Washington Business Journal 50 Fastest Growing Companies (also their #1 SDVOSB), SmartCEO GovStar Industry Small Business, SmartCEO Future 50, Ernst & Young Entrepreneur of the Award, VAR 500, DHS Small Business of the Year - 2016 and Best Places to work in Virginia (seven years in a row). As a testament to our success, ThunderCat has grown from \$28 million (2008) to \$694 million (2019), a 2,380% increase.

ThunderCat Technology, LLC is certified across multiple partners and the latest technologies impacting servers, storage, networking, virtualization, cloud and cyber security. It also means our engineers, sales managers and support staff are committed to excellence as evident in our total sales of \$1.77 billion across 7,334 Delivery Orders (DOs) over the last three years. In total, ThunderCat has sold \$3.7 billion in products and services over 14,400 total orders.

B Total Number and Location of Salespeople

ThunderCat Technology, LLC employs a total of 92 people, 40 of which are engaged in sales. These sales functions include: Face-to-face, Quote Generation or Solicitation response. These personnel cover and travel throughout the U.S. and visit their agencies overseas. Their home bases of operation include:

FL	MI	VA
IL	NJ	WA
MD	NY	

C. Number and Location of Support Centers

ThunderCat Technology, LLC is shopping for space to establish an integration center. ThunderCat has maintained ISO 9001 certification since 2012 and has expanded the Management System to incorporate Supply Chain Risk Management controls. ThunderCat's established SCRM system addresses requirements in both ISO 28000:2007 and ISO 20243:2018. An external audit will occur in August 2020 to achieve initial ISO 28000 certification. Following certification, ThunderCat will self-certify against ISO 20243. For the time being we provide the greatest possible discounts by 'drop shipping' directly from the OEMs. With over 100 OEMs in our portfolio, customer support is tailored between OEMs, Distributors and ourselves in order to tailor the ideal package to support customer requirements.

This document is proprietary and is intended solely for the use and information of the client to whom it is addressed.

"A Service-Disabled, Veteran-Owned Small Business"



D. Annual Sales for the Three Previous Fiscal Years

2017 - \$389 million

2018 - \$591 million

2019 - \$694 million

Da. FEIN and Dun & Bradstreet Report

Federal ID Number: 26-1638572

E. Green/Environmental Initiatives

Given our roots as a Federal Reseller, we procure equipment consistent with requirements for Energy Star® (e.g., large screens), Federal Energy Management Program (FEMP) and *Electronic Product Environmental Assessment Tool (EPEAT)* products (e.g., monitors).

F. Diversity Programs

ThunderCat Technology maintains relationships with over 100 businesses encompassing every size category. To keep Labor and Other Direct Costs (ODCs) such as travel low, ThunderCat has a ready network of Small Businesses to draw from. For larger-scale projects, we turn to Tribal-owned or Tribal-affiliated Small Disadvantaged Businesses (SDBs) given the number of employees, their Past Performance and ability to serve dispersed locations. As a result, they are in a better position to implement a region-wide or state-wide solution. For Woman-Owned Small Businesses (WOSBs), we have outreach to the Women's Business Enterprise National Council (WBENC). Their regional partnership organizations (<https://www.wbenc.org/regional-partner-organizations>) are especially critical in identifying WOSBs that are on the other side of the state yet within reasonable proximity to the Place of Performance. The network of Veteran Owned and Service Disabled Veteran Owned businesses are very well connected through the philanthropy of ThunderCat's CEO Tom Deierlein. HubZones are interesting because on more than one occasion we have pointed out the potential status to a small business partner that was not aware of the significance of their location. Another Small Business affiliation is the start-up. Many universities have IT start-up incubators so that new businesses can attract seed capital or start-up funding. Other university-led IT start-ups can cover down on multiple small business categories such as Historically Black Colleges and Universities (HBCU) and HubZone at the same time.

G. Certifications

ThunderCat Technology, LLC is certified by the Department of Veterans Affairs as a Service Disabled Veteran Owned Small Business. ThunderCat's record is found at the following search engine on the VA's website: <https://www.vip.vetbiz.va.gov/Home/>.



ThunderCat Technology, LLC

State:
Location: Reston Virginia
Last Verified: 6/5/2019
Expiration Date: 6/5/2022
D.B.A:
DUNS: 809887164
Phone: (703) 674-0216
Email: tom@thundercattech.com
Web: <http://www.thundercattech.com>

ThunderCat Technology, LLC has been vetted by the State Commerce Commission for eligibility as a Virginia Corporation and a Service Disabled Veteran Owned Small Business.

Business Type	Certification No	Certification Start Date	Certification End Date
✓ Small Business	723626	1/22/20	1/22/25
Service Disabled Veteran Owned	723626	1/22/20	1/22/25

H. Relationships with Subcontractors or Affiliates

The key factor that defines ThunderCat as a ‘World Class Small Business’ providing ‘World Class products’ is the relationships we maintain to support key customers buying through OMNIA. Leading ThunderCat is SLED Director Kent Stokley. Kent exercises the responsibility, accountability and authority for control and oversight of all functions necessary for successful performance on the OMNIA contract. Kent’s goal is to be responsive to the needs of the OMNIA customer by securing and maintaining productive, cost effective relationships with OEMs and service providers.

The processes for managing our supplier and subcontracting partners are driven by our ISO 9001:2015-registered Quality Management System (QMS). Our QMS dictates a review process where suppliers and partners are evaluated for:

- 1) Timely delivery of product
- 2) Accuracy of product shipped
- 3) Timely resolution of support issues
- 4) Technological relevancy
- 5) The long-term product viability of suppliers

Over the life of the contract, ThunderCat may secure additional Teaming Arrangements for the purpose of evaluating new vendors and products for OMNIA. Our participation in vendor advisory panels and participation in industry days and exhibitions helps broaden our industry expertise. By keeping in close contact with our partners, our understanding of the needs of the OMNIA customer at the enterprise level translates into the deepest possible discounting structures as well as Enterprise Licensing Agreements (ELA). We further monitor and improve our Teaming Arrangements by conducting:

- Information Sharing: Involving collecting, disseminating and analyzing information to better understand customer requirements.
- Relationship Building: Developing deeper supplier relationships based on mutual goals and common service levels.
- Using Proven Practices: Employing ISO 9001:2015-driven processes with a laser focus on maximum efficiency at all stages of delivery.

- **Systems Transparency:** Employing processes that are monitored for improvement and adjusted for the benefit of meeting and exceeding OMNIA customer expectations.

Systems transparency is achieved when ISO-driven management and quality processes are driven by an audited Customer Relationship Model (CRM) and Enterprise Resource Planning (ERP) solution. ThunderCat uses the former *Great Plains*, now known as Microsoft Dynamics GP. This capability allows us to flag Small Business partners so that payment turnaround time is greatly reduced. Orders requiring software products and billable work are processed in a timely manner pursuant to OMNIA Terms and Conditions, the Order and Teaming Agreement (TA). We run reconciliation reports for trend analysis purposes and make adjustments to our approach accordingly. A solid company in its own right, ThunderCat has never missed payments, resorted to reduced payments nor allowed Accounts Payable to slip. In the event of non-performance, adequate notification will be given to OMNIA, the OMNIA customer and the company in question.

Although ThunderCat Technology is a SWaM-certified Service Disabled Veteran Owned Small Business in its own right, we are equally conscientious of other enterprises, including. Minority Owned, Economically Disadvantaged Women Owned, those living in HubZones or on tribal lands. Also taken into consideration are the traditional Historically Black Colleges and Universities (HBCUs). Taking into consideration the type of relationship OMNIA has with communities across the country, we would advocate a Commercial Small Business Plan. This way, companies on OMNIA would be able to incorporate other Small Business enterprises into an expanded customer base. The reason this makes more sense is because it opens the possibility of mapping skills to requirements outside the scope of a specific order to other customers.

I. Differentiating Suppliers from Competitors

As an impartial advocate for the OMNIA customer, we have occasionally had to choose between our relationship with the customer and with potential partners. The reason that choosing the customer became the better strategy is because over time relationships and trust develops. More often than not we are solicited for our opinions in areas such as mitigation, infrastructure improvements and longer term IT investments. Given this unique position, we are often approached by the OEMs and given competitive pricing. In situations where we approach to OEM, we

J. Past Litigation, Bankruptcy and Reorganization

Last year, two partners sued each other. ThunderCat was not named as a Plaintiff. We responded to a court order to surrender communications during the discovery process which we complied with.

K. Felony Conviction Notice

On Sept 9, 2015, an employee pled guilty to one count of conspiracy to commit wire fraud and major government fraud. The underlying conduct related to certain ‘third bid,’ or courtesy bid practices, as well as wrongdoing associated with a Sept 2009 sale (more than 10 years ago). He resigned prior to plea. He was never suspended nor debarred. He returned the company in 2017 after full review and approval of the Suspension and Debarment Official (SDO) with oversight on the case. This individual is not involved in this sale or any public sector sales, commercial only.

L. Debarment or Suspensions

N/A

1.2 Distribution & Logistics (Section 3.2)

A. Description of Full Line of Products and Services

The following list depicts ThunderCat’s current Line Card of Storage, Software, Cloud and Cybersecurity products:

2019/2020 Line Card

A10 Networks	Bricata, Inc.	Dataram
Accellion, Inc.	BriefCam	Decipher Technology Studios
Acquia	Broadcom	Decision Lens
AddOn Networks	Bugcrowd, Inc.	DefendX
Adobe	Cables to Go	Dell
Advanced HPC	Calabrio	Digi-Trax
Ains	Canon	Digital Guardian
Allied Telesis	Canon Solutions America, Inc.	Digital Shadows
Alteryx	Carbon Black	DocuSign
Amazon Web Services	CaseWare International	Docutrend
Anaconda, Inc.	CCX	Druva
Analyst Platform, LLC	Centrify Corporation	Dtex Systems
APC	Chatsworth	Duo Beyond
Apcon	Checkpoint	Eaton
App Dynamics	Cinemassive	Eizo
Appian	Cisco	Ekahau
Apple	Citrix	Elastic
Applied Data System	Clearwell Systems, Inc.	Elemental
Appspace	Cloudbees	EMC
Arista Networks Inc	Cloudera	ENDRUN TECHNOLOGIES LLC
Arris	CloudTamer	Enterprise Vision
Aruba Networks	Cofense	ePLUS
Asure Software	Cohesity	Ergotron
Aternity	CommScope	Everbridge
Atlassian Pty Ltd	Commvault	Extra Hop
AttackIQ	ComponentSource	Extreme Networks
Autodesk	Concurrent Real-Time, Inc.	F5
AvePoint	Corning	Fidelis
AVI-SPL	Corterix	FireEye
Avocent	Cray	Firemon
Babel Street	Creative Radicals	Fivecast
Barco	Crenlo	Flashpoint
Bassec	Crestron	FM Systems
BeyondTrust Corporation	Crossmatch	ForeScout Technologies, Inc
Big Switch Networks	Crowdstrike	Forgerock
Blackberry	Crystal	Fujitsu
Blue Jeans	Cyber-Ark	Gemalto
Blue Medora	Cylance	GetWellNetwork Inc
BlueCoat	Data Distributing	Gigamon
BorderLAN, Inc	Datacard	Gitlab
Box, Inc.	DataDirect Networks	GlideFast
GLOBALSCAPE	MicroStrategy	Pure Storage

This document is proprietary and is intended solely for the use and information of the client to whom it is addressed.

“A Service-Disabled, Veteran-Owned Small Business”

Google	MIST	Qlik
GoToAssist	Mobatek	QLogic
Granicus	MobileIron	QStar
Haivision	Morpheus	Qualys, Inc.
Harness, Inc.	Nagios	Quantum
Hewlett Packard	Napatech	Quantum Secure
Hitachi	NCipher	Quest
Hitachi Healthcare	NEC	QUIKTRON
IBM-New	NetAPP	Qumulo
Idera, Inc.	NetBrain	Radiant Logic
InfoBlox	NetScout	Raritan
Informatica	NetSource	RealVNC
Integrated Biometrics	Nexsan	Recorded Futures
Intel	Nintex	Red Canary
Intelligent InSites	NLYTE	Red Hat
Interos Inc	Ntrepid	Red River Services
IVANTI	Nuance	RedSeal
Ixia	Nutanix	RightStar, Inc.
Juniper	Nvidia	Rimage
Kingston	ObservIT, Inc	Riverbed
KLAS Telecom	Olympus	RSA
Kofax	Omnitron	Rubrik
Legrand, SA	Onyx	SafeNet
Lenovo	OPSWAT	Salesforce
Linksys	Origin High Performance PC	Samsung
LMG Security	Ortronics, Inc.	Sandisk
LogiTech	Palo Alto	SAP
LogRhythm, Inc	Panasonic	Sayari
Lookingglass	Pandora FMS	Sc2 Corp
Lookout	Panduit	Scott-Clark
Mark Logic	Pelican	Seagate
Markforged	Pentaho	SecureWorks, Inc
McAfee	Pentax	Security Compass
Media Platform	Pershing	Service Now
MediaPro	Phalanx Security	SevOne
MediaStar	Pivotal	SITSCAPE
Mediware	Polaris	Socrata
Mellanox	Practical Code, LLC	Solar Winds
Micro Focus	Proline	Solarwinds
Microchip	Proofpoint	Sole Source Technolc
Microsemi	Pulse Secure	Son Technology
Microsoft	Puppet	Sonatype
Sonicwall	Virtru Corporation	

Sonitor	VirusTotal
Sonus	Vitec
Spectra Logic	VMware
Splunk	VQ Communications
Sprinklr	Western Digital
Stanley Convergent Security Solutions	Wind River Sales Co., Inc.
Startech.com	Windward
Steelhead	Xmedius
Symantec	York Telecom Corporation
Syncsort	You Test Me
Tableau	Zerto
Tangent	Zovy
Tanium	Zscaler
Tasktop	
Tenable	
Thales	
Thomson Reuters - Special Services	
Threadfix	
TIBCO Software	
Topaz Systems	
Towerstream Corporation	
Transition Networks	
Trend Micro	
TRENDnet INC	
Tripplite	
Tripwire	
Trustwave	
Tufin Technologies	
Twilio Inc.	
Twistlock	
UiPath	
Valor Construction, LLC	
Variphy	
Varonis	
VBrick	
Veeam	
Velocity Micro	
Veracode	
Veritas	
Viavi	
Vidyo	
Vigilant Solutions	

B. Proposed Distribution

ThunderCat maintains relationships with multiple distributors that service all 50 states.



Section D/E details examples of partner companies, their location and their facility size.

C. Auditing Value Chain Pricing

As evident by the 7,334 total orders processed during the last three years, ThunderCat's CRM is able to track value chain fluctuations or pricing anomalies within the pricing structure at a near-instantaneous level. All order receipts, notifications and updates will be recorded in the CRM by date and time (and later submitted as part of the Monthly Activity Report's Performance Log). What is key here is that we can establish a metric to alert us of a price fluctuation greater than 2-4% for example. The generated report will be structured to include: Contractor order number, customer order number, summary of items ordered and total amount of the order. These customer details will also be included in the Monthly Financial Report.

D/E Partner Companies & Description of Distribution Facilities

ThunderCat has outgrown its integration facility in Reston, VA. Pending our move to a new facility (10,000 sq. ft.) near the Washington-Dulles Airport, we are currently renting a secured space in Sterling, VA. In addition, ThunderCat has reachback facilities offered through various partners throughout the United States. Not including OEM facilities such as Dell in Round Rock, TX (226,000 sq. ft.), distributors such as Arrow Electronics (Syracuse, NY – 33,663 sq. ft. and Phoenix, AZ – 212,000 sq. ft.), Tech Data (Fontana, CA and Swedesboro, NJ – 435,000 total sq. ft. each) and Synnex (Greenville, SC – 110,000 sq. ft.) operate ISO-certified integration and distribution centers.



ThunderCat has maintained ISO 9001 certification since 2012 and has expanded the Management System to incorporate Supply Chain Risk Management controls. ThunderCat's established SCRM system addresses requirements in both ISO 28000:2007 and ISO 20243:2018. An external audit will occur in August 2020 to achieve initial ISO 28000 certification. Following certification, ThunderCat will self-certify against ISO 20243

1.3 Marketing and Sales (Section 3.3)

A. 90-Day Plan for 'Go-to-Market' Strategy

Tradeshows – ThunderCat will be present at tradeshows centered around OMNIA partners/target agencies. Our SLED one-pagers will hold the OMNIA contract info & logo on them to be distributed at these shows. During this initial 90 days, ThunderCat will schedule displays at five tradeshows during the year to specifically promote OMNIA.

Press Release – Upon award, a press release will be sent through ThunderCat’s Press Release (PR) web distribution center and pushed through social media sites: Twitter, LinkedIn, and Facebook. PR will state contract award info, link to OMNIA’s site, and POC through ThunderCat.

SEO Campaign (Search Engine Optimization) – ThunderCat will implement an SEO campaign to increase the quantity and quality of traffic to our website through organic search engine results. Specifically using keywords associated with the OMNIA contract, ThunderCat will also target particular state, local, and educational institutions.

Re-targeting Ad Campaign – Ads promoting the OMNIA contract will be pushed through a LinkedIn re-targeting ad campaign. This will help capture user demographics and organic traffic to our site.

Website branding – OMNIA logo will be added to the corporate webpage & listed under our SLED contracts page. <https://www.thundercattech.com/contract-vehicles/sled-contracts>.

Kick-off & Sales Training – Within the first seven days of award, a kick-off meeting will be conducted to integrate the sales force, corporate executives and the operations staff. The purpose of this meeting is to equip and empower the sales force with the tools necessary to promote OMNIA. This includes an overview of the OMNIA Master Agreement, how to coordinate use of the vehicle, the SLED one-pagers and use of the tradeshow display banner. In order to maximize the greatest number of leads, a target list will delineate specific responsibilities. This prevents waste and redundancy while at the same time expand ThunderCat’s participation in OMNIA the quickest way possible.

B. 90-Day Plan for ‘Market-the-Master-Agreement’ Strategy

The 90-Day ‘Master the Market’ Strategy is detailed as follows:

Day	Action	Lead	Comments
D-Day	Notification	SLED	Alert Executives, Contracts, PMO, Sales, Marketing and Support Staff
D+1	Master Agreement Signed & Exchanged	Contracts	
	Schedule Kick-off	PMO	Executives, Sales, Marketing and Support Staff
D+2	Toll Free Number/OMNIA Email	IT	Lead Notification
D+3	Co-branded Press Release, SEO	Marketing	Mass push of new Logo

Day	Action	Lead	Comments
	optimization, Website update		
D+5	Kickoff Meeting	SLED/PMO	Executives, Sales, Marketing and Support Staff
D+7	Call Plan & One- pagers sent to Customer Base	SLED	Promote OMNIA
D+8	Press Release	Marketing	
	SEO Campaign		
	Website Branding		
D+10	Synchronization Meeting	SLED/Marketing	<ul style="list-style-type: none"> • Triangulate Trade Show, Summit and Conference Participation • Notification of Target Customers • Travel for Next 180 Days
	Submit Marketing Materials to OMNIA	Marketing	Permission for reproduction
D+13	Co-Branded Marketing Materials	Marketing	Submit to Graphics Company Trade Show Banner Design and Handouts for Mass Production
D+13 to D+30	Coordinate Trade Show, Summit and Conference Participation	SLED	
D+18	Provide Final List to Marketing	SLED	
D+20	Discuss Trade Publication Advertisement with OMNIA	Marketing	
	Inspect/Accept Co-Branded Materials	Marketing	
D+30 To D+45	Event 1	SLED/Marketing	
D+60 To D+90	Event 2	SLED Sales	
D+90	Meeting with OMNIA	SLED Director	<ul style="list-style-type: none"> • Exchange of Information • Progress Report

C. Transition Strategy of Existing Public Agency Customers to the Master Agreement

There are three ways to promote OMNIA with existing customers:

- The announcement: We already have a target list of who stands the most to benefit from the OMNIA vehicle. Most if not all, are already familiar with OMNIA
- The face-to-face meeting: We schedule meetings with existing customers to gauge future projects and interests. This is where they receive directly from us the attributes and advantages of the new contract vehicle: 1) Pre-solicited and awarded, 2) Best public sector pricing, 3) No cost to participate and 4) Non-exclusive.
- The follow-up: This is where we notify customers that we will be at an event and maintain a booth. For those not already planning to attend, this provides an impulse decision to break away from the office for a couple of days.

D. Promoting OMNIA Logo

The OMNIA logo will become part of the SLED Team's public image. We use logos in our emails, proposal responses, website and handouts. Our goal during the first year is to establish ourselves as fast-rising 'brand ambassadors' in the national SLED public sector arena.

E. Proactive Direct Sales

In addition to use of the logo, we steer potential customers to OMNIA by touting the same attributes mentioned earlier in Section C, i.e., Pre-solicited and awarded, Best Pricing, No participation cost and non-exclusive. ThunderCat however, envisions a 360-degree concept of proactivity where execution and follow-up assures flawless customer service and repeat sales. In accordance with the Terms and Conditions shared with the customer, orders and inquiries will be responded to within a specified timeframe. For example direct orders through OMNIA will be acknowledged and settled by the SLED Customer Service Manager via e-mail, with a copy of the order within four business-hours of order acceptance. All manual or complex orders will be acknowledged and accepted within the four-day window. On-line orders made via an OMNIA or customer-specified portal are acknowledged the same way. Requests for Technical Submissions (in addition to quotes) are conducted using a 'backward-planning' methodology; with our goal is to submit the day before. Depending on Lead Time, there are either two formal and one informal final reviews or an informal initial session followed by a formal and a final. There is also a review and kickoff involving the cross competencies of ThunderCat which include but are not limited to: Contracts, Engineers and Architects, Finance, Program Management Office under SLED and Executive oversight. The conduct of coordinating a customer response is tracked within our ISO for coherence and effectiveness twice a year. To make a customer relationship work within the OMNIA contracting model, the vehicle is as much conducive to relationship building as it is a means of transaction.

F. Training National Sales Force on Master Agreement

No one will be able to close business on the OMNIA vehicle without the proper training and certification by the SLED Director. Any new sales personnel after the kick-off (Section A) will demonstrate a knowledge of the Master Agreement, its terms and conditions as a condition of their in-processing at ThunderCat. This onboarding process will add the available public agencies currently serviced by ThunderCat as well as the ‘low hanging fruit’ that needs engagement. Follow-on training updates will be given monthly following the monthly sales meeting which is conducted via video-teleconference.

G. Name/Title/Email/Phone for Key People

Title	Name	Email	Phone
Chief Operating Officer	David Schlosser	dschlosser@thundercattech.com	(703) 674-0247
Marketing Officer	Megan Battaglia	mbattaglia@thundercatech.com	(703) 674-0229
SLED Sales Director	Kent Stokely	kstokely@thundercattech.com	(703) 568-3378
Director of Operations	Kevin Sieve	ksieve@thundercattech.com	(703) 674-0267
Chief Financial Officer	Matt Smith	msmith@thundercattech.com	(703) 674-0248
Director Financial Operations	Cristin Cowan	ccowan@thundercattech.com	(703) 674-0243
Contracts Manager	Jean Kim	jkim@thundercattech.com	(301) 996-0140

H. Structure of National Sales Force

The Chief Operating Officer of ThunderCat Technology is David Schlosser, (703) 674-0247 or dschlosser@thundercattech.com. Although ThunderCat is geographically centered in the DC Metro area, its reach is truly national. In the Figure below, the geographic location is deceptive given the amount of travel and video-conferencing that takes place. For example, two members of our Health Sales Team crisscross across the country, accumulating over \$150 million in sales over a two-year period. For the sake of clarity, the term ‘Generic’ is used to accurately convey their location although internally we often associate them individually with their biggest customer. All sales personnel, regardless of location can be brought to bear to explore and expand OMNIA’s customer base. Almost half of ThunderCat is engaged in the sales function at any given time.

Area	Locations	Scope
------	-----------	-------

*Collaborative Practice includes Audio-Visual, Conferencing, Mobile and other telephony

I. Strategy to Grow and Implement the National Program

This is why the ‘D+90’ meeting with OMNIA mentioned in Section B is critical. It would be a waste of time to project a full year out being new to the vehicle. Real-world events such as that going on at the time of this submission requires us to be vigilant and flexible to the changing needs of the public customer at any given time. This also applies to the OMNIA vehicle itself. One way to become a national brand under the OMNIA banner is to intercede when others are not meeting expectations. In our ecosystem, reputation is everything. Being able to solve hard problems is what grew us to the levels that we are at in such a short amount of time. We are certain that we will expand our loyal following by doing the same thing for OMNIA.

J. Public Agency Sales and Largest Customer

ThunderCat Technology, LLC has only branched into State, Local and Educational (SLED) institutions in the last two years. For the sake of accuracy we are providing three tables: ‘Top 10’ Federal Agencies – Fiscal Year 2019, ‘Top 10’ Federal Sales – Fiscal Year 2019, Top SLED Agencies – Fiscal Year 2019 and Top SLED Sales – Fiscal Year 2019.

‘Top 10’ Federal Agencies - Fiscal Year 2019

Agency	Amt
--------	-----



*Sales cut across Fiscal Years and vary by Period of Performance
Also See Tab 5 – Value Add for Top Cybersecurity Deliveries*

K. Information Systems Capabilities and Limitations

ThunderCat's CRM is able to track value receipts, notifications and updates by date and time. Reporting will be structured into a spreadsheet that includes: Contractor order number, customer order number, summary of items ordered, total amount of the order as well as statuses by date and time.

Routine shipments will take less than 10 days 90% of the time unless waived by the ordering official. Shipments for these type of orders utilize the standard configuration contract line items and do not require any variations. Shipment for complex orders will be accomplished less than 20 days 90% of the time and noted in the Delivery Report's comment section as a 'complex order.' All shipments are tracked internally which the Internal Sales Team continuously monitors in order to keep the OMNIA customer fully informed. All shipping dates and times, regardless of order size, are generated automatically and itemized in the Delivery Report.

L. Sales Commitment

N/A per our Master Agreement with OMNIA Partners, Public Sector

M. Detail Strategies When Confronted with Agency-generated Proposals

ThunderCat Technology, LLC is only interested in responding to SLED solicitations through OMNIA. To check every individual local portal for sales defeats the whole purpose of the vehicle. If confronted with an extraneous opportunity, we will ask the customer why the OMNIA vehicle is not ideal for these requirements. This way, we operate in full transparency with customers and partners alike. We cannot offer the same OEM 'deal-registered' pricing as OMNIA because the contract vehicle is modelled for much higher volume.

Tab 4: Qualification and Experience

Tab 4: Qualification and Experience**Overview**

ThunderCat Technology, LLC, is an ISO 9001:2015, Value Added Reseller (VAR) and Service-Disabled Veteran Owned Small Business (100% Combat-related Disability) with numerous industry awards and exceptional evaluations for Government contracts. In the IT industry, ThunderCat has won CRN Tech Elite 250 (seven times), INC5000 (five years in a row), Forbes Most Promising Small Businesses, Washington Technology Fast 50, Washington Technology Top 100, Solution Provider 500, CRN Fast Growth 100, Washington Business Journal 50 Fastest Growing Companies (also their #1 SDVOSB), SmartCEO GovStar Industry Small Business, SmartCEO Future 50, Ernst & Young Entrepreneur of the Award, VAR 500, DHS Small Business of the Year - 2016 and Best Places to work in Virginia (seven years in a row). As a testament to our success, ThunderCat has grown from \$28 million (2008) to \$694 million (2019), a 2,380% increase.

ThunderCat Technology, LLC is certified across multiple partners and the latest technologies impacting servers, storage, networking, virtualization, cloud and cyber security. It also means our engineers, sales managers and support staff are committed to excellence as evident in our total sales of \$1.77 billion across 7,334 Delivery Orders (DOs) over the last three years. In total, ThunderCat has sold \$3.7 billion in products and services over 14,400 total orders.

Future Qualifications Include Supply Chain Certification and an Integrated Support Center

ThunderCat Technology, LLC does not maintain a support center. Instead we provide the greatest possible discounts by 'drop shipping' directly from the OEMs. With over 100 OEMs in our portfolio, customer support is tailored between OEMs, Distributors and ourselves in order to tailor the ideal package to support customer requirements.

ThunderCat's established SCRM system addresses requirements in both ISO 28000:2007 and ISO 20243:2018. An external audit will occur in August 2020 to achieve initial ISO 28000 certification. Following certification, ThunderCat will self-certify against ISO 20243. For the time being we provide the greatest possible discounts by 'drop shipping' directly from the OEMs. With over 100 OEMs in our portfolio, customer support is tailored between OEMs, Distributors and ourselves in order to tailor the ideal package to support customer requirements.

ThunderCat's Current Line Card

2019/2020 Line Card

A10 Networks	Bricata, Inc.	Dataram
Accellion, Inc.	BriefCam	Decipher Technology Studios
Acquia	Broadcom	Decision Lens
AddOn Networks	Bugcrowd, Inc.	DefendX
Adobe	Cables to Go	Dell
Advanced HPC	Calabrio	Digi-Trax
Ains	Canon	Digital Guardian
Allied Telesis	Canon Solutions America, Inc.	Digital Shadows
Alteryx	Carbon Black	DocuSign
Amazon Web Services	CaseWare International	Docutrend
Anaconda, Inc.	CCX	Druva
Analyst Platform, LLC	Centrify Corporation	Dtex Systems
APC	Chatsworth	Duo Beyond
Apcon	Checkpoint	Eaton
App Dynamics	Cinemassive	Eizo
Appian	Cisco	Ekahau
Apple	Citrix	Elastic
Applied Data System	Clearwell Systems, Inc.	Elemental
Appspace	Cloudbees	EMC
Arista Networks Inc	Cloudera	ENDRUN TECHNOLOGIES LLC
Arris	CloudTamer	Enterprise Vision
Aruba Networks	Cofense	ePLUS
Asure Software	Cohesity	Ergotron
Aternity	CommScope	Everbridge
Atlassian Pty Ltd	Commvault	Extra Hop
AttackIQ	ComponentSource	Extreme Networks
Autodesk	Concurrent Real-Time, Inc.	F5
AvePoint	Corning	Fidelis
AVI-SPL	Cortecix	FireEye
Avocent	Cray	Firemon
Babel Street	Creative Radicals	Fivecast
Barco	Crenlo	Flashpoint
Bassec	Crestron	FM Systems
BeyondTrust Corporation	Crossmatch	ForeScout Technologies, Inc
Big Switch Networks	Crowdstrike	Forgerock
Blackberry	Crystal	Fujitsu
Blue Jeans	Cyber-Ark	Gemalto
Blue Medora	Cylance	GetWellNetwork Inc
BlueCoat	Data Distributing	Gigamon
BorderLAN, Inc	Datacard	Gitlab
Box, Inc.	DataDirect Networks	GlideFast
GLOBALSCAPE	MicroStrategy	Pure Storage

Google	MIST	Qlik
GoToAssist	Mobatek	QLogic
Granicus	MobileIron	QStar
Haivision	Morpheus	Qualys, Inc.
Harness, Inc.	Nagios	Quantum
Hewlett Packard	Napatech	Quantum Secure
Hitachi	NCipher	Quest
Hitachi Healthcare	NEC	QUIKTRON
IBM-New	NetAPP	Qumulo
Idera, Inc.	NetBrain	Radiant Logic
InfoBlox	NetScout	Raritan
Informatica	NetSource	RealVNC
Integrated Biometrics	Nexsan	Recorded Futures
Intel	Nintex	Red Canary
Intelligent InSites	NLYTE	Red Hat
Interos Inc	Ntrepid	Red River Services
IVANTI	Nuance	RedSeal
Ixia	Nutanix	RightStar, Inc.
Juniper	Nvidia	Rimage
Kingston	ObservIT, Inc	Riverbed
KLAS Telecom	Olympus	RSA
Kofax	Omnitron	Rubrik
Legrand, SA	Onyx	SafeNet
Lenovo	OPSWAT	Salesforce
Linksys	Origin High Performance PC	Samsung
LMG Security	Ortronics, Inc.	Sandisk
LogiTech	Palo Alto	SAP
LogRhythm, Inc	Panasonic	Sayari
Lookingglass	Pandora FMS	Sc2 Corp
Lookout	Panduit	Scott-Clark
Mark Logic	Pelican	Seagate
Markforged	Pentaho	SecureWorks, Inc
McAfee	Pentax	Security Compass
Media Platform	Pershing	Service Now
MediaPro	Phalanx Security	SevOne
MediaStar	Pivotal	SITSCAPE
Mediware	Polaris	Socrata
Mellanox	Practical Code, LLC	Solar Winds
Micro Focus	Proline	Solarwinds
Microchip	Proofpoint	Sole Source Technolc
Microsemi	Pulse Secure	Son Technology
Microsoft	Puppet	Sonatype
Sonicwall	Virtru Corporation	

Sonitor	VirusTotal
Sonus	Vitec
Spectra Logic	VMware
Splunk	VQ Communications
Sprinklr	Western Digital
Stanley Convergent Security Solutions	Wind River Sales Co., Inc.
Startech.com	Windward
Steelhead	Xmedius
Symantec	York Telecom Corporation
Syncsort	You Test Me
Tableau	Zerto
Tangent	Zovy
Tanium	Zscaler
Tasktop	
Tenable	
Thales	
Thomson Reuters - Special Services	
Threadfix	
TIBCO Software	
Topaz Systems	
Towerstream Corporation	
Transition Networks	
Trend Micro	
TRENDnet INC	
Tripplite	
Tripwire	
Trustwave	
Tufin Technologies	
Twilio Inc.	
Twistlock	
UiPath	
Valor Construction, LLC	
Variphy	
Varonis	
VBrick	
Veeam	
Velocity Micro	
Veracode	
Veritas	
Viavi	
Vidyo	
Vigilant Solutions	

Tab 5: Value Add

**Tab 5: Value Add
Performance Ratings**

In the Federal procurement system, evaluations are called **Contractor's Performance Assessment Report** or 'CPAR' A CPAR assesses a contractor's performance and provides a record, both positive and negative, on a given contractor during a specific period of time. Each assessment is based on objective facts and supported by program and contract management data, such as cost performance reports, customer comments, quality reviews, technical interchange meetings, financial solvency assessments, construction/production management reviews, contractor operations reviews, functional performance evaluations, and earned contract incentives.

Date Range: January 2019 – December 2019

Size Sample: Total of 201 CPARs received

Results: 201 Received Satisfactory or higher ratings

100% Satisfaction rate across all government agencies and contracts

Graded Criteria on every CPAR

Quality: 100% Satisfactory or higher ratings

Schedule: 100% Satisfactory or higher ratings

Cost Control: 100% Satisfactory or higher ratings

Management: 100% Satisfactory or higher ratings

Small Business Subcontracting: 100% Satisfactory or higher ratings

Regulatory Compliance: 100% Satisfactory or higher ratings

Cyber OEM Certifications

The following breaks down our top OEMs by certification status. As a seven-year award winner of the CRN Tech Elite 250, ThunderCat personnel are consistently enrolled in OEM certification programs for the products we sell. In many cases our certification level pays off by realizing the best discounts available on the market. In 'Brand Name or Equal' scenarios, we engage competitors to gauge their seriousness in providing hard discounts in order to capture a relationship with a strategic client. This is because an established relationship during a contract's period of performance ranges on average between three to five years. In other instances, we fill in for the OEM in order to provide the quickest response time. The significance of this is because OEMs usually offer heavily discounted services with their product offerings. OEMs do not readily grant companies permission to perform in their stead unless they are extremely confident in the company. ThunderCat Technology enjoys such a role. In Tab 3, we listed the top 50 cybersecurity companies we support by reselling. Of the 50, here are the ones we have an extensive relationship with:

OEM	Status	OEM	Status



Some OEMs do not have certification programs while others are extensive. In more than one instance, the OEM certification encompasses areas in parallel with cybersecurity such as storage, unified communications and operating system software amongst others.

Cybersecurity Specializations

To have the type of cybersecurity support offered by ThunderCat, you have to have a dedicated team of experts able to solve real problems facing public sector customers today. Of the 64 cybersecurity deliveries over \$1 million during the last three years, here are the 10 largest:

Tab 6: Additional Required Documents
(Appendix C)

Appendix C
ADDITIONAL REQUIRED DOCUMENTS

- DOC #1 Acknowledgment and Acceptance of Region 4 ESC's Open Records Policy
- DOC #2 Antitrust Certification Statements (Tex. Government Code § 2155.005)
- DOC #3 Implementation of House Bill 1295 Certificate of Interested Parties (Form 1295)
- DOC #4 Texas Government Code 2270 Verification Form

Appendix C, Doc #1

ACKNOWLEDGMENT AND ACCEPTANCE
OF REGION 4 ESC's OPEN RECORDS POLICY

OPEN RECORDS POLICY

All proposals, information and documents submitted are subject to the Public Information Act requirements governed by the State of Texas once a Contract(s) is executed. If an Offeror believes its response, or parts of its response, may be exempted from disclosure, the Offeror must specify page-by-page and line-by-line the parts of the response, which it believes, are exempt and include detailed reasons to substantiate the exemption. Price is not confidential and will not be withheld. Any unmarked information will be considered public information and released, if requested under the Public Information Act.

The determination of whether information is confidential and not subject to disclosure is the duty of the Office of Attorney General (OAG). Region 4 ESC must provide the OAG sufficient information to render an opinion and therefore, vague and general claims to confidentiality by the Offeror are not acceptable. Region 4 ESC must comply with the opinions of the OAG. Region 4 ESC assumes no responsibility for asserting legal arguments on behalf of any Offeror. Offeror is advised to consult with their legal counsel concerning disclosure issues resulting from this procurement process and to take precautions to safeguard trade secrets and other proprietary information.

Signature below certifies complete acceptance of Region 4 ESC's Open Records Policy, except as noted below (additional pages may be attached, if necessary).


Check one of the following responses to the Acknowledgment and Acceptance of Region 4 ESC's Open Records Policy below:

- We acknowledge Region 4 ESC's Open Records Policy and declare that no information submitted with this proposal, or any part of our proposal, is exempt from disclosure under the Public Information Act.
- We declare the following information to be a trade secret or proprietary and exempt from disclosure under the Public Information Act.

(Note: Offeror must specify page-by-page and line-by-line the parts of the response, which it believes, are exempt. In addition, Offeror must include detailed reasons to substantiate the exemption(s). Price is not confident and will not be withheld. All information believed to be a trade secret or proprietary must be listed. It is further understood that failure to identify such information, in strict accordance with the instructions, will result in that information being considered public information and released, if requested under the Public Information Act.)

4/9/2020

 Date


 Contracts

 Authorized Signature & Title

ANTITRUST CERTIFICATION STATEMENTS
(Tex. Government Code § 2155.005)
Attorney General Form

I affirm under penalty of perjury of the laws of the State of Texas that:

1. I am duly authorized to execute this Contract on my own behalf or on behalf of the company, corporation, firm, partnership or individual (Company) listed below;
2. In connection with this proposal, neither I nor any representative of the Company has violated any provision of the Texas Free Enterprise and Antitrust Act, Tex. Bus. & Comm. Code Chapter 15;
3. In connection with this proposal, neither I nor any representative of the Company has violated any federal antitrust law; and
4. Neither I nor any representative of the Company has directly or indirectly communicated any of the contents of this proposal to a competitor of the Company or any other company, corporation, firm, partnership or individual engaged in the same line of business as the Company.

Company	Contact	
<u>ThunderCat Technology, LLC</u>		Signature
_____		Jean Kim
		Printed Name
Address	Official Authorizing Proposal	Position with Company
<u>1925 Isaac Newton Square, Suite 180</u>		Contracts
<u>Reston, VA 20190</u>		_____
		Signature

		Printed Name
Phone		_____
		Position with Company
Fax		_____

Implementation of House Bill 1295**Certificate of Interested Parties (Form 1295):**

In 2015, the Texas Legislature adopted House Bill 1295, which added section 2252.908 of the Government Code. The law states that a governmental entity or state agency may not enter into certain contracts with a business entity unless the business entity submits a disclosure of interested parties to the governmental entity or state agency at the time the business entity submits the signed contract to the governmental entity or state agency. The law applies only to a contract of a governmental entity or state agency that either (1) requires an action or vote by the governing body of the entity or agency before the contract may be signed or (2) has a value of at least \$1 million. The disclosure requirement applies to a contract entered into on or after January 1, 2016.

The Texas Ethics Commission was required to adopt rules necessary to implement that law, prescribe the disclosure of interested parties form, and post a copy of the form on the commission's website. The commission adopted the Certificate of Interested Parties form (Form 1295) on October 5, 2015. The commission also adopted new rules (Chapter 46) on November 30, 2015, to implement the law. The commission does not have any additional authority to enforce or interpret House Bill 1295.

Filing Process:

Starting on January 1, 2016, the commission made available on its website a new filing application that must be used to file Form 1295. A business entity must use the application to enter the required information on Form 1295 and print a copy of the completed form, which will include a certification of filing that will contain a unique certification number. An authorized agent of the business entity must sign the printed copy of the form. The completed Form 1295 with the certification of filing must be filed with the governmental body or state agency with which the business entity is entering into the contract.

The governmental entity or state agency must notify the commission, using the commission's filing application, of the receipt of the filed Form 1295 with the certification of filing not later than the 30th day after the date the contract binds all parties to the contract. This process is known as acknowledging the certificate. The commission will post the acknowledged Form 1295 to its website within seven business days after receiving notice from the governmental entity or state agency. The posted acknowledged form does not contain the declaration of signature information provided by the business.

A certificate will stay in the pending state until it is acknowledged by the governmental agency. Only acknowledged certificates are posted to the commission's website.

Electronic Filing Application: https://www.ethics.state.tx.us/whatsnew/elf_info_form1295.htm

Frequently Asked Questions:

https://www.ethics.state.tx.us/resources/FAQs/FAQ_Form1295.php

Changes to Form 1295: <https://www.ethics.state.tx.us/data/filinginfo/1295Changes.pdf>

Texas Government Code 2270 Verification Form

House Bill 89 (85R Legislative Session), which adds Chapter 2270 to the Texas Government Code, provides that a governmental entity may not enter into a contract with a company without verification that the contracting vendor does not and will not boycott Israel during the term of the contract.

Furthermore, Senate Bill 252 (85R Legislative Session), which amends Chapter 2252 of the Texas Government Code to add Subchapter F, prohibits contracting with a company engaged in business with Iran, Sudan or a foreign terrorist organization identified on a list prepared by the Texas Comptroller.

I, Jean Kim, as an authorized representative of

ThunderCat Technology, LLC, a contractor engaged by


Insert Name of Company

Region 4 Education Service Center, 7145 West Tidwell Road, Houston, TX 77092, verify by this writing that the above-named company affirms that it (1) does not boycott Israel; and (2) will not boycott Israel during the term of this contract, or any contract with the above-named Texas governmental entity in the future.

Also, our company is not listed on and we do not do business with companies that are on the Texas Comptroller of Public Accounts list of Designated Foreign Terrorists Organizations found at <https://comptroller.texas.gov/purchasing/docs/foreign-terrorist.pdf>.

I further affirm that if our company's position on this issue is reversed and this affirmation is no longer valid, that the above-named Texas governmental entity will be notified in writing within one (1) business day and we understand that our company's failure to affirm and comply with the requirements of Texas Government Code 2270 et seq. shall be grounds for immediate contract termination without penalty to the above-named Texas governmental entity.

I swear and affirm that the above is true and correct.



Signature of Named Authorized Company Representative

4/9/2020

Date

EXHIBIT F
FEDERAL FUNDS CERTIFICATIONS

FEDERAL CERTIFICATIONS
ADDENDUM FOR AGREEMENT FUNDED BY U.S. FEDERAL GRANT

TO WHOM IT MAY CONCERN:

Participating Agencies may elect to use federal funds to purchase under the Master Agreement. This form should be completed and returned.

DEFINITIONS

Contract means a legal instrument by which a non-Federal entity purchases property or services needed to carry out the project or program under a Federal award. The term as used in this part does not include a legal instrument, even if the non-Federal entity considers it a contract, when the substance of the transaction meets the definition of a Federal award or subaward

Contractor means an entity that receives a contract as defined in Contract.

Cooperative agreement means a legal instrument of financial assistance between a Federal awarding agency or pass-through entity and a non-Federal entity that, consistent with 31 U.S.C. 6302–6305:

- (a) Is used to enter into a relationship the principal purpose of which is to transfer anything of value from the Federal awarding agency or pass-through entity to the non-Federal entity to carry out a public purpose authorized by a law of the United States (see 31 U.S.C. 6101(3)); and not to acquire property or services for the Federal government or pass-through entity's direct benefit or use;
- (b) Is distinguished from a grant in that it provides for substantial involvement between the Federal awarding agency or pass-through entity and the non-Federal entity in carrying out the activity contemplated by the Federal award.
- (c) The term does not include:
 - (1) A cooperative research and development agreement as defined in 15 U.S.C. 3710a; or
 - (2) An agreement that provides only:
 - (i) Direct United States Government cash assistance to an individual;
 - (ii) A subsidy;
 - (iii) A loan;
 - (iv) A loan guarantee; or
 - (v) Insurance.

Federal awarding agency means the Federal agency that provides a Federal award directly to a non-Federal entity

Federal award has the meaning, depending on the context, in either paragraph (a) or (b) of this section:

- (a)(1) The Federal financial assistance that a non-Federal entity receives directly from a Federal awarding agency or indirectly from a pass-through entity, as described in § 200.101 Applicability; or
- (2) The cost-reimbursement contract under the Federal Acquisition Regulations that a non-Federal entity receives directly from a Federal awarding agency or indirectly from a pass-through entity, as described in § 200.101 Applicability.
- (b) The instrument setting forth the terms and conditions. The instrument is the grant agreement, cooperative agreement, other agreement for assistance covered in paragraph (b) of § 200.40 Federal financial assistance, or the cost-reimbursement contract awarded under the Federal Acquisition Regulations.
- (c) Federal award does not include other contracts that a Federal agency uses to buy goods or services from a contractor or a contract to operate Federal government owned, contractor operated facilities (GOCOs).
- (d) See also definitions of Federal financial assistance, grant agreement, and cooperative agreement.

Non-Federal entity means a state, local government, Indian tribe, institution of higher education (IHE), or nonprofit organization that carries out a Federal award as a recipient or subrecipient.

Nonprofit organization means any corporation, trust, association, cooperative, or other organization, not including IHEs, that:

- (a) Is operated primarily for scientific, educational, service, charitable, or similar purposes in the public interest;
- (b) Is not organized primarily for profit; and

(c) Uses net proceeds to maintain, improve, or expand the operations of the organization.

Obligations means, when used in connection with a non-Federal entity's utilization of funds under a Federal award, orders placed for property and services, contracts and subawards made, and similar transactions during a given period that require payment by the non-Federal entity during the same or a future period.

Pass-through entity means a non-Federal entity that provides a subaward to a subrecipient to carry out part of a Federal program.

Recipient means a non-Federal entity that receives a Federal award directly from a Federal awarding agency to carry out an activity under a Federal program. The term recipient does not include subrecipients.

Simplified acquisition threshold means the dollar amount below which a non-Federal entity may purchase property or services using small purchase methods. Non-Federal entities adopt small purchase procedures in order to expedite the purchase of items costing less than the simplified acquisition threshold. The simplified acquisition threshold is set by the Federal Acquisition Regulation at 48 CFR Subpart 2.1 (Definitions) and in accordance with 41 U.S.C. 1908. As of the publication of this part, the simplified acquisition threshold is \$250,000, but this threshold is periodically adjusted for inflation. (Also see definition of § 200.67 Micro-purchase.)

Subaward means an award provided by a pass-through entity to a subrecipient for the subrecipient to carry out part of a Federal award received by the pass-through entity. It does not include payments to a contractor or payments to an individual that is a beneficiary of a Federal program. A subaward may be provided through any form of legal agreement, including an agreement that the pass-through entity considers a contract.

Subrecipient means a non-Federal entity that receives a subaward from a pass-through entity to carry out part of a Federal program; but does not include an individual that is a beneficiary of such program. A subrecipient may also be a recipient of other Federal awards directly from a Federal awarding agency.

Termination means the ending of a Federal award, in whole or in part at any time prior to the planned end of period of performance.

The following certifications and provisions may be required and apply when Participating Agency expends federal funds for any purchase resulting from this procurement process. Pursuant to 2 C.F.R. § 200.326, all contracts, including small purchases, awarded by the Participating Agency and the Participating Agency's subcontractors shall contain the procurement provisions of Appendix II to Part 200, as applicable.

APPENDIX II TO 2 CFR PART 200

(A) Contracts for more than the simplified acquisition threshold currently set at \$250,000, which is the inflation adjusted amount determined by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) as authorized by 41 U.S.C. 1908, must address administrative, contractual, or legal remedies in instances where contractors violate or breach contract terms, and provide for such sanctions and penalties as appropriate.

Pursuant to Federal Rule (A) above, when a Participating Agency expends federal funds, the Participating Agency reserves all rights and privileges under the applicable laws and regulations with respect to this procurement in the event of breach of contract by either party.

Does offeror agree? YES JK Initials of Authorized Representative of offeror

(B) Termination for cause and for convenience by the grantee or subgrantee including the manner by which it will be effected and the basis for settlement. (All contracts in excess of \$10,000)

Pursuant to Federal Rule (B) above, when a Participating Agency expends federal funds, the Participating Agency reserves the right to immediately terminate any agreement in excess of \$10,000 resulting from this procurement process in the event of a breach or default of the agreement by Offeror as detailed in the terms of the contract.

Does offeror agree? YES JK Initials of Authorized Representative of offeror

(C) Equal Employment Opportunity. Except as otherwise provided under 41 CFR Part 60, all contracts that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 must include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 CFR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

Pursuant to Federal Rule (C) above, when a Participating Agency expends federal funds on any federally assisted construction contract, the equal opportunity clause is incorporated by reference herein.

Does offeror agree to abide by the above? YES JK Initials of Authorized Representative of offeror

(D) Davis-Bacon Act, as amended (40 U.S.C. 3141-3148). When required by Federal program legislation, all prime construction contracts in excess of \$2,000 awarded by non-Federal entities must include a provision for compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, contractors must be required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, contractors must be required to pay wages not less than once a week. The non-Federal entity must place a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation. The decision to award a contract or subcontract must be conditioned upon the acceptance of the wage determination. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency. The contracts must also include a provision for compliance with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each contractor or subrecipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency.

Pursuant to Federal Rule (D) above, when a Participating Agency expends federal funds during the term of an award for all contracts and subgrants for construction or repair, offeror will be in compliance with all applicable Davis-Bacon Act provisions.

Does offeror agree? YES JK Initials of Authorized Representative of offeror

(E) Contract Work Hours and Safety Standards Act (40 U.S.C. 3701-3708). Where applicable, all contracts awarded by the non-Federal entity in excess of \$100,000 that involve the employment of mechanics or laborers must include a provision for compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, each contractor must be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

Pursuant to Federal Rule (E) above, when a Participating Agency expends federal funds, offeror certifies that offeror will be in compliance with all applicable provisions of the Contract Work Hours and Safety Standards Act during the term of an award for all contracts by Participating Agency resulting from this procurement process.

Does offeror agree? YES JK Initials of Authorized Representative of offeror

(F) Rights to Inventions Made Under a Contract or Agreement. If the Federal award meets the definition of "funding agreement" under 37 CFR §401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

Pursuant to Federal Rule (F) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term of an award for all contracts by Participating Agency resulting from this procurement process, the offeror agrees to comply with all applicable requirements as referenced in Federal Rule (F) above.

Does offeror agree? YES JK Initials of Authorized Representative of offeror

(G) Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended— Contracts and subgrants of amounts in excess of \$150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251- 1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA)

Pursuant to Federal Rule (G) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term of an award for all contracts by Participating Agency member resulting from this procurement process, the offeror agrees to comply with all applicable requirements as referenced in Federal Rule (G) above.

Does offeror agree? YES JK Initials of Authorized Representative of offeror

(H) Debarment and Suspension (Executive Orders 12549 and 12689)—A contract award (see 2 CFR 180.220) must not be made to parties listed on the government wide exclusions in the System for Award Management (SAM), in accordance with the Executive Office of the President Office of Management and Budget (OMB) guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), “Debarment and Suspension.” SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

Pursuant to Federal Rule (H) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term of an award for all contracts by Participating Agency resulting from this procurement process, the offeror certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation by any federal department or agency. If at any time during the term of an award the offeror or its principals becomes debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation by any federal department or agency, the offeror will notify the Participating Agency.

Does offeror agree? YES JK Initials of Authorized Representative of offeror

(I) Byrd Anti-Lobbying Amendment (31 U.S.C. 1352)—Contractors that apply or bid for an award exceeding \$100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

Pursuant to Federal Rule (I) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term and after the awarded term of an award for all contracts by Participating Agency resulting from this procurement process, the offeror certifies that it is in compliance with all applicable provisions of the Byrd Anti-Lobbying Amendment (31 U.S.C. 1352). The undersigned further certifies that:

- (1) No Federal appropriated funds have been paid or will be paid for on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of congress, or an employee of a Member of Congress in connection with the awarding of a Federal contract, the making of a Federal grant, the making of a Federal loan, the entering into a cooperative agreement, and the extension, continuation, renewal, amendment, or modification of a Federal contract, grant, loan, or cooperative agreement.
- (2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of congress, or an employee of a Member of Congress in connection with this Federal grant or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, “Disclosure Form to Report Lobbying”, in accordance with its instructions.
- (3) The undersigned shall require that the language of this certification be included in the award documents for all covered sub-awards exceeding \$100,000 in Federal funds at all appropriate tiers and that all subrecipients shall certify and disclose accordingly.

Does offeror agree? YES JK Initials of Authorized Representative of offeror

RECORD RETENTION REQUIREMENTS FOR CONTRACTS INVOLVING FEDERAL FUNDS

When federal funds are expended by Participating Agency for any contract resulting from this procurement process, offeror certifies that it will comply with the record retention requirements detailed in 2 CFR § 200.333. The offeror further certifies that offeror will retain all records as required by 2 CFR § 200.333 for a period of three years after grantees or subgrantees submit final expenditure reports or quarterly or annual financial reports, as applicable, and all other pending matters are closed.

Does offeror agree? YES JK Initials of Authorized Representative of offeror

CERTIFICATION OF COMPLIANCE WITH THE ENERGY POLICY AND CONSERVATION ACT

When Participating Agency expends federal funds for any contract resulting from this procurement process, offeror certifies that it will comply with the mandatory standards and policies relating to energy efficiency which are contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act (42 U.S.C. 6321 et seq.; 49 C.F.R. Part 18).

Does offeror agree? YES JK Initials of Authorized Representative of offeror

CERTIFICATION OF COMPLIANCE WITH BUY AMERICA PROVISIONS

To the extent purchases are made with Federal Highway Administration, Federal Railroad Administration, or Federal Transit Administration funds, offeror certifies that its products comply with all applicable provisions of the Buy America Act and agrees to provide such certification or applicable waiver with respect to specific products to any Participating Agency upon request. Purchases made in accordance with the Buy America Act must still follow the applicable procurement rules calling for free and open competition.

Does offeror agree? YES JK Initials of Authorized Representative of offeror

CERTIFICATION OF ACCESS TO RECORDS – 2 C.F.R. § 200.336

Offeror agrees that the Inspector General of the Agency or any of their duly authorized representatives shall have access to any documents, papers, or other records of offeror that are pertinent to offeror's discharge of its obligations under the Contract for the purpose of making audits, examinations, excerpts, and transcriptions. The right also includes timely and reasonable access to offeror's personnel for the purpose of interview and discussion relating to such documents.

Does offeror agree? YES JK Initials of Authorized Representative of offeror

CERTIFICATION OF APPLICABILITY TO SUBCONTRACTORS

Offeror agrees that all contracts it awards pursuant to the Contract shall be bound by the foregoing terms and conditions.

Does offeror agree? YES JK Initials of Authorized Representative of offeror

Offeror agrees to comply with all federal, state, and local laws, rules, regulations and ordinances, as applicable. It is further acknowledged that offeror certifies compliance with all provisions, laws, acts, regulations, etc. as specifically noted above.

Offeror's Name: ThunderCat Technology, LLC

Address, City, State, and Zip Code: 1925 Isaac Newton Square, Suite 180, Reston, VA 20190

Phone Number: 703-674-0216 Fax Number: 571-323-0918

Printed Name and Title of Authorized Representative: Jean Kim, Contracts

Email Address: contracts@thundercattech.com

Signature of Authorized Representative:  Date: 4/9/2020

FEMA SPECIAL CONDITIONS

Awarded Supplier(s) may need to respond to events and losses where products and services are needed for the immediate and initial response to emergency situations such as, but not limited to, water damage, fire damage, vandalism cleanup, biohazard cleanup, sewage decontamination, deodorization, and/or wind damage during a disaster or emergency situation. By submitting a proposal, the Supplier is accepted these FEMA Special Conditions required by the Federal Emergency Management Agency (FEMA).

“Contract” in the below pages under FEMA SPECIAL CONDITIONS is also referred to and defined as the “Master Agreement”.

“Contractor” in the below pages under FEMA SPECIAL CONDITIONS is also referred to and defined as “Supplier” or “Awarded Supplier”.

Conflicts of Interest

No employee, officer, or agent may participate in the selection, award, or administration of a contract supported by a FEMA award if he or she has a real or apparent conflict of interest. Such a conflict would arise when the employee, officer, or agent, any member of his or her immediate family, his or her partner, or an organization which employs or is about to employ any of these parties, has a financial or other interest in or a tangible personal benefit from a firm considered for award. 2 C.F.R. § 200.318(c)(1); See also Standard Form 424D, ¶ 7; Standard Form 424B, ¶ 3. i. FEMA considers a “financial interest” to be the potential for gain or loss to the employee, officer, or agent, any member of his or her immediate family, his or her partner, or an organization which employs or is about to employ any of these parties as a result of the particular procurement. The prohibited financial interest may arise from ownership of certain financial instruments or investments such as stock, bonds, or real estate, or from a salary, indebtedness, job offer, or similar interest that might be affected by the particular procurement. ii. FEMA considers an “apparent” conflict of interest to exist where an actual conflict does not exist, but where a reasonable person with knowledge of the relevant facts would question the impartiality of the employee, officer, or agent participating in the procurement. c. Gifts. The officers, employees, and agents of the Participating Public Agency nor the Participating Public Agency (“NFE”) must neither solicit nor accept gratuities, favors, or anything of monetary value from contractors or parties to subcontracts. However, NFE’s may set standards for situations in which the financial interest is de minimus, not substantial, or the gift is an unsolicited item of nominal value. 2 C.F.R. § 200.318(c)(1). d. Violations. The NFE’s written standards of conduct must provide for disciplinary actions to be applied for violations of such standards by officers, employees, or agents of the NFE. 2 C.F.R. § 200.318(c)(1). For example, the penalty for a NFE’s employee may be dismissal, and the penalty for a contractor might be the termination of the contract.

Contractor Integrity

A contractor must have a satisfactory record of integrity and business ethics. Contractors that are debarred or suspended as described in Chapter III, ¶ 6.d must be rejected and cannot receive contract awards at any level.

Public Policy

A contractor must comply with the public policies of the Federal Government and state, local government, or tribal government. This includes, among other things, past and current compliance with the:

- a. Equal opportunity and nondiscrimination laws
- b. Five affirmative steps described at 2 C.F.R. § 200.321(b) for all subcontracting under contracts supported by FEMA financial assistance; and FEMA Procurement Guidance June 21, 2016 Page IV- 7
- c. Applicable prevailing wage laws, regulations, and executive orders

Affirmative Steps

For any subcontracting opportunities, Contractor must take the following Affirmative steps:

1. Placing qualified small and minority businesses and women’s business enterprises on solicitation lists;
2. Assuring that small and minority businesses, and women’s business enterprises are solicited whenever they are potential sources;
3. Dividing total requirements, when economically feasible, into smaller tasks or quantities to permit maximum participation by small and minority businesses, and women’s business enterprises;
4. Establishing delivery schedules, where the requirement permits, which encourage participation by small and minority businesses, and women’s business enterprises; and

5. Using the services and assistance, as appropriate, of such organizations as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce.

Prevailing Wage Requirements

When applicable, the awarded Contractor (s) and any and all subcontractor(s) agree to comply with all laws regarding prevailing wage rates including the Davis-Bacon Act, applicable to this solicitation and/or Participating Public Agencies. The Participating Public Agency shall notify the Contractor of the applicable pricing/prevailing wage rates and must apply any local wage rates requested. The Contractor and any subcontractor(s) shall comply with the prevailing wage rates set by the Participating Public Agency.

Federal Requirements

If products and services are issued in response to an emergency or disaster recovery the items below, located in this FEMA Special Conditions section of the Federal Funds Certifications, are activated and required when federal funding may be utilized.

2 C.F.R. § 200.326 and 2 C.F.R. Part 200, Appendix II, Required Contract Clauses

1. Termination for Convenience:

The right to terminate this Contract for the convenience of the Participating Public Agency is retained by the Participating Public Agency. In the event of a termination for convenience by the Participating Public Agency, the Participating Public Agency shall, at least ten (10) calendar days in advance, deliver written notice of the termination for convenience to Contractor. Upon Contractor's receipt of such written notice, Contractor immediately shall cease the performance of the Work and shall take reasonable and appropriate action to secure and protect the Work then in place. Contractor shall then be paid by the Participating Public Agency, in accordance with the terms and provisions of the Contract Documents, an amount not to exceed the actual labor costs incurred, the actual cost of all materials installed and the actual cost of all materials stored at the project site or away from the project site, as approved in writing by the Participating Public Agency but not yet paid for and which cannot be returned, and actual, reasonable and documented demobilization costs, if any, paid by Contractor and approved by the Participating Public Agency in connection with the Scope of Work in place which is completed as of the date of termination by the Participating Public Agency and that is in conformance with the Contract Documents, less all amounts previously paid for the Work. No amount ever shall be owed or paid to Contractor for lost or anticipated profits on any part of the Scope of Work not performed or for consequential damages of any kind.

2. Equal Employment Opportunity:

The Participating Public Agency highly encourages Contractors to implement Affirmative Action practices in their employment programs. This means Contractor should not discriminate against any employee or applicant for employment because of race, color, religion, sex, pregnancy, sexual orientation, political belief or affiliation, age, disability or genetic information.

During the performance of this contract, the contractor agrees as follows:

(1) The contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following: Employment, upgrading, demotion, or transfer, recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the contracting officer setting forth the provisions of this nondiscrimination clause.

(2) The contractor will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

(3) The contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the contractor's legal duty to furnish information.

(4) The contractor will send to each labor union or representative of workers with which it has a collective bargaining agreement or other contract or understanding, a notice to be provided by the agency contracting officer, advising the labor union or workers' representative of the contractor's commitments under section 202 of Executive Order 11246 of September 24, 1965, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

(5) The contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

(6) The contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by the rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the contracting agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

(7) In the event of the contractor's non-compliance with the nondiscrimination clauses of this contract or with any of such rules, regulations, or orders, this contract may be canceled, terminated or suspended in whole or in part and the contractor may be declared ineligible for further Government contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

(8) The contractor will include the provisions of paragraphs (1) through (8) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The contractor will take such action with respect to any subcontract or purchase order as may be directed by the Secretary of Labor as a means of enforcing such provisions including sanctions for noncompliance: *Provided*, however, that in the event the contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction, the contractor may request the United States to enter into such litigation to protect the interests of the United States.

3. "During the performance of this contract, the contractor agrees as follows:

- (1) The contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, or national origin. The contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, or national origin. Such action shall include, but not be limited to the following: Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.
- (2) The contractor will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive considerations for employment without regard to race, color, religion, sex, or national origin.
- (3) The contractor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice

to be provided advising the said labor union or workers' representatives of the contractor's commitments under this section, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

- (4) The contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.
- (5) The contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.
- (6) In the event of the contractor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this contract may be canceled, terminated, or suspended in whole or in part and the contractor may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions as may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.
- (7) The contractor will include the portion of the sentence immediately preceding paragraph (1) and the provisions of paragraphs (1) through (7) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance: Provided, however, That in the event a contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the administering agency the contractor may request the United States to enter into such litigation to protect the interests of the United States."

4. Davis Bacon Act and Copeland Anti-Kickback Act.

- a. Applicability of Davis-Bacon Act. The Davis-Bacon Act only applies to the emergency Management Preparedness Grant Program, Homeland Security Grant Program, Nonprofit Security Grant Program, Tribal Homeland Security Grant Program, Port Security Grant Program, and Transit Security Grant Program. **It does not apply to other FEMA grant and cooperative agreement programs, including the Public Assistance Program.**
- b. All prime construction contracts in excess of \$2,000 awarded by non-Federal entities must include a provision for compliance with the Davis-Bacon Act (40 U.S.C. §§ 3141-3144 and 3146-3148) as supplemented by Department of Labor regulations at 29 C.F.R. Part 5 (Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction)). See 2 C.F.R. Part 200, Appendix II, ¶ D.
- c. In accordance with the statute, contractors must be required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, contractors must be required to pay wages not less than once a week.
- d. The non-Federal entity must place a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation. The decision to award a contract or subcontract must be conditioned upon the acceptance of the wage determination. The non-Federal entity must report all suspected or reported violations to the Federal awarding

agency.

- e. In contracts subject to the Davis-Bacon Act, the contracts must also include a provision for compliance with the Copeland "Anti-Kickback" Act (40 U.S.C. § 3145), as supplemented by Department of Labor regulations at 29 C.F.R. Part 3 (Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States). The Copeland Anti- Kickback Act provides that each contractor or subrecipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The non-Federal entity must report all suspected or reported violations to FEMA.
- f. The regulation at 29 C.F.R. § 5.5(a) does provide the required contract clause that applies to compliance with both the Davis-Bacon and Copeland Acts. However, as discussed in the previous subsection, the Davis-Bacon Act does not apply to Public Assistance recipients and subrecipients. **In situations where the Davis-Bacon Act does not apply, neither does the Copeland "Anti-Kickback Act."** However, for purposes of grant programs where both clauses do apply, FEMA requires the following contract clause:

"Compliance with the Copeland "Anti-Kickback" Act.

- (1) Contractor. The contractor shall comply with 18 U.S.C. § 874, 40U.S.C. § 3145, and the requirements of 29 C.F.R. pt. 3 as may be applicable, which are incorporated by reference into this contract.
- (2) Subcontracts. The contractor or subcontractor shall insert in any subcontracts the clause above and such other clauses as the FEMA may by appropriate instructions require, and also a clause requiring the subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for the compliance by any subcontractor or lower tier subcontractor with all of these contract clauses
- (3) Breach. A breach of the contract clauses above may be grounds for termination of the contract, and for debarment as a contractor and subcontractor as provided in 29 C.F.R. § 5.12."

5. Contract Work Hours and Safety Standards Act.

- a. Applicability: This requirement applies to all FEMA grant and cooperative agreement programs.
- b. Where applicable (see 40 U.S.C. § 3701), all contracts awarded by the non-Federal entity in excess of \$100,000 that involve the employment of mechanics or laborers must include a provision for compliance with 40 U.S.C. §§ 3702 and 3704, as supplemented by Department of Labor regulations at 29 C.F.R. Part 5. See 2 C.F.R. Part 200, Appendix II, ¶ E.
- c. Under 40 U.S.C. § 3702, each contractor must be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the workweek.
- d. The requirements of 40 U.S.C. § 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.
- e. The regulation at 29 C.F.R. § 5.5(b) provides the required contract clause concerning compliance with the Contract Work Hours and Safety Standards Act:

“Compliance with the Contract Work Hours and Safety Standards Act.

- (1) Overtime requirements. No contractor or subcontractor contracting for any part of the contract work which may require or involve the employment of laborers or mechanics shall require or permit any such laborer or mechanic in any workweek in which he or she is employed on such work to work in excess of forty hours in such workweek unless such laborer or mechanic receives compensation at a rate not less than one and one-half times the basic rate of pay for all hours worked in excess of forty hours in such workweek.
- (2) Violation; liability for unpaid wages; liquidated damages. In the event of any violation of the clause set forth in paragraph (1) of this section the contractor and any subcontractor responsible therefor shall be liable for the unpaid wages. In addition, such contractor and subcontractor shall be liable to the United States (in the case of work done under contract for the District of Columbia or a territory, to such District or to such territory), for liquidated damages. Such liquidated damages shall be computed with respect to each individual laborer or mechanic, including watchmen and guards, employed in violation of the clause set forth in paragraph (1) of this section, in the sum of \$10 for each calendar day on which such individual was required or permitted to work in excess of the standard workweek of forty hours without payment of the overtime wages required by the clause set forth in paragraph (1) of this section.
- (3) Withholding for unpaid wages and liquidated damages. The (write in the name of the Federal agency or the loan or grant recipient) shall upon its own action or upon written request of an authorized representative of the Department of Labor withhold or cause to be withheld, from any moneys payable on account of work performed by the contractor or subcontractor under any such contract or any other Federal contract with the same prime contractor, or any other federally-assisted contract subject to the Contract Work Hours and Safety Standards Act, which is held by the same prime contractor, such sums as may be determined to be necessary to satisfy any liabilities of such contractor or subcontractor for unpaid wages and liquidated damages as provided in the clause set forth in paragraph (2) of this section.
- (4) Subcontracts. The contractor or subcontractor shall insert in any subcontracts the clauses set forth in paragraph (1) through (4) of this section and also a clause requiring the subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for compliance by any subcontractor or lower tier subcontractor with the clauses set forth in paragraphs (1) through (4) of this section.”

6. Rights to Inventions Made Under a Contract or Agreement.

- a. Stafford Act Disaster Grants. This requirement **does not apply to the Public Assistance, Hazard Mitigation Grant Program, Fire Management Assistance Grant Program, Crisis Counseling Assistance and Training Grant Program, Disaster Case Management Grant Program, and Federal Assistance to Individuals and Households – Other Needs Assistance Grant Program, as**

FEMA awards under these programs do not meet the definition of “funding agreement.”

- b. If the FEMA award meets the definition of “funding agreement” under 37 C.F.R. § 401.2(a) and the non-Federal entity wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that “funding agreement,” the non-Federal entity must comply with the requirements of 37 C.F.R. Part 401 (Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements), and any implementing regulations issued by FEMA. See 2 C.F.R.

- c. The regulation at 37 C.F.R. § 401.2(a) currently defines “funding agreement” as any contract, grant, or cooperative agreement entered into between any Federal agency, other than the Tennessee Valley Authority, and any contractor for the performance of experimental, developmental, or research work funded in whole or in part by the Federal government. This term also includes any assignment, substitution of parties, or subcontract of any type entered into for the performance of experimental, developmental, or research work under a funding agreement as defined in the first sentence of this paragraph.
7. Clean Air Act and the Federal Water Pollution Control Act. Contracts of amounts in excess of \$150,000 must contain a provision that requires the contractor to agree to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. §§ 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. §§ 1251-1387). Violations must be reported to FEMA and the Regional Office of the Environmental Protection Agency. See 2 C.F.R. Part 200, Appendix II, ¶ G.
- a. The following provides a sample contract clause concerning compliance for contracts of amounts in excess of \$150,000:

“Clean Air Act

 - (1) The contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq.
 - (2) The contractor agrees to report each violation to the (name of the state agency or local or Indian tribal government) and understands and agrees that the (name of the state agency or local or Indian tribal government) will, in turn, report each violation as required to assure notification to the (name of recipient), Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.
 - (3) The contractor agrees to include these requirements in each subcontract exceeding \$150,000 financed in whole or in part with Federal assistance provided by FEMA.

Federal Water Pollution Control Act

 - (1) The contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.
 - (2) The contractor agrees to report each violation to the (name of the state agency or local or Indian tribal government) and understands and agrees that the (name of the state agency or local or Indian tribal government) will, in turn, report each violation as required to assure notification to the (name of recipient), Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.
 - (3) The contractor agrees to include these requirements in each subcontract exceeding \$150,000 financed in whole or in part with Federal assistance provided by FEMA.”
8. Debarment and Suspension.
- a. Applicability: This requirement applies to all FEMA grant and cooperative agreement programs.
 - b. Non-federal entities and contractors are subject to the debarment and suspension regulations implementing Executive Order 12549, *Debarment and Suspension* (1986) and Executive Order 12689, *Debarment and Suspension* (1989) at 2 C.F.R. Part 180 and the Department of Homeland Security’s regulations at 2 C.F.R. Part 3000 (Non procurement Debarment and

Suspension).

- c. These regulations restrict awards, subawards, and contracts with certain parties that are debarred, suspended, or otherwise excluded from or ineligible for participation in Federal assistance programs and activities. See 2 C.F.R. Part 200, Appendix II, ¶ H; and *Procurement Guidance for Recipients and Subrecipients Under 2 C.F.R. Part 200 (Uniform Rules): Supplement to the Public Assistance Procurement Disaster Assistance Team (PDAT) Field Manual Chapter IV, ¶ 6.d, and Appendix C, ¶ 2 [hereinafter PDAT Supplement]*. A contract award must not be made to parties listed in the SAM Exclusions. SAM Exclusions is the list maintained by the General Services Administration that contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. SAM exclusions can be accessed at www.sam.gov. See 2 C.F.R. § 180.530; PDAT Supplement, Chapter IV, ¶ 6.d and Appendix C, ¶ 2.
- d. In general, an “excluded” party cannot receive a Federal grant award or a contract within the meaning of a “covered transaction,” to include subawards and subcontracts. This includes parties that receive Federal funding indirectly, such as contractors to recipients and subrecipients. The key to the exclusion is whether there is a “covered transaction,” which is any non-procurement transaction (unless excepted) at either a “primary” or “secondary” tier. Although “covered transactions” do not include contracts awarded by the Federal Government for purposes of the non-procurement common rule and DHS’s implementing regulations, it does include some contracts awarded by recipients and subrecipient.
- e. Specifically, a covered transaction includes the following contracts for goods or services:
 - (1) The contract is awarded by a recipient or subrecipient in the amount of at least \$25,000.
 - (2) The contract requires the approval of FEMA, regardless of amount.
 - (3) The contract is for federally required audit services.
 - (4) A subcontract is also a covered transaction if it is awarded by the contractor of a recipient or subrecipient and requires either the approval of FEMA or is in excess of \$25,000.
- d. The following provides a debarment and suspension clause. It incorporates an optional method of verifying that contractors are not excluded or disqualified:

“Suspension and Debarment

- (1) This contract is a covered transaction for purposes of 2 C.F.R. pt. 180 and 2 C.F.R. pt. 3000. As such the contractor is required to verify that none of the contractor, its principals (defined at 2 C.F.R. § 180.995), or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935).
- (2) The contractor must comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.
- (3) This certification is a material representation of fact relied upon by (insert name of subrecipient). If it is later determined that the contractor did not comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, in addition to remedies available to (name of state agency serving as recipient and name of subrecipient), the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.
- (4) The bidder or proposer agrees to comply with the requirements of 2 C.F.R. pt. 180,

subpart C and 2 C.F.R. pt. 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. The bidder or proposer further agrees to include a provision requiring such compliance in its lower tier covered transactions.”

9. Byrd Anti-Lobbying Amendment.

- a. Applicability: This requirement applies to all FEMA grant and cooperative agreement programs.
- b. Contractors that apply or bid for an award of \$100,000 or more must file the required certification. See 2 C.F.R. Part 200, Appendix II, ¶ 1; 44 C.F.R. Part 18; *PDAT Supplement*, Chapter IV, 6.c; Appendix C, ¶ 4.
- c. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. § 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award. See *PDAT Supplement*, Chapter IV, ¶ 6.c and Appendix C, ¶ 4.
- d. The following provides a Byrd Anti-Lobbying contract clause:

“Byrd Anti-Lobbying Amendment, 31 U.S.C. § 1352 (as amended)

Contractors who apply or bid for an award of \$100,000 or more shall file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Each tier shall also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the recipient.”

APPENDIX A, 44 C.F.R. PART 18 – CERTIFICATION REGARDING LOBBYING

Certification for Contracts, Grants, Loans, and Cooperative Agreements (To be submitted with each bid or offer exceeding \$100,000)

The undersigned [Contractor] certifies, to the best of his or her knowledge, that:

1. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.
2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the

undersigned shall complete and submit Standard Form- LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

3. The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by 31, U.S.C. § 1352 (as amended by the Lobbying Disclosure Act of 1995). Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

The Contractor, ThunderCat Technology, LLC, certifies or affirms the truthfulness and accuracy of each statement of its certification and disclosure, if any. In addition, the Contractor understands and agrees that the provisions of 31 U.S.C. § 3801 et seq., apply to this certification and disclosure, if any.


Signature of Contractor's Authorized Official

Jean Kim, Contracts
Name and Title of Contractor's Authorized Official

4/9/2020
Date

10. Procurement of Recovered Materials.

- a. Applicability: This requirement applies to all FEMA grant and cooperative agreement programs.
- b. A non-Federal entity that is a state agency or agency of a political subdivision of a state and its contractors must comply with Section 6002 of the Solid Waste Disposal Act, Pub. L. No. 89-272 (1965) (codified as amended by the Resource Conservation and Recovery Act at 42 U.S.C. § 6962). See 2 C.F.R. Part 200, Appendix II, ¶ J; 2 C.F.R. § 200.322; PDAT Supplement, Chapter V, ¶ 7.
- c. The requirements of Section 6002 include procuring only items designated in guidelines of the EPA at 40 C.F.R. Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds \$10,000 or the value of the quantity acquired by the preceding fiscal year exceeded \$10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.
- d. The following provides the clause that a state agency or agency of a political subdivision of a state and its contractors can include in contracts meeting the above contract thresholds:

"(1) In the performance of this contract, the Contractor shall make maximum use of products containing recovered materials that are EPA- designated items unless the product cannot be acquired—

- (i) Competitively within a timeframe providing for compliance with the contract performance schedule;
- (ii) Meeting contract performance requirements; or
- (iii) At a reasonable price.

(2) Information about this requirement, along with the list of EPA- designate items, is available at EPA's Comprehensive Procurement Guidelines web site, <https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program>."

11. Additional FEMA Requirements.

- a. The Uniform Rules authorize FEMA to require additional provisions for non- Federal entity contracts. FEMA, pursuant to this authority, requires or recommends the following:

- b. Changes.

To be eligible for FEMA assistance under the non-Federal entity's FEMA grant or cooperative agreement, the cost of the change, modification, change order, or constructive change must be allowable, allocable, within the scope of its grant or cooperative agreement, and reasonable for the completion of project scope. FEMA recommends, therefore, that a non-Federal entity include a changes clause in its contract that describes how, if at all, changes can be made by either party to alter the method, price, or schedule of the work without breaching the contract. The language of the clause may differ depending on the nature of the contract and the end-item procured.

- c. Access to Records.

All non-Federal entities must place into their contracts a provision that all contractors and their successors, transferees, assignees, and subcontractors acknowledge and agree to comply with applicable provisions governing Department and FEMA access to records, accounts, documents, information, facilities, and staff. See DHS Standard Terms and Conditions, v 3.0, ¶ XXVI (2013).

- d. The following provides a contract clause regarding access to records:

"Access to Records. The following access to records requirements apply to this contract:

(1) The contractor agrees to provide (insert name of state agency or local or Indian tribal government), (insert name of recipient), the FEMA Administrator, the Comptroller General of the United States, or any of their authorized representatives access to any books, documents, papers, and records of the Contractor which are directly pertinent to this contract for the purposes of making audits, examinations, excerpts, and transcriptions.

(2) The Contractor agrees to permit any of the foregoing parties to reproduce by any means whatsoever or to copy excerpts and transcriptions as reasonably needed.

(3) The contractor agrees to provide the FEMA Administrator or his authorized representatives access to construction or other work sites pertaining to the work being completed under the contract."

12. DHS Seal, Logo, and Flags.

- a. All non-Federal entities must place in their contracts a provision that a contractor shall not use the DHS seal(s), logos, crests, or reproductions of flags or likenesses of DHS agency officials without specific FEMA pre-approval. See DHS Standard Terms and Conditions, v 3.0, ¶ XXV (2013).
- b. The following provides a contract clause regarding DHS Seal, Logo, and Flags: “The contractor shall not use the DHS seal(s), logos, crests, or reproductions of flags or likenesses of DHS agency officials without specific FEMA pre- approval.”

13. Compliance with Federal Law, Regulations, and Executive Orders.

- a. All non-Federal entities must place into their contracts an acknowledgement that FEMA financial assistance will be used to fund the contract along with the requirement that the contractor will comply with all applicable federal law, regulations, executive orders, and FEMA policies, procedures, and directives.
- b. The following provides a contract clause regarding Compliance with Federal Law, Regulations, and Executive Orders: “This is an acknowledgement that FEMA financial assistance will be used to fund the contract only. The contractor will comply will all applicable federal law, regulations, executive orders, FEMA policies, procedures, and directives.”

14. No Obligation by Federal Government.

- a. The non-Federal entity must include a provision in its contract that states that the Federal Government is not a party to the contract and is not subject to any obligations or liabilities to the non-Federal entity, contractor, or any other party pertaining to any matter resulting from the contract.
- b. The following provides a contract clause regarding no obligation by the Federal Government: “The Federal Government is not a party to this contract and is not subject to any obligations or liabilities to the non-Federal entity, contractor, or any other party pertaining to any matter resulting from the contract.”

15. Program Fraud and False or Fraudulent Statements or Related Acts.

- a. The non-Federal entity must include a provision in its contract that the contractor acknowledges that 31 U.S.C. Chap. 38 (Administrative Remedies for False Claims and Statements) applies to its actions pertaining to the contract.
- b. The following provides a contract clause regarding Fraud and False or Fraudulent or Related Acts: “The contractor acknowledges that 31 U.S.C. Chap. 38 (Administrative Remedies for False Claims and Statements) applies to the contractor’s actions pertaining to this contract.”

Additional contract clauses per 2 C.F.R. § 200.325

For applicable construction/reconstruction/renovation and related services: A payment and performance bond are both required for 100 percent of the contract price. A “performance bond” is one executed in connection with a contract to secure fulfillment of all the contractor’s obligations under such contract. A “payment bond” is one executed in connection with a contract to assure payment as required by law of all persons supplying labor and material in the execution of the work provided in the contract.

Offeror agrees to comply with all terms and conditions outlined in the FEMA Special Conditions section of this solicitation.

Offeror's Name:

ThunderCat Technology, LLC

Address, City, State, and Zip Code:

1925 Isaac Newton Square, Suite 180, Reston, VA 20190

Phone Number: 703-674-0216

Fax Number: 571-323-0918

Printed Name and Title of Authorized

Representative: Jean Kim, Contracts

Email Address: contracts@thundercattech.com

Signature of Authorized Representative:



Date: 4/9/2020

EXHIBIT G
NEW JERSEY BUSINESS COMPLIANCE

NEW JERSEY BUSINESS COMPLIANCE

Suppliers intending to do business in the State of New Jersey must comply with policies and procedures required under New Jersey statutes. All offerors submitting proposals must complete the following forms specific to the State of New Jersey. Completed forms should be submitted with the offeror's response to the RFP. Failure to complete the New Jersey packet will impact OMNIA Partners' ability to promote the Master Agreement in the State of New Jersey.

DOC #1	Ownership Disclosure Form
DOC #2	Non-Collusion Affidavit
DOC #3	Affirmative Action Affidavit
DOC #4	Political Contribution Disclosure Form
DOC #5	Stockholder Disclosure Certification
DOC #6	Certification of Non-Involvement in Prohibited Activities in Iran
DOC #7	New Jersey Business Registration Certificate

New Jersey suppliers are required to comply with the following New Jersey statutes when applicable:

- all anti-discrimination laws, including those contained in N.J.S.A. 10:2-1 through N.J.S.A. 10:2-14, N.J.S.A. 10:5-1, and N.J.S.A. 10:5-31 through 10:5-38;
- Prevailing Wage Act, N.J.S.A. 34:11-56.26, for all contracts within the contemplation of the Act;
- Public Works Contractor Registration Act, N.J.S.A. 34:11-56.26; and
- Bid and Performance Security, as required by the applicable municipal or state statutes.

**OWNERSHIP DISCLOSURE FORM
(N.J.S. 52:25-24.2)**

Pursuant to the requirements of P.L. 1999, Chapter 440 effective April 17, 2000 (Local Public Contracts Law), the offeror shall complete the form attached to these specifications listing the persons owning 10 percent (10%) or more of the firm presenting the proposal.

Company Name: ThunderCat Technology, LLC

Street: 1925 Isaac Newton Square, Suite 180

City, State, Zip Code: Reston, VA 20190

Complete as appropriate:

I _____, certify that I am the sole owner of _____, that there are no partners and the business is not incorporated, and the provisions of N.J.S. 52:25-24.2 do not apply.

OR:

I _____, a partner in _____, do hereby certify that the following is a list of all individual partners who own a 10% or greater interest therein. I further certify that if one (1) or more of the partners is itself a corporation or partnership, there is also set forth the names and addresses of the stockholders holding 10% or more of that corporation's stock or the individual partners owning 10% or greater interest in that partnership.

OR:

I Jean Kim, an authorized representative of ThunderCat Technology, LLC, a corporation, do hereby certify that the following is a list of the names and addresses of all stockholders in the corporation who own 10% or more of its stock of any class. I further certify that if one (1) or more of such stockholders is itself a corporation or partnership, that there is also set forth the names and addresses of the stockholders holding 10% or more of the corporation's stock or the individual partners owning a 10% or greater interest in that partnership.

(Note: If there are no partners or stockholders owning 10% or more interest, indicate none.)

Name	Address	Interest
Thomas Deierlein	19 Westbury Road, Garden City, NY 11530	100%

I further certify that the statements and information contained herein, are complete and correct to the best of my knowledge and belief.

4/9/2020
Date

 Contracts
Authorized Signature and Title

NON-COLLUSION AFFIDAVIT

Company Name: ThunderCat Technology, LLC

Street: 1925 Isaac Newton Square, Suite 180

City, State, Zip Code: Reston, VA 20190

State of Virginia

County of Fairfax

I, _____ of the _____
Name City

in the County of _____, State of _____
of full age, being duly sworn according to law on my oath depose and say that:

I am the _____ of the firm of _____
Title Company Name

the Offeror making the Proposal for the goods, services or public work specified under the attached proposal, and that I executed the said proposal with full authority to do so; that said Offeror has not directly or indirectly entered into any agreement, participated in any collusion, or otherwise taken any action in restraint of free, competitive bidding in connection with the above proposal, and that all statements contained in said proposal and in this affidavit are true and correct, and made with full knowledge that relies upon the truth of the statements contained in said proposal and in the statements contained in this affidavit in awarding the contract for the said goods, services or public work.

I further warrant that no person or selling agency has been employed or retained to solicit or secure such contract upon an agreement or understanding for a commission, percentage, brokerage or contingent fee, except bona fide employees or bona fide established commercial or selling agencies maintained by

Company Name

Authorized Signature & Title

Subscribed and sworn before me

this _____ day of _____, 20____

Notary Public of _____

My commission expires _____, 20____

SEAL

**AFFIRMATIVE ACTION AFFIDAVIT
(P.L. 1975, C.127)**

Company Name: ThunderCat Technology, LLC

Street: 1925 Isaac Newton Square, Suite 180

City, State, Zip Code: Reston, VA 20190

Proposal Certification:

Indicate below company's compliance with New Jersey Affirmative Action regulations. Company's proposal will be accepted even if company is not in compliance at this time. No contract and/or purchase order may be issued, however, until all Affirmative Action requirements are met.

Required Affirmative Action Evidence:

Procurement, Professional & Service Contracts (Exhibit A)

Vendors must submit with proposal:

- 1. A photo copy of their Federal Letter of Affirmative Action Plan Approval

OR

- 2. A photo copy of their Certificate of Employee Information Report

OR

- 3. A complete Affirmative Action Employee Information Report (AA302) _____

Public Work – Over \$50,000 Total Project Cost:

A. No approved Federal or New Jersey Affirmative Action Plan. We will complete Report Form AA201-A upon receipt from the

B. Approved Federal or New Jersey Plan – certificate enclosed

I further certify that the statements and information contained herein, are complete and correct to the best of my knowledge and belief.

4/9/2020
Date

 *Contracts*
Authorized Signature and Title

P.L. 1995, c. 127 (N.J.A.C. 17:27)
MANDATORY AFFIRMATIVE ACTION LANGUAGE

PROCUREMENT, PROFESSIONAL AND SERVICE
CONTRACTS

During the performance of this contract, the contractor agrees as follows:

The contractor or subcontractor, where applicable, will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation. The contractor will take affirmative action to ensure that such applicants are recruited and employed, and that employees are treated during employment, without regard to their age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation. Such action shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Public Agency Compliance Officer setting forth provisions of this non-discrimination clause.

The contractor or subcontractor, where applicable will, in all solicitations or advertisement for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation.

The contractor or subcontractor, where applicable, will send to each labor union or representative of workers with which it has a collective bargaining agreement or other contract or understanding, a notice, to be provided by the agency contracting officer advising the labor union or workers' representative of the contractor's commitments under this act and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

The contractor or subcontractor, where applicable, agrees to comply with any regulations promulgated by the Treasurer pursuant to P.L. 1975, c. 127, as amended and supplemented from time to time and the Americans with Disabilities Act.

The contractor or subcontractor agrees to attempt in good faith to employ minority and female workers trade consistent with the applicable county employment goal prescribed by N.J.A.C. 17:27-5.2 promulgated by the Treasurer pursuant to P.L. 1975, C.127, as amended and supplemented from time to time or in accordance with a binding determination of the applicable county employment goals determined by the Affirmative Action Office pursuant to N.J.A.C. 17:27-5.2 promulgated by the Treasurer pursuant to P.L. 1975, C.127, as amended and supplemented from time to time.

The contractor or subcontractor agrees to inform in writing appropriate recruitment agencies in the area, including employment agencies, placement bureaus, colleges, universities, labor unions, that it does not discriminate on the basis of age, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation, and that it will discontinue the use of any recruitment agency which engages in direct or indirect discriminatory practices.

The contractor or subcontractor agrees to revise any of its testing procedures, if necessary, to assure that all personnel testing conforms with the principles of job-related testing, as established by the statutes and court decisions of the state of New Jersey and as established by applicable Federal law and applicable Federal court decisions.

The contractor or subcontractor agrees to review all procedures relating to transfer, upgrading, downgrading and lay-off to ensure that all such actions are taken without regard to age, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation, and conform with the applicable employment goals, consistent with the statutes and court decisions of the State of New Jersey, and applicable Federal law and applicable Federal court decisions.

The contractor and its subcontractors shall furnish such reports or other documents to the Affirmative Action Office as may be requested by the office from time to time in order to carry out the purposes of these regulations, and public agencies shall furnish such information as may be requested by the Affirmative Action Office for conducting a compliance investigation pursuant to Subchapter 10 of the Administrative Code (NJAC 17:27).



Signature of Procurement Agent

C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM

Public Agency Instructions

This page provides guidance to public agencies entering into contracts with business entities that are required to file Political Contribution Disclosure forms with the agency. **It is not intended to be provided to contractors.** What follows are instructions on the use of form local units can provide to contractors that are required to disclose political contributions pursuant to N.J.S.A. 19:44A-20.26 (P.L. 2005, c. 271, s.2). Additional information on the process is available in Local Finance Notice 2006-1 (http://www.nj.gov/dca/divisions/dlgs/resources/lfns_2006.html). Please refer back to these instructions for the appropriate links, as the Local Finance Notices include links that are no longer operational.

1. The disclosure is required for all contracts in excess of \$17,500 that are **not awarded** pursuant to a “fair and open” process (N.J.S.A. 19:44A-20.7).
2. Due to the potential length of some contractor submissions, the public agency should consider allowing data to be submitted in electronic form (i.e., spreadsheet, pdf file, etc.). Submissions must be kept with the contract documents or in an appropriate computer file and be available for public access. **The form is worded to accept this alternate submission.** The text should be amended if electronic submission will not be allowed.
3. The submission must be **received from the contractor and** on file at least 10 days prior to award of the contract. Resolutions of award should reflect that the disclosure has been received and is on file.
4. The contractor must disclose contributions made to candidate and party committees covering a wide range of public agencies, including all public agencies that have elected officials in the county of the public agency, state legislative positions, and various state entities. The Division of Local Government Services recommends that contractors be provided a list of the affected agencies. This will assist contractors in determining the campaign and political committees of the officials and candidates affected by the disclosure.
 - a. The Division has prepared model disclosure forms for each county. They can be downloaded from the “County PCD Forms” link on the Pay-to-Play web site at <http://www.nj.gov/dca/divisions/dlgs/programs/lpcl.html#12>. They will be updated from time-to-time as necessary.
 - b. A public agency using these forms **should edit them to properly reflect the correct legislative district(s)**. As the forms are county-based, **they list all legislative districts** in each county. **Districts that do not represent the public agency should be removed from the lists.**
 - c. Some contractors may find it easier to provide a single list that covers all contributions, regardless of the county. These submissions are appropriate and should be accepted.
 - d. The form may be used “as-is”, subject to edits as described herein.
 - e. The “Contractor Instructions” sheet is intended to be provided with the form. It is recommended that the Instructions and the form be printed on the same piece of paper. The form notes that the Instructions are printed on the back of the form; where that is not the case, the text should be edited accordingly.
 - f. The form is a Word document and can be edited to meet local needs, and posted for download on web sites, used as an e-mail attachment, or provided as a printed document.
5. It is recommended that the contractor also complete a “Stockholder Disclosure Certification.” This will assist the local unit in its obligation to ensure that contractor did not make any prohibited contributions to the committees listed on the Business Entity Disclosure Certification in the 12 months prior to the contract (See Local Finance Notice 2006-7 for additional information on this obligation at http://www.nj.gov/dca/divisions/dlgs/resources/lfns_2006.html). A sample Certification form is part of this package and the instruction to complete it is included in the Contractor Instructions. NOTE: This section is not applicable to Boards of Education.

C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM

Contractor Instructions

Business entities (contractors) receiving contracts from a public agency that are NOT awarded pursuant to a “fair and open” process (defined at N.J.S.A. 19:44A-20.7) are subject to the provisions of P.L. 2005, c. 271, s.2 (N.J.S.A. 19:44A-20.26). This law provides that 10 days prior to the award of such a contract, the contractor shall disclose contributions to:

- any State, county, or municipal committee of a political party
- any legislative leadership committee*
- any continuing political committee (a.k.a., political action committee)
- any candidate committee of a candidate for, or holder of, an elective office:
 - of the public entity awarding the contract
 - of that county in which that public entity is located
 - of another public entity within that county
 - or of a legislative district in which that public entity is located or, when the public entity is a county, of any legislative district which includes all or part of the county

The disclosure must list reportable contributions to any of the committees that exceed \$300 per election cycle that were made during the 12 months prior to award of the contract. See N.J.S.A. 19:44A-8 and 19:44A-16 for more details on reportable contributions.

N.J.S.A. 19:44A-20.26 itemizes the parties from whom contributions must be disclosed when a business entity is not a natural person. This includes the following:

- individuals with an “interest” ownership or control of more than 10% of the profits or assets of a business entity or 10% of the stock in the case of a business entity that is a corporation for profit
- all principals, partners, officers, or directors of the business entity or their spouses
- any subsidiaries directly or indirectly controlled by the business entity
- IRS Code Section 527 New Jersey based organizations, directly or indirectly controlled by the business entity and filing as continuing political committees, (PACs).

When the business entity is a natural person, “a contribution by that person’s spouse or child, residing therewith, shall be deemed to be a contribution by the business entity.” [N.J.S.A. 19:44A-20.26(b)] The contributor must be listed on the disclosure.

Any business entity that fails to comply with the disclosure provisions shall be subject to a fine imposed by ELEC in an amount to be determined by the Commission which may be based upon the amount that the business entity failed to report.

The enclosed list of agencies is provided to assist the contractor in identifying those public agencies whose elected official and/or candidate campaign committees are affected by the disclosure requirement. It is the contractor’s responsibility to identify the specific committees to which contributions may have been made and need to be disclosed. The disclosed information may exceed the minimum requirement.

The enclosed form, a content-consistent facsimile, or an electronic data file containing the required details (along with a signed cover sheet) may be used as the contractor’s submission and is disclosable to the public under the Open Public Records Act.

The contractor must also complete the attached Stockholder Disclosure Certification. This will assist the agency in meeting its obligations under the law. **NOTE: This section does not apply to Board of Education contracts.**

* N.J.S.A. 19:44A-3(s): “The term “legislative leadership committee” means a committee established, authorized to be established, or designated by the President of the Senate, the Minority Leader of the Senate, the Speaker of the General Assembly or the Minority Leader of the General Assembly pursuant to section 16 of P.L.1993, c.65 (C.19:44A-10.1) for the purpose of receiving contributions and making expenditures.”


C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM
 Required Pursuant to N.J.S.A. 19:44A-20.26

This form or its permitted facsimile must be submitted to the local unit no later than 10 days prior to the award of the contract.

Part I – Vendor Information

Vendor Name:	ThunderCat Technology, LLC		
Address:	1925 Isaac Newton Square, Suite 180		
City:	Reston	State: VA	Zip: 20190

The undersigned being authorized to certify, hereby certifies that the submission provided herein represents compliance with the provisions of N.J.S.A. 19:44A-20.26 and as represented by the Instructions accompanying this form.

	Jean Kim	Contracts
Signature	Printed Name	Title

Part II – Contribution Disclosure

Disclosure requirement: Pursuant to N.J.S.A. 19:44A-20.26 this disclosure must include all reportable political contributions (more than \$300 per election cycle) over the 12 months prior to submission to the committees of the government entities listed on the form provided by the local unit.

Check here if disclosure is provided in electronic form

Contributor Name	Recipient Name	Date	Dollar Amount
			\$

Check here if the information is continued on subsequent page(s)

List of Agencies with Elected Officials Required for Political Contribution Disclosure
N.J.S.A. 19:44A-20.26

County Name:

State: Governor, and Legislative Leadership Committees

Legislative District #s:

State Senator and two members of the General Assembly per district.

County:

Freeholders

{County Executive}

County Clerk

Surrogate

Sheriff

Municipalities (Mayor and members of governing body, regardless of title):

**USERS SHOULD CREATE THEIR OWN FORM, OR DOWNLOAD
FROM THE PAY TO PLAY SECTION OF THE DLGS WEBSITE A
COUNTY-BASED, CUSTOMIZABLE FORM.**

STOCKHOLDER DISCLOSURE CERTIFICATION

Name of Business:

I certify that the list below contains the names and home addresses of all stockholders holding 10% or more of the issued and outstanding stock of the undersigned.

OR

I certify that no one stockholder owns 10% or more of the issued and outstanding stock of the undersigned.

Check the box that represents the type of business organization:

Partnership

Corporation

Sole Proprietorship

Limited Partnership

Limited Liability Corporation

Limited Liability Partnership

Subchapter S Corporation

Sign and notarize the form below, and, if necessary, complete the stockholder list below.

Stockholders:

Name:	Name:
Home Address:	Home Address:
Name:	Name:
Home Address:	Home Address:
Name:	Name:
Home Address:	Home Address:

Subscribed and sworn before me this ____ day of _____, 2__.	_____
(Notary Public)	(Affiant)
My Commission expires:	_____
	(Print name & title of affiant)
	(Corporate Seal)

Certification of Non-Involvement in Prohibited Activities in Iran

Pursuant to N.J.S.A. 52:32-58, Offerors must certify that neither the Offeror, nor any of its parents, subsidiaries, and/or affiliates (as defined in N.J.S.A. 52:32 – 56(e) (3)), is listed on the Department of the Treasury’s List of Persons or Entities Engaging in Prohibited Investment Activities in Iran and that neither is involved in any of the investment activities set forth in N.J.S.A. 52:32 – 56(f).

Offerors wishing to do business in New Jersey through this contract must fill out the Certification of Non-Involvement in Prohibited Activities in Iran here:

http://www.state.nj.us/humanservices/dfd/info/standard/fdc/disclosure_investmentact.pdf.

Offerors should submit the above form completed with their proposal.

DOC #7

**NEW JERSEY BUSINESS REGISTRATION CERTIFICATE
(N.J.S.A. 52:32-44)**

Offerors wishing to do business in New Jersey must submit their State Division of Revenue issued Business Registration Certificate with their proposal here. Failure to do so will disqualify the Offeror from offering products or services in New Jersey through any resulting contract.

<http://www.state.nj.us/treasury/revenue/forms/njreg.pdf>

EXHIBIT H ADVERTISING COMPLIANCE REQUIREMENT

Pursuant to certain state notice provisions, including but not limited to Oregon Revised Statutes Chapter 279A.220, the following public agencies and political subdivisions of the referenced public agencies are eligible to register with OMNIA Partners and access the Master Agreement contract award made pursuant to this solicitation, and are hereby given notice of the foregoing request for proposals for purposes of complying with the procedural requirements of said statutes:

Nationwide:

State of Alabama	State of Hawaii	State of Massachusetts	State of New Mexico	State of South Dakota
State of Alaska	State of Idaho	State of Michigan	State of New York	State of Tennessee
State of Arizona	State of Illinois	State of Minnesota	State of North Carolina	State of Texas
State of Arkansas	State of Indiana	State of Mississippi	State of North Dakota	State of Utah
State of California	State of Iowa	State of Missouri	State of Ohio	State of Vermont
State of Colorado	State of Kansas	State of Montana	State of Oklahoma	State of Virginia
State of Connecticut	State of Kentucky	State of Nebraska	State of Oregon	State of Washington
State of Delaware	State of Louisiana	State of Nevada	State of Pennsylvania	State of West Virginia
State of Florida	State of Maine	State of New Hampshire	State of Rhode Island	State of Wisconsin
State of Georgia	State of Maryland	State of New Jersey	State of South Carolina	State of Wyoming
District of Columbia				

Lists of political subdivisions and local governments in the above referenced states / districts may be found at http://www.usa.gov/Agencies/State_and_Territories.shtml and <https://www.usa.gov/local-governments>.

Certain Public Agencies and Political Subdivisions:

**CITIES, TOWNS, VILLAGES AND BOROUGHS
INCLUDING BUT NOT LIMITED TO:**

BAKER CITY GOLF COURSE, OR
 CITY OF ADAIR VILLAGE, OR
 CITY OF ASHLAND, OR
 CITY OF AUMSVILLE, OR
 CITY OF AURORA, OR
 CITY OF BAKER, OR
 CITY OF BATON ROUGE, LA
 CITY OF BEAVERTON, OR
 CITY OF BEND, OR
 CITY OF BOARDMAN, OR
 CITY OF BONANAZA, OR
 CITY OF BOSSIER CITY, LA
 CITY OF BROOKINGS, OR
 CITY OF BURNS, OR
 CITY OF CANBY, OR
 CITY OF CANYONVILLE, OR
 CITY OF CLATSKANIE, OR
 CITY OF COBURG, OR
 CITY OF CONDON, OR
 CITY OF COQUILLE, OR
 CITY OF CORVALLI, OR
 CITY OF CORVALLIS PARKS AND RECREATION
 DEPARTMENT, OR
 CITY OF COTTAGE GROVE, OR
 CITY OF DONALD, OR
 CITY OF EUGENE, OR
 CITY OF FOREST GROVE, OR
 CITY OF GOLD HILL, OR
 CITY OF GRANTS PASS, OR
 CITY OF GRESHAM, OR
 CITY OF HILLSBORO, OR
 CITY OF INDEPENDENCE, OR
 CITY AND COUNTY OF HONOLULU, HI

CITY OF KENNER, LA
 CITY OF LA GRANDE, OR
 CITY OF LAFAYETTE, LA
 CITY OF LAKE CHARLES, OR
 CITY OF LEBANON, OR
 CITY OF MCMINNVILLE, OR
 CITY OF MEDFORD, OR
 CITY OF METAIRIE, LA
 CITY OF MILL CITY, OR
 CITY OF MILWAUKIE, OR
 CITY OF MONROE, LA
 CITY OF MOSIER, OR
 CITY OF NEW ORLEANS, LA
 CITY OF NORTH PLAINS, OR
 CITY OF OREGON CITY, OR
 CITY OF PILOT ROCK, OR
 CITY OF PORTLAND, OR
 CITY OF POWERS, OR
 CITY OF PRINEVILLE, OR
 CITY OF REDMOND, OR
 CITY OF REEDSPORT, OR
 CITY OF RIDDLE, OR
 CITY OF ROGUE RIVER, OR
 CITY OF ROSEBURG, OR
 CITY OF SALEM, OR
 CITY OF SANDY, OR
 CITY OF SCAPPOOSE, OR
 CITY OF SHADY COVE, OR
 CITY OF SHERWOOD, OR
 CITY OF SHREVEPORT, LA
 CITY OF SILVERTON, OR
 CITY OF SPRINGFIELD, OR
 CITY OF ST. HELENS, OR
 CITY OF ST. PAUL, OR
 CITY OF SULPHUR, LA

CITY OF TIGARD, OR
CITY OF TROUTDALE, OR
CITY OF TUALATIN, OR
CITY OF WALKER, LA
CITY OF WARRENTON, OR
CITY OF WEST LINN, OR
CITY OF WILSONVILLE, OR
CITY OF WINSTON, OR
CITY OF WOODBURN, OR
LEAGUE OF OREGON CITIES
THE CITY OF HAPPY VALLEY OREGON
ALPINE, UT
ALTA, UT
ALTAMONT, UT
ALTON, UT
AMALGA, UT
AMERICAN FORK CITY, UT
ANNABELLA, UT
ANTIMONY, UT
APPLE VALLEY, UT
AURORA, UT
BALLARD, UT
BEAR RIVER CITY, UT
BEAVER, UT
BICKNELL, UT
BIG WATER, UT
BLANDING, UT
BLUFFDALE, UT
BOULDER, UT
CITY OF BOUNTIFUL, UT
BRIAN HEAD, UT
BRIGHAM CITY CORPORATION, UT
BRYCE CANYON CITY, UT
CANNONVILLE, UT
CASTLE DALE, UT
CASTLE VALLEY, UT
CITY OF CEDAR CITY, UT
CEDAR FORT, UT
CITY OF CEDAR HILLS, UT
CENTERFIELD, UT
CENTERVILLE CITY CORPORATION, UT
CENTRAL VALLEY, UT
CHARLESTON, UT
CIRCLEVILLE, UT
CLARKSTON, UT
CLAWSON, UT
CLEARFIELD, UT
CLEVELAND, UT
CLINTON CITY CORPORATION, UT
COALVILLE, UT
CORINNE, UT
CORNISH, UT
COTTONWOOD HEIGHTS, UT
DANIEL, UT
DELTA, UT
DEWEYVILLE, UT
DRAPER CITY, UT
DUCHESNE, UT
EAGLE MOUNTAIN, UT
EAST CARBON, UT
ELK RIDGE, UT
ELMO, UT
ELSNORE, UT
ELWOOD, UT
EMERY, UT
ENOCH, UT

ENTERPRISE, UT
EPHRAIM, UT
ESCALANTE, UT
EUREKA, UT
FAIRFIELD, UT
FAIRVIEW, UT
FARMINGTON, UT
FARR WEST, UT
FAYETTE, UT
FERRON, UT
FIELDING, UT
FILLMORE, UT
FOUNTAIN GREEN, UT
FRANCIS, UT
FRUIT HEIGHTS, UT
GARDEN CITY, UT
GARLAND, UT
GENOLA, UT
GLENDALE, UT
GLENWOOD, UT
GOSHEN, UT
GRANTSVILLE, UT
GREEN RIVER, UT
GUNNISON, UT
HANKSVILLE, UT
HARRISVILLE, UT
HATCH, UT
HEBER CITY CORPORATION, UT
HELPER, UT
HENEFER, UT
HENRIEVILLE, UT
HERRIMAN, UT
HIDEOUT, UT
HIGHLAND, UT
HILDALE, UT
HINCKLEY, UT
HOLDEN, UT
HOLLADAY, UT
HONEYVILLE, UT
HOOPER, UT
HOWELL, UT
HUNTINGTON, UT
HUNTSVILLE, UT
CITY OF HURRICANE, UT
HYDE PARK, UT
HYRUM, UT
INDEPENDENCE, UT
IVINS, UT
JOSEPH, UT
JUNCTION, UT
KAMAS, UT
KANAB, UT
KANARRAVILLE, UT
KANOSH, UT
KAYSVILLE, UT
KINGSTON, UT
KOOSHAREM, UT
LAKETOWN, UT
LA VERKIN, UT
LAYTON, UT
LEAMINGTON, UT
LEEDS, UT
LEHI CITY CORPORATION, UT
LEVAN, UT
LEWISTON, UT
LINDON, UT

LOA, UT
LOGAN CITY, UT
LYMAN, UT
LYNNNDYL, UT
MANILA, UT
MANTI, UT
MANTUA, UT
MAPLETON, UT
MARRIOTT-SLATERVILLE, UT
MARYSVALE, UT
MAYFIELD, UT
MEADOW, UT
MENDON, UT
MIDVALE CITY INC., UT
MIDWAY, UT
MILFORD, UT
MILLVILLE, UT
MINERSVILLE, UT
MOAB, UT
MONA, UT
MONROE, UT
CITY OF MONTICELLO, UT
MORGAN, UT
MORONI, UT
MOUNT PLEASANT, UT
MURRAY CITY CORPORATION, UT
MYTON, UT
NAPLES, UT
NEPHI, UT
NEW HARMONY, UT
NEWTON, UT
NIBLEY, UT
NORTH LOGAN, UT
NORTH OGDEN, UT
NORTH SALT LAKE CITY, UT
OAK CITY, UT
OAKLEY, UT
OGDEN CITY CORPORATION, UT
OPHIR, UT
ORANGEVILLE, UT
ORDERVILLE, UT
OREM, UT
PANGUITCH, UT
PARADISE, UT
PARAGONAH, UT
PARK CITY, UT
PAROWAN, UT
PAYSON, UT
PERRY, UT
PLAIN CITY, UT
PLEASANT GROVE CITY, UT
PLEASANT VIEW, UT
PLYMOUTH, UT
PORTAGE, UT
PRICE, UT
PROVIDENCE, UT
PROVO, UT
RANDOLPH, UT
REDMOND, UT
RICHFIELD, UT
RICHMOND, UT
RIVERDALE, UT
RIVER HEIGHTS, UT
RIVERTON CITY, UT
ROCKVILLE, UT
ROCKY RIDGE, UT

ROOSEVELT CITY CORPORATION, UT
ROY, UT
RUSH VALLEY, UT
CITY OF ST. GEORGE, UT
SALEM, UT
SALINA, UT
SALT LAKE CITY CORPORATION, UT
SANDY, UT
SANTA CLARA, UT
SANTAQUIN, UT
SARATOGA SPRINGS, UT
SCIPIO, UT
SCOFIELD, UT
SIGURD, UT
SMITHFIELD, UT
SNOWVILLE, UT
CITY OF SOUTH JORDAN, UT
SOUTH OGDEN, UT
CITY OF SOUTH SALT LAKE, UT
SOUTH WEBER, UT
SPANISH FORK, UT
SPRING CITY, UT
SPRINGDALE, UT
SPRINGVILLE, UT
STERLING, UT
STOCKTON, UT
SUNNYSIDE, UT
SUNSET CITY CORP, UT
SYRACUSE, UT
TABIONA, UT
CITY OF TAYLORSVILLE, UT
TOOELE CITY CORPORATION, UT
TOQUERVILLE, UT
TORREY, UT
TREMONTON CITY, UT
TRENTON, UT
TROPIC, UT
UINTAH, UT
VERNAL CITY, UT
VERNON, UT
VINEYARD, UT
VIRGIN, UT
WALES, UT
WALLSBURG, UT
WASHINGTON CITY, UT
WASHINGTON TERRACE, UT
WELLINGTON, UT
WELLSVILLE, UT
WENDOVER, UT
WEST BOUNTIFUL, UT
WEST HAVEN, UT
WEST JORDAN, UT
WEST POINT, UT
WEST VALLEY CITY, UT
WILLARD, UT
WOODLAND HILLS, UT
WOODRUFF, UT
WOODS CROSS, UT

COUNTIES AND PARISHES INCLUDING BUT NOT LIMITED TO:

ASCENSION PARISH, LA
ASCENSION PARISH, LA, CLEAR OF COURT
CADDO PARISH, LA
CALCASIEU PARISH, LA
CALCASIEU PARISH SHERIFF'S OFFICE, LA

CITY AND COUNTY OF HONOLULU, HI
CLACKAMAS COUNTY, OR
CLACKAMAS COUNTY DEPT OF TRANSPORTATION,
OR
CLATSOP COUNTY, OR
COLUMBIA COUNTY, OR
COOS COUNTY, OR
COOS COUNTY HIGHWAY DEPARTMENT, OR
COUNTY OF HAWAII, OR
CROOK COUNTY, OR
CROOK COUNTY ROAD DEPARTMENT, OR
CURRY COUNTY, OR
DESCHUTES COUNTY, OR
DOUGLAS COUNTY, OR
EAST BATON ROUGE PARISH, LA
GILLIAM COUNTY, OR
GRANT COUNTY, OR
HARNEY COUNTY, OR
HARNEY COUNTY SHERIFFS OFFICE, OR
HAWAII COUNTY, HI
HOOD RIVER COUNTY, OR
JACKSON COUNTY, OR
JEFFERSON COUNTY, OR
JEFFERSON PARISH, LA
JOSEPHINE COUNTY GOVERNMENT, OR
LAFAYETTE CONSOLIDATED GOVERNMENT, LA
LAFAYETTE PARISH, LA
LAFAYETTE PARISH CONVENTION & VISITORS
COMMISSION
LAFOURCHE PARISH, LA
KAUAI COUNTY, HI
KLAMATH COUNTY, OR
LAKE COUNTY, OR
LANE COUNTY, OR
LINCOLN COUNTY, OR
LINN COUNTY, OR
LIVINGSTON PARISH, LA
MALHEUR COUNTY, OR
MAUI COUNTY, HI
MARION COUNTY, SALEM, OR
MORROW COUNTY, OR
MULTNOMAH COUNTY, OR
MULTNOMAH COUNTY BUSINESS AND
COMMUNITY SERVICES, OR
MULTNOMAH COUNTY SHERIFFS OFFICE, OR
MULTNOMAH LAW LIBRARY, OR
ORLEANS PARISH, LA
PLAQUEMINES PARISH, LA
POLK COUNTY, OR
RAPIDES PARISH, LA
SAINT CHARLES PARISH, LA
SAINT CHARLES PARISH PUBLIC SCHOOLS, LA
SAINT LANDRY PARISH, LA
SAINT TAMMANY PARISH, LA
SHERMAN COUNTY, OR
TERREBONNE PARISH, LA
TILLAMOOK COUNTY, OR
TILLAMOOK COUNTY SHERIFF'S OFFICE, OR
TILLAMOOK COUNTY GENERAL HOSPITAL, OR
UMATILLA COUNTY, OR
UNION COUNTY, OR
WALLOWA COUNTY, OR
WASCO COUNTY, OR
WASHINGTON COUNTY, OR
WEST BATON ROUGE PARISH, LA
WHEELER COUNTY, OR

YAMHILL COUNTY, OR
COUNTY OF BOX ELDER, UT
COUNTY OF CACHE, UT
COUNTY OF RICH, UT
COUNTY OF WEBER, UT
COUNTY OF MORGAN, UT
COUNTY OF DAVIS, UT
COUNTY OF SUMMIT, UT
COUNTY OF DAGGETT, UT
COUNTY OF SALT LAKE, UT
COUNTY OF TOOELE, UT
COUNTY OF UTAH, UT
COUNTY OF WASATCH, UT
COUNTY OF DUCHESNE, UT
COUNTY OF Uintah, UT
COUNTY OF CARBON, UT
COUNTY OF SANPETE, UT
COUNTY OF JUAB, UT
COUNTY OF MILLARD, UT
COUNTY OF SEVIER, UT
COUNTY OF EMERY, UT
COUNTY OF GRAND, UT
COUNTY OF BEVER, UT
COUNTY OF PIUTE, UT
COUNTY OF WAYNE, UT
COUNTY OF SAN JUAN, UT
COUNTY OF GARFIELD, UT
COUNTY OF KANE, UT
COUNTY OF IRON, UT
COUNTY OF WASHINGTON, UT

**OTHER AGENCIES INCLUDING ASSOCIATIONS,
BOARDS, DISTRICTS, COMMISSIONS, COUNCILS,
PUBLIC CORPORATIONS, PUBLIC DEVELOPMENT
AUTHORITIES, RESERVATIONS AND UTILITIES
INCLUDING BUT NOT LIMITED TO:**

ADAIR R.F.P.D., OR
ADEL WATER IMPROVEMENT DISTRICT, OR
ADRIAN R.F.P.D., OR
AGNESS COMMUNITY LIBRARY, OR
AGNESS-ILLAHE R.F.P.D., OR
AGRICULTURE EDUCATION SERVICE EXTENSION
DISTRICT, OR
ALDER CREEK-BARLOW WATER DISTRICT NO. 29,
OR
ALFALFA FIRE DISTRICT, OR
ALSEA R.F.P.D., OR
ALSEA RIVIERA WATER IMPROVEMENT DISTRICT,
OR
AMITY FIRE DISTRICT, OR
ANTELOPE MEADOWS SPECIAL ROAD DISTRICT, OR
APPLE ROGUE DISTRICT IMPROVEMENT COMPANY,
OR
APPLEGATE VALLEY R.F.P.D. #9, OR
ARCH CAPE DOMESTIC WATER SUPPLY DISTRICT,
OR
ARCH CAPE SANITARY DISTRICT, OR
ARNOLD IRRIGATION DISTRICT, OR
ASH CREEK WATER CONTROL DISTRICT, OR
ATHENA CEMETERY MAINTENANCE DISTRICT, OR
AUMSVILLE R.F.P.D., OR
AURORA R.F.P.D., OR
AZALEA R.F.P.D., OR
BADGER IMPROVEMENT DISTRICT, OR
BAILEY-SPENCER R.F.P.D., OR
BAKER COUNTY LIBRARY DISTRICT, OR

BAKER R.F.P.D., OR
BAKER RIVERTON ROAD DISTRICT, OR
BAKER VALLEY IRRIGATION DISTRICT, OR
BAKER VALLEY S.W.C.D., OR
BAKER VALLEY VECTOR CONTROL DISTRICT, OR
BANDON CRANBERRY WATER CONTROL DISTRICT,
OR
BANDON R.F.P.D., OR
BANKS FIRE DISTRICT, OR
BANKS FIRE DISTRICT #13, OR
BAR L RANCH ROAD DISTRICT, OR
BARLOW WATER IMPROVEMENT DISTRICT, OR
BASIN AMBULANCE SERVICE DISTRICT, OR
BASIN TRANSIT SERVICE TRANSPORTATION
DISTRICT, OR
BATON ROUGE WATER COMPANY
BAY AREA HEALTH DISTRICT, OR
BAYSHORE SPECIAL ROAD DISTRICT, OR
BEAR VALLEY SPECIAL ROAD DISTRICT, OR
BEAVER CREEK WATER CONTROL DISTRICT, OR
BEAVER DRAINAGE IMPROVEMENT COMPANY,
INC., OR
BEAVER SLOUGH DRAINAGE DISTRICT, OR
BEAVER SPECIAL ROAD DISTRICT, OR
BEAVER WATER DISTRICT, OR
BELLE MER S.I.G.L. TRACTS SPECIAL ROAD
DISTRICT, OR
BEND METRO PARK AND RECREATION DISTRICT
BENTON S.W.C.D., OR
BERNDT SUBDIVISION WATER IMPROVEMENT
DISTRICT, OR
BEVERLY BEACH WATER DISTRICT, OR
BIENVILLE PARISH FIRE PROTECTION DISTRICT 6,
LA
BIG BEND IRRIGATION DISTRICT, OR
BIGGS SERVICE DISTRICT, OR
BLACK BUTTE RANCH DEPARTMENT OF POLICE
SERVICES, OR
BLACK BUTTE RANCH R.F.P.D., OR
BLACK MOUNTAIN WATER DISTRICT, OR
BLODGETT-SUMMIT R.F.P.D., OR
BLUE MOUNTAIN HOSPITAL DISTRICT, OR
BLUE MOUNTAIN TRANSLATOR DISTRICT, OR
BLUE RIVER PARK & RECREATION DISTRICT, OR
BLUE RIVER WATER DISTRICT, OR
BLY R.F.P.D., OR
BLY VECTOR CONTROL DISTRICT, OR
BLY WATER AND SANITARY DISTRICT, OR
BOARDMAN CEMETERY MAINTENANCE DISTRICT,
OR
BOARDMAN PARK AND RECREATION DISTRICT
BOARDMAN R.F.P.D., OR
BONANZA BIG SPRINGS PARK & RECREATION
DISTRICT, OR
BONANZA MEMORIAL PARK CEMETERY DISTRICT,
OR
BONANZA R.F.P.D., OR
BONANZA-LANGELL VALLEY VECTOR CONTROL
DISTRICT, OR
BORING WATER DISTRICT #24, OR
BOULDER CREEK RETREAT SPECIAL ROAD
DISTRICT, OR
BRIDGE R.F.P.D., OR
BROOKS COMMUNITY SERVICE DISTRICT, OR
BROWNSVILLE R.F.P.D., OR
BUELL-RED PRAIRIE WATER DISTRICT, OR

BUNKER HILL R.F.P.D. #1, OR
BUNKER HILL SANITARY DISTRICT, OR
BURLINGTON WATER DISTRICT, OR
BURNT RIVER IRRIGATION DISTRICT, OR
BURNT RIVER S.W.C.D., OR
CALAPOOIA R.F.P.D., OR
CAMAS VALLEY R.F.P.D., OR
CAMELLIA PARK SANITARY DISTRICT, OR
CAMMANN ROAD DISTRICT, OR
CAMP SHERMAN ROAD DISTRICT, OR
CANBY AREA TRANSIT, OR
CANBY R.F.P.D. #62, OR
CANBY UTILITY BOARD, OR
CANNON BEACH R.F.P.D., OR
CANYONVILLE SOUTH UMPQUA FIRE DISTRICT, OR
CAPE FERRELO R.F.P.D., OR
CAPE FOULWEATHER SANITARY DISTRICT, OR
CARLSON PRIMROSE SPECIAL ROAD DISTRICT, OR
CARMEL BEACH WATER DISTRICT, OR
CASCADE VIEW ESTATES TRACT 2, OR
CEDAR CREST SPECIAL ROAD DISTRICT, OR
CEDAR TRAILS SPECIAL ROAD DISTRICT, OR
CEDAR VALLEY - NORTH BANK R.F.P.D., OR
CENTRAL CASCADES FIRE AND EMS, OR
CENTRAL CITY ECONOMIC OPPORTUNITY CORP, LA
CENTRAL LINCOLN P.U.D., OR
CENTRAL OREGON COAST FIRE & RESCUE
DISTRICT, OR
CENTRAL OREGON INTERGOVERNMENTAL
COUNCIL
CENTRAL OREGON IRRIGATION DISTRICT, OR
CHAPARRAL WATER CONTROL DISTRICT, OR
CHARLESTON FIRE DISTRICT, OR
CHARLESTON SANITARY DISTRICT, OR
CHARLOTTE ANN WATER DISTRICT, OR
CHEHALEM PARK & RECREATION DISTRICT, OR
CHEHALEM PARK AND RECREATION DISTRICT
CHEMULT R.F.P.D., OR
CHENOWITH WATER P.U.D., OR
CHERRIOTS, OR
CHETCO COMMUNITY PUBLIC LIBRARY DISTRICT,
OR
CHILOQUIN VECTOR CONTROL DISTRICT, OR
CHILOQUIN-AGENCY LAKE R.F.P.D., OR
CHINOOK DRIVE SPECIAL ROAD DISTRICT, OR
CHR DISTRICT IMPROVEMENT COMPANY, OR
CHRISTMAS VALLEY DOMESTIC WATER DISTRICT,
OR
CHRISTMAS VALLEY PARK & RECREATION
DISTRICT, OR
CHRISTMAS VALLEY R.F.P.D., OR
CITY OF BOGALUSA SCHOOL BOARD, LA
CLACKAMAS COUNTY FIRE DISTRICT #1, OR
CLACKAMAS COUNTY SERVICE DISTRICT #1, OR
CLACKAMAS COUNTY VECTOR CONTROL
DISTRICT, OR
CLACKAMAS RIVER WATER
CLACKAMAS RIVER WATER, OR
CLACKAMAS S.W.C.D., OR
CLATSKANIE DRAINAGE IMPROVEMENT
COMPANY, OR
CLATSKANIE LIBRARY DISTRICT, OR
CLATSKANIE P.U.D., OR
CLATSKANIE PARK & RECREATION DISTRICT, OR
CLATSKANIE PEOPLE'S UTILITY DISTRICT
CLATSKANIE R.F.P.D., OR

CLATSOP CARE CENTER HEALTH DISTRICT, OR
CLATSOP COUNTY S.W.C.D., OR
CLATSOP DRAINAGE IMPROVEMENT COMPANY #15,
INC., OR
CLEAN WATER SERVICES
CLEAN WATER SERVICES, OR
CLOVERDALE R.F.P.D., OR
CLOVERDALE SANITARY DISTRICT, OR
CLOVERDALE WATER DISTRICT, OR
COALEDO DRAINAGE DISTRICT, OR
COBURG FIRE DISTRICT, OR
COLESTIN RURAL FIRE DISTRICT, OR
COLTON R.F.P.D., OR
COLTON WATER DISTRICT #11, OR
COLUMBIA 911 COMMUNICATIONS DISTRICT, OR
COLUMBIA COUNTY 4-H & EXTENSION SERVICE
DISTRICT, OR
COLUMBIA DRAINAGE VECTOR CONTROL, OR
COLUMBIA IMPROVEMENT DISTRICT, OR
COLUMBIA R.F.P.D., OR
COLUMBIA RIVER FIRE & RESCUE, OR
COLUMBIA RIVER PUD, OR
COLUMBIA S.W.C.D., OR
COLUMBIA S.W.C.D., OR
CONFEDERATED TRIBES OF THE UMATILLA INDIAN
RESERVATION
COOS COUNTY AIRPORT DISTRICT, OR
COOS COUNTY AIRPORT DISTRICT, OR
COOS COUNTY AREA TRANSIT SERVICE DISTRICT,
OR
COOS COUNTY AREA TRANSIT SERVICE DISTRICT,
OR
COOS FOREST PROTECTIVE ASSOCIATION
COOS S.W.C.D., OR
COQUILLE R.F.P.D., OR
COQUILLE VALLEY HOSPITAL DISTRICT, OR
CORBETT WATER DISTRICT, OR
CORNELIUS R.F.P.D., OR
CORP RANCH ROAD WATER IMPROVEMENT, OR
CORVALLIS R.F.P.D., OR
COUNTRY CLUB ESTATES SPECIAL WATER
DISTRICT, OR
COUNTRY CLUB WATER DISTRICT, OR
COUNTRY ESTATES ROAD DISTRICT, OR
COVE CEMETERY MAINTENANCE DISTRICT, OR
COVE ORCHARD SEWER SERVICE DISTRICT, OR
COVE R.F.P.D., OR
CRESCENT R.F.P.D., OR
CRESCENT SANITARY DISTRICT, OR
CRESCENT WATER SUPPLY AND IMPROVEMENT
DISTRICT, OR
CROOK COUNTY AGRICULTURE EXTENSION
SERVICE DISTRICT, OR
CROOK COUNTY CEMETERY DISTRICT, OR
CROOK COUNTY FIRE AND RESCUE, OR
CROOK COUNTY PARKS & RECREATION DISTRICT,
OR
CROOK COUNTY S.W.C.D., OR
CROOK COUNTY VECTOR CONTROL DISTRICT, OR
CROOKED RIVER RANCH R.F.P.D., OR
CROOKED RIVER RANCH SPECIAL ROAD DISTRICT,
OR
CRYSTAL SPRINGS WATER DISTRICT, OR
CURRY COUNTY 4-H & EXTENSION SERVICE
DISTRICT, OR

CURRY COUNTY PUBLIC TRANSIT SERVICE
DISTRICT, OR
CURRY COUNTY S.W.C.D., OR
CURRY HEALTH DISTRICT, OR
CURRY PUBLIC LIBRARY DISTRICT, OR
DALLAS CEMETERY DISTRICT #4, OR
DARLEY DRIVE SPECIAL ROAD DISTRICT, OR
DAVID CROCKETT STEAM FIRE COMPANY #1, LA
DAYS CREEK R.F.P.D., OR
DAYTON FIRE DISTRICT, OR
DEAN MINARD WATER DISTRICT, OR
DEE IRRIGATION DISTRICT, OR
DEER ISLAND DRAINAGE IMPROVEMENT
COMPANY, OR
DELL BROGAN CEMETERY MAINTENANCE
DISTRICT, OR
DEPOE BAY R.F.P.D., OR
DESCHUTES COUNTY 911 SERVICE DISTRICT, OR
DESCHUTES COUNTY R.F.P.D. #2, OR
DESCHUTES PUBLIC LIBRARY DISTRICT, OR
DESCHUTES S.W.C.D., OR
DESCHUTES VALLEY WATER DISTRICT, OR
DEVILS LAKE WATER IMPROVEMENT DISTRICT, OR
DEXTER R.F.P.D., OR
DEXTER SANITARY DISTRICT, OR
DORA-SITKUM R.F.P.D., OR
DOUGLAS COUNTY FIRE DISTRICT #2, OR
DOUGLAS S.W.C.D., OR
DRAKES CROSSING R.F.P.D., OR
DRRH SPECIAL ROAD DISTRICT #6, OR
DRY GULCH DITCH DISTRICT IMPROVEMENT
COMPANY, OR
DUFUR RECREATION DISTRICT, OR
DUMBECK LANE DOMESTIC WATER SUPPLY, OR
DUNDEE R.F.P.D., OR
DURKEE COMMUNITY BUILDING PRESERVATION
DISTRICT, OR
EAGLE POINT IRRIGATION DISTRICT, OR
EAGLE VALLEY CEMETERY MAINTENANCE
DISTRICT, OR
EAGLE VALLEY R.F.P.D., OR
EAGLE VALLEY S.W.C.D., OR
EAST FORK IRRIGATION DISTRICT, OR
EAST MULTNOMAH S.W.C.D., OR
EAST SALEM SERVICE DISTRICT, OR
EAST UMATILLA CHEMICAL CONTROL DISTRICT,
OR
EAST UMATILLA COUNTY AMBULANCE AREA
HEALTH DISTRICT, OR
EAST UMATILLA COUNTY R.F.P.D., OR
EAST VALLEY WATER DISTRICT, OR
ELGIN COMMUNITY PARKS & RECREATION
DISTRICT, OR
ELGIN HEALTH DISTRICT, OR
ELGIN R.F.P.D., OR
ELKTON ESTATES PHASE II SPECIAL ROAD
DISTRICT, OR
ELKTON R.F.P.D., OR
EMERALD P.U.D., OR
ENTERPRISE IRRIGATION DISTRICT, OR
ESTACADA CEMETERY MAINTENANCE DISTRICT,
OR
ESTACADA R.F.P.D. #69, OR
EUGENE R.F.P.D. # 1, OR
EUGENE WATER AND ELECTRIC BOARD
EVANS VALLEY FIRE DISTRICT #6, OR

FAIR OAKS R.F.P.D., OR
FAIRVIEW R.F.P.D., OR
FAIRVIEW WATER DISTRICT, OR
FALCON HEIGHTS WATER AND SEWER, OR
FALCON-COVE BEACH WATER DISTRICT, OR
FALL RIVER ESTATES SPECIAL ROAD DISTRICT, OR
FARGO INTERCHANGE SERVICE DISTRICT, OR
FARMERS IRRIGATION DISTRICT, OR
FAT ELK DRAINAGE DISTRICT, OR
FERN RIDGE PUBLIC LIBRARY DISTRICT, OR
FERN VALLEY ESTATES IMPROVEMENT DISTRICT,
OR
FOR FAR ROAD DISTRICT, OR
FOREST GROVE R.F.P.D., OR
FOREST VIEW SPECIAL ROAD DISTRICT, OR
FORT ROCK-SILVER LAKE S.W.C.D., OR
FOUR RIVERS VECTOR CONTROL DISTRICT, OR
FOX CEMETERY MAINTENANCE DISTRICT, OR
GARDINER R.F.P.D., OR
GARDINER SANITARY DISTRICT, OR
GARIBALDI R.F.P.D., OR
GASTON R.F.P.D., OR
GATES R.F.P.D., OR
GEARHART R.F.P.D., OR
GILLIAM S.W.C.D., OR
GLENDALE AMBULANCE DISTRICT, OR
GLENDALE R.F.P.D., OR
GLENEDEN BEACH SPECIAL ROAD DISTRICT, OR
GLENEDEN SANITARY DISTRICT, OR
GLENWOOD WATER DISTRICT, OR
GLIDE - IDLEYLD SANITARY DISTRICT, OR
GLIDE R.F.P.D., OR
GOLD BEACH - WEDDERBURN R.F.P.D., OR
GOLD HILL IRRIGATION DISTRICT, OR
GOLDFINCH ROAD DISTRICT, OR
GOSHEN R.F.P.D., OR
GOVERNMENT CAMP ROAD DISTRICT, OR
GOVERNMENT CAMP SANITARY DISTRICT, OR
GRAND PRAIRIE WATER CONTROL DISTRICT, OR
GRAND RONDE SANITARY DISTRICT, OR
GRANT COUNTY TRANSPORTATION DISTRICT, OR
GRANT S.W.C.D., OR
GRANTS PASS IRRIGATION DISTRICT, OR
GREATER BOWEN VALLEY R.F.P.D., OR
GREATER ST. HELENS PARK & RECREATION
DISTRICT, OR
GREATER TOLEDO POOL RECREATION DISTRICT,
OR
GREEN KNOLLS SPECIAL ROAD DISTRICT, OR
GREEN SANITARY DISTRICT, OR
GREENACRES R.F.P.D., OR
GREENBERRY IRRIGATION DISTRICT, OR
GREENSPRINGS RURAL FIRE DISTRICT, OR
HAHLEN ROAD SPECIAL DISTRICT, OR
HAINES CEMETERY MAINTENANCE DISTRICT, OR
HAINES FIRE PROTECTION DISTRICT, OR
HALSEY-SHEDD R.F.P.D., OR
HAMLET R.F.P.D., OR
HARBOR R.F.P.D., OR
HARBOR SANITARY DISTRICT, OR
HARBOR WATER P.U.D., OR
HARNEY COUNTY HEALTH DISTRICT, OR
HARNEY S.W.C.D., OR
HARPER SOUTH SIDE IRRIGATION DISTRICT, OR
HARRISBURG FIRE AND RESCUE, OR
HAUSER R.F.P.D., OR

HAZELDELL RURAL FIRE DISTRICT, OR
HEBO JOINT WATER-SANITARY AUTHORITY, OR
HECETA WATER P.U.D., OR
HELIX CEMETERY MAINTENANCE DISTRICT #4, OR
HELIX PARK & RECREATION DISTRICT, OR
HELIX R.F.P.D. #7-411, OR
HEPPNER CEMETERY MAINTENANCE DISTRICT, OR
HEPPNER R.F.P.D., OR
HEPPNER WATER CONTROL DISTRICT, OR
HEREFORD COMMUNITY HALL RECREATION
DISTRICT, OR
HERMISTON CEMETERY DISTRICT, OR
HERMISTON IRRIGATION DISTRICT, OR
HIDDEN VALLEY MOBILE ESTATES IMPROVEMENT
DISTRICT, OR
HIGH DESERT PARK & RECREATION DISTRICT, OR
HIGHLAND SUBDIVISION WATER DISTRICT, OR
HONOLULU INTERNATIONAL AIRPORT
HOOD RIVER COUNTY LIBRARY DISTRICT, OR
HOOD RIVER COUNTY TRANSPORTATION DISTRICT,
OR
HOOD RIVER S.W.C.D., OR
HOOD RIVER VALLEY PARKS & RECREATION
DISTRICT, OR
HOODLAND FIRE DISTRICT #74
HOODLAND FIRE DISTRICT #74, OR
HORSEFLY IRRIGATION DISTRICT, OR
HOSKINS-KINGS VALLEY R.F.P.D., OR
HOUSING AUTHORITY OF PORTLAND
HUBBARD R.F.P.D., OR
HUDSON BAY DISTRICT IMPROVEMENT COMPANY,
OR
I N (KAY) YOUNG DITCH DISTRICT IMPROVEMENT
COMPANY, OR
ICE FOUNTAIN WATER DISTRICT, OR
IDAHO POINT SPECIAL ROAD DISTRICT, OR
IDANHA-DETROIT RURAL FIRE PROTECTION
DISTRICT, OR
ILLINOIS VALLEY FIRE DISTRICT
ILLINOIS VALLEY R.F.P.D., OR
ILLINOIS VALLEY S.W.C.D., OR
IMBLER R.F.P.D., OR
INTERLACHEN WATER P.U.D., OR
IONE LIBRARY DISTRICT, OR
IONE R.F.P.D. #6-604, OR
IRONSIDE CEMETERY MAINTENANCE DISTRICT, OR
IRONSIDE RURAL ROAD DISTRICT #5, OR
IRRIGON PARK & RECREATION DISTRICT, OR
IRRIGON R.F.P.D., OR
ISLAND CITY AREA SANITATION DISTRICT, OR
ISLAND CITY CEMETERY MAINTENANCE DISTRICT,
OR
JACK PINE VILLAGE SPECIAL ROAD DISTRICT, OR
JACKSON COUNTY FIRE DISTRICT #3, OR
JACKSON COUNTY FIRE DISTRICT #4, OR
JACKSON COUNTY FIRE DISTRICT #5, OR
JACKSON COUNTY LIBRARY DISTRICT, OR
JACKSON COUNTY VECTOR CONTROL DISTRICT, OR
JACKSON S.W.C.D., OR
JASPER KNOLLS WATER DISTRICT, OR
JEFFERSON COUNTY EMERGENCY MEDICAL
SERVICE DISTRICT, OR
JEFFERSON COUNTY FIRE DISTRICT #1, OR
JEFFERSON COUNTY LIBRARY DISTRICT, OR
JEFFERSON COUNTY S.W.C.D., OR
JEFFERSON PARK & RECREATION DISTRICT, OR

JEFFERSON R.F.P.D., OR
JOB'S DRAINAGE DISTRICT, OR
JOHN DAY WATER DISTRICT, OR
JOHN DAY-CANYON CITY PARKS & RECREATION DISTRICT, OR
JOHN DAY-FERNHILL R.F.P.D. #5-108, OR
JORDAN VALLEY CEMETERY DISTRICT, OR
JORDAN VALLEY IRRIGATION DISTRICT, OR
JOSEPHINE COMMUNITY LIBRARY DISTRICT, OR
JOSEPHINE COUNTY 4-H & EXTENSION SERVICE DISTRICT, OR
JOSEPHINE COUNTY 911 AGENCY, OR
JUNCTION CITY R.F.P.D., OR
JUNCTION CITY WATER CONTROL DISTRICT, OR
JUNIPER BUTTE ROAD DISTRICT, OR
JUNIPER CANYON WATER CONTROL DISTRICT, OR
JUNIPER FLAT DISTRICT IMPROVEMENT COMPANY, OR
JUNIPER FLAT R.F.P.D., OR
JUNO NONPROFIT WATER IMPROVEMENT DISTRICT, OR
KEATING R.F.P.D., OR
KEATING S.W.C.D., OR
KEIZER R.F.P.D., OR
KELLOGG RURAL FIRE DISTRICT, OR
KENO IRRIGATION DISTRICT, OR
KENO PINES ROAD DISTRICT, OR
KENO R.F.P.D., OR
KENT WATER DISTRICT, OR
KERBY WATER DISTRICT, OR
K-GB-LB WATER DISTRICT, OR
KILCHIS WATER DISTRICT, OR
KLAMATH 9-1-1 COMMUNICATIONS DISTRICT, OR
KLAMATH BASIN IMPROVEMENT DISTRICT, OR
KLAMATH COUNTY DRAINAGE SERVICE DISTRICT, OR
KLAMATH COUNTY EXTENSION SERVICE DISTRICT, OR
KLAMATH COUNTY FIRE DISTRICT #1, OR
KLAMATH COUNTY FIRE DISTRICT #3, OR
KLAMATH COUNTY FIRE DISTRICT #4, OR
KLAMATH COUNTY FIRE DISTRICT #5, OR
KLAMATH COUNTY LIBRARY SERVICE DISTRICT, OR
KLAMATH COUNTY PREDATORY ANIMAL CONTROL DISTRICT, OR
KLAMATH DRAINAGE DISTRICT, OR
KLAMATH FALLS FOREST ESTATES SPECIAL ROAD DISTRICT UNIT #2, OR
KLAMATH INTEROPERABILITY RADIO GROUP, OR
KLAMATH IRRIGATION DISTRICT, OR
KLAMATH RIVER ACRES SPECIAL ROAD DISTRICT, OR
KLAMATH S.W.C.D., OR
KLAMATH VECTOR CONTROL DISTRICT, OR
KNAPPA-SVENSEN-BURNSIDE R.F.P.D., OR
LA GRANDE CEMETERY MAINTENANCE DISTRICT, OR
LA GRANDE R.F.P.D., OR
LA PINE PARK & RECREATION DISTRICT, OR
LA PINE R.F.P.D., OR
LABISH VILLAGE SEWAGE & DRAINAGE, OR
LACOMB IRRIGATION DISTRICT, OR
LAFAYETTE AIRPORT COMMISSION, LA
LAFORCHE PARISH HEALTH UNIT – DHH-OPH REGION 3

LIDLAW WATER DISTRICT, OR
LAKE CHINOOK FIRE & RESCUE, OR
LAKE COUNTY 4-H & EXTENSION SERVICE DISTRICT, OR
LAKE COUNTY LIBRARY DISTRICT, OR
LAKE CREEK R.F.P.D. - JACKSON, OR
LAKE CREEK R.F.P.D. - LANE COUNTY, OR
LAKE DISTRICT HOSPITAL, OR
LAKE GROVE R.F.P.D. NO. 57, OR
LAKE GROVE WATER DISTRICT, OR
LAKE LABISH WATER CONTROL DISTRICT, OR
LAKE POINT SPECIAL ROAD DISTRICT, OR
LAKESIDE R.F.P.D. #4, OR
LAKESIDE WATER DISTRICT, OR
LAKEVIEW R.F.P.D., OR
LAKEVIEW S.W.C.D., OR
LAMONTAI IMPROVEMENT DISTRICT, OR
LANE FIRE AUTHORITY, OR
LANE LIBRARY DISTRICT, OR
LANE TRANSIT DISTRICT, OR
LANGELL VALLEY IRRIGATION DISTRICT, OR
LANGLOIS PUBLIC LIBRARY, OR
LANGLOIS R.F.P.D., OR
LANGLOIS WATER DISTRICT, OR
LAZY RIVER SPECIAL ROAD DISTRICT, OR
LEBANON AQUATIC DISTRICT, OR
LEBANON R.F.P.D., OR
LEWIS & CLARK R.F.P.D., OR
LINCOLN COUNTY LIBRARY DISTRICT, OR
LINCOLN S.W.C.D., OR
LINN COUNTY EMERGENCY TELEPHONE AGENCY, OR
LINN S.W.C.D., OR
LITTLE MUDDY CREEK WATER CONTROL, OR
LITTLE NESTUCCA DRAINAGE DISTRICT, OR
LITTLE SWITZERLAND SPECIAL ROAD DISTRICT, OR
LONE PINE IRRIGATION DISTRICT, OR
LONG PRAIRIE WATER DISTRICT, OR
LOOKINGGLASS OLALLA WATER CONTROL DISTRICT, OR
LOOKINGGLASS RURAL FIRE DISTRICT, OR
LORANE R.F.P.D., OR
LOST & BOULDER DITCH IMPROVEMENT DISTRICT, OR
LOST CREEK PARK SPECIAL ROAD DISTRICT, OR
LOUISIANA PUBLIC SERVICE COMMISSION, LA
LOUISIANA WATER WORKS
LOWELL R.F.P.D., OR
LOWER MCKAY CREEK R.F.P.D., OR
LOWER MCKAY CREEK WATER CONTROL DISTRICT, OR
LOWER POWDER RIVER IRRIGATION DISTRICT, OR
LOWER SILETZ WATER DISTRICT, OR
LOWER UMPQUA HOSPITAL DISTRICT, OR
LOWER UMPQUA PARK & RECREATION DISTRICT, OR
LOWER VALLEY WATER IMPROVEMENT DISTRICT, OR
LUCE LONG DITCH DISTRICT IMPROVEMENT CO., OR
LUSTED WATER DISTRICT, OR
LYONS R.F.P.D., OR
LYONS-MEHAMA WATER DISTRICT, OR
MADRAS AQUATIC CENTER DISTRICT, OR
MAKAI SPECIAL ROAD DISTRICT, OR
MALHEUR COUNTY S.W.C.D., OR

MALHEUR COUNTY VECTOR CONTROL DISTRICT, OR
MALHEUR DISTRICT IMPROVEMENT COMPANY, OR
MALHEUR DRAINAGE DISTRICT, OR
MALHEUR MEMORIAL HEALTH DISTRICT, OR
MALIN COMMUNITY CEMETERY MAINTENANCE DISTRICT, OR
MALIN COMMUNITY PARK & RECREATION DISTRICT, OR
MALIN IRRIGATION DISTRICT, OR
MALIN R.F.P.D., OR
MAPLETON FIRE DEPARTMENT, OR
MAPLETON WATER DISTRICT, OR
MARCOLA WATER DISTRICT, OR
MARION COUNTY EXTENSION & 4H SERVICE DISTRICT, OR
MARION COUNTY FIRE DISTRICT #1, OR
MARION JACK IMPROVEMENT DISTRICT, OR
MARION S.W.C.D., OR
MARY'S RIVER ESTATES ROAD DISTRICT, OR
MCDONALD FOREST ESTATES SPECIAL ROAD DISTRICT, OR
MCKAY ACRES IMPROVEMENT DISTRICT, OR
MCKAY DAM R.F.P.D. # 7-410, OR
MCKENZIE FIRE & RESCUE, OR
MCKENZIE PALISADES WATER SUPPLY CORPORATION, OR
MCMINNVILLE R.F.P.D., OR
MCNULTY WATER P.U.D., OR
MEADOWS DRAINAGE DISTRICT, OR
MEDFORD IRRIGATION DISTRICT, OR
MEDFORD R.F.P.D. #2, OR
MEDFORD WATER COMMISSION
MEDICAL SPRINGS R.F.P.D., OR
MELHEUR COUNTY JAIL, OR
MERLIN COMMUNITY PARK DISTRICT, OR
MERRILL CEMETERY MAINTENANCE DISTRICT, OR
MERRILL PARK DISTRICT, OR
MERRILL R.F.P.D., OR
METRO REGIONAL GOVERNMENT
METRO REGIONAL PARKS
METROPOLITAN EXPOSITION RECREATION COMMISSION
METROPOLITAN SERVICE DISTRICT (METRO)
MID COUNTY CEMETERY MAINTENANCE DISTRICT, OR
MID-COLUMBIA FIRE AND RESCUE, OR
MIDDLE FORK IRRIGATION DISTRICT, OR
MIDLAND COMMUNITY PARK, OR
MIDLAND DRAINAGE IMPROVEMENT DISTRICT, OR
MILES CROSSING SANITARY SEWER DISTRICT, OR
MILL CITY R.F.P.D. #2-303, OR
MILL FOUR DRAINAGE DISTRICT, OR
MILLICOMA RIVER PARK & RECREATION DISTRICT, OR
MILLINGTON R.F.P.D. #5, OR
MILO VOLUNTEER FIRE DEPARTMENT, OR
MILTON-FREEWATER AMBULANCE SERVICE AREA HEALTH DISTRICT, OR
MILTON-FREEWATER WATER CONTROL DISTRICT, OR
MIROCO SPECIAL ROAD DISTRICT, OR
MIST-BIRKENFELD R.F.P.D., OR
MODOC POINT IRRIGATION DISTRICT, OR
MODOC POINT SANITARY DISTRICT, OR
MOHAWK VALLEY R.F.P.D., OR

MOLALLA AQUATIC DISTRICT, OR
MOLALLA R.F.P.D. #73, OR
MONITOR R.F.P.D., OR
MONROE R.F.P.D., OR
MONUMENT CEMETERY MAINTENANCE DISTRICT, OR
MONUMENT S.W.C.D., OR
MOOREA DRIVE SPECIAL ROAD DISTRICT, OR
MORO R.F.P.D., OR
MORROW COUNTY HEALTH DISTRICT, OR
MORROW COUNTY UNIFIED RECREATION DISTRICT, OR
MORROW S.W.C.D., OR
MOSIER FIRE DISTRICT, OR
MOUNTAIN DRIVE SPECIAL ROAD DISTRICT, OR
MT. ANGEL R.F.P.D., OR
MT. HOOD IRRIGATION DISTRICT, OR
MT. LAKI CEMETERY DISTRICT, OR
MT. VERNON R.F.P.D., OR
MULINO WATER DISTRICT #1, OR
MULTNOMAH COUNTY DRAINAGE DISTRICT #1, OR
MULTNOMAH COUNTY R.F.P.D. #10, OR
MULTNOMAH COUNTY R.F.P.D. #14, OR
MULTNOMAH EDUCATION SERVICE DISTRICT
MYRTLE CREEK R.F.P.D., OR
NEAH-KAH-NIE WATER DISTRICT, OR
NEDONNA R.F.P.D., OR
NEHALEM BAY FIRE AND RESCUE, OR
NEHALEM BAY HEALTH DISTRICT, OR
NEHALEM BAY WASTEWATER AGENCY, OR
NESIKA BEACH-OPHIR WATER DISTRICT, OR
NESKOWIN REGIONAL SANITARY AUTHORITY, OR
NESKOWIN REGIONAL WATER DISTRICT, OR
NESTUCCA R.F.P.D., OR
NETARTS WATER DISTRICT, OR
NETARTS-OCEANSIDE R.F.P.D., OR
NETARTS-OCEANSIDE SANITARY DISTRICT, OR
NEW BRIDGE WATER SUPPLY DISTRICT, OR
NEW CARLTON FIRE DISTRICT, OR
NEW ORLEANS REDEVELOPMENT AUTHORITY, LA
NEW PINE CREEK R.F.P.D., OR
NEWBERG R.F.P.D., OR
NEWBERRY ESTATES SPECIAL ROAD DISTRICT, OR
NEWPORT R.F.P.D., OR
NEWT YOUNG DITCH DISTRICT IMPROVEMENT COMPANY, OR
NORTH ALBANY R.F.P.D., OR
NORTH BAY R.F.P.D. #9, OR
NORTH CLACKAMAS PARKS & RECREATION DISTRICT, OR
NORTH COUNTY RECREATION DISTRICT, OR
NORTH DOUGLAS COUNTY FIRE & EMS, OR
NORTH DOUGLAS PARK & RECREATION DISTRICT, OR
NORTH GILLIAM COUNTY HEALTH DISTRICT, OR
NORTH GILLIAM COUNTY R.F.P.D., OR
NORTH LAKE HEALTH DISTRICT, OR
NORTH LEBANON WATER CONTROL DISTRICT, OR
NORTH LINCOLN FIRE & RESCUE DISTRICT #1, OR
NORTH LINCOLN HEALTH DISTRICT, OR
NORTH MORROW VECTOR CONTROL DISTRICT, OR
NORTH SHERMAN COUNTY R.F.P.D., OR
NORTH UNIT IRRIGATION DISTRICT, OR
NORTHEAST OREGON HOUSING AUTHORITY, OR
NORTHEAST WHEELER COUNTY HEALTH DISTRICT, OR

NORTHERN WASCO COUNTY P.U.D., OR
NORTHERN WASCO COUNTY PARK & RECREATION DISTRICT, OR
NYE DITCH USERS DISTRICT IMPROVEMENT, OR
NYSSA ROAD ASSESSMENT DISTRICT #2, OR
NYSSA RURAL FIRE DISTRICT, OR
NYSSA-ARCADIA DRAINAGE DISTRICT, OR
OAK LODGE WATER SERVICES, OR
OAKLAND R.F.P.D., OR
OAKVILLE COMMUNITY CENTER, OR
OCEANSIDE WATER DISTRICT, OR
OCHOCO IRRIGATION DISTRICT, OR
OCHOCO WEST WATER AND SANITARY AUTHORITY, OR
ODELL SANITARY DISTRICT, OR
OLD OWYHEE DITCH IMPROVEMENT DISTRICT, OR
OLNEY-WALLUSKI FIRE & RESCUE DISTRICT, OR
ONTARIO LIBRARY DISTRICT, OR
ONTARIO R.F.P.D., OR
OPHIR R.F.P.D., OR
OREGON COAST COMMUNITY ACTION
OREGON HOUSING AND COMMUNITY SERVICES
OREGON INTERNATIONAL PORT OF COOS BAY, OR
OREGON LEGISLATIVE ADMINISTRATION
OREGON OUTBACK R.F.P.D., OR
OREGON POINT, OR
OREGON TRAIL LIBRARY DISTRICT, OR
OTTER ROCK WATER DISTRICT, OR
OWW UNIT #2 SANITARY DISTRICT, OR
OWYHEE CEMETERY MAINTENANCE DISTRICT, OR
OWYHEE IRRIGATION DISTRICT, OR
PACIFIC CITY JOINT WATER-SANITARY AUTHORITY, OR
PACIFIC COMMUNITIES HEALTH DISTRICT, OR
PACIFIC RIVIERA #3 SPECIAL ROAD DISTRICT, OR
PALATINE HILL WATER DISTRICT, OR
PALMER CREEK WATER DISTRICT IMPROVEMENT COMPANY, OR
PANORAMIC ACCESS SPECIAL ROAD DISTRICT, OR
PANTHER CREEK ROAD DISTRICT, OR
PANTHER CREEK WATER DISTRICT, OR
PARKDALE R.F.P.D., OR
PARKDALE SANITARY DISTRICT, OR
PENINSULA DRAINAGE DISTRICT #1, OR
PENINSULA DRAINAGE DISTRICT #2, OR
PHILOMATH FIRE AND RESCUE, OR
PILOT ROCK CEMETERY MAINTENANCE DISTRICT #5, OR
PILOT ROCK PARK & RECREATION DISTRICT, OR
PILOT ROCK R.F.P.D., OR
PINE EAGLE HEALTH DISTRICT, OR
PINE FLAT DISTRICT IMPROVEMENT COMPANY, OR
PINE GROVE IRRIGATION DISTRICT, OR
PINE GROVE WATER DISTRICT-KLAMATH FALLS, OR
PINE GROVE WATER DISTRICT-MAUPIN, OR
PINE VALLEY CEMETERY DISTRICT, OR
PINE VALLEY R.F.P.D., OR
PINWOOD COUNTRY ESTATES SPECIAL ROAD DISTRICT, OR
PIONEER DISTRICT IMPROVEMENT COMPANY, OR
PISTOL RIVER CEMETERY MAINTENANCE DISTRICT, OR
PISTOL RIVER FIRE DISTRICT, OR
PLEASANT HILL R.F.P.D., OR
PLEASANT HOME WATER DISTRICT, OR

POCAHONTAS MINING AND IRRIGATION DISTRICT, OR
POE VALLEY IMPROVEMENT DISTRICT, OR
POE VALLEY PARK & RECREATION DISTRICT, OR
POE VALLEY VECTOR CONTROL DISTRICT, OR
POLK COUNTY FIRE DISTRICT #1, OR
POLK S.W.C.D., OR
POMPADOUR WATER IMPROVEMENT DISTRICT, OR
PONDEROSA PINES EAST SPECIAL ROAD DISTRICT, OR
PORT OF ALSEA, OR
PORT OF ARLINGTON, OR
PORT OF ASTORIA, OR
PORT OF BANDON, OR
PORT OF BRANDON, OR
PORT OF BROOKINGS HARBOR, OR
PORT OF CASCADE LOCKS, OR
PORT OF COQUILLE RIVER, OR
PORT OF GARIBALDI, OR
PORT OF GOLD BEACH, OR
PORT OF HOOD RIVER, OR
PORT OF MORGAN CITY, LA
PORT OF MORROW, OR
PORT OF NEHALEM, OR
PORT OF NEWPORT, OR
PORT OF PORT ORFORD, OR
PORT OF PORTLAND, OR
PORT OF SIUSLAW, OR
PORT OF ST. HELENS, OR
PORT OF THE DALLES, OR
PORT OF TILLAMOOK BAY, OR
PORT OF TOLEDO, OR
PORT OF UMATILLA, OR
PORT OF UMPQUA, OR
PORT ORFORD CEMETERY MAINTENANCE DISTRICT, OR
PORT ORFORD PUBLIC LIBRARY DISTRICT, OR
PORT ORFORD R.F.P.D., OR
PORTLAND DEVELOPMENT COMMISSION, OR
PORTLAND FIRE AND RESCUE
PORTLAND HOUSING CENTER, OR
POWDER R.F.P.D., OR
POWDER RIVER R.F.P.D., OR
POWDER VALLEY WATER CONTROL DISTRICT, OR
POWERS HEALTH DISTRICT, OR
PRAIRIE CEMETERY MAINTENANCE DISTRICT, OR
PRINEVILLE LAKE ACRES SPECIAL ROAD DISTRICT #1, OR
PROSPECT R.F.P.D., OR
QUAIL VALLEY PARK IMPROVEMENT DISTRICT, OR
QUEENER IRRIGATION IMPROVEMENT DISTRICT, OR
RAINBOW WATER DISTRICT, OR
RAINIER CEMETERY DISTRICT, OR
RAINIER DRAINAGE IMPROVEMENT COMPANY, OR
RALEIGH WATER DISTRICT, OR
REDMOND AREA PARK & RECREATION DISTRICT, OR
REDMOND FIRE AND RESCUE, OR
RIDDLE FIRE PROTECTION DISTRICT, OR
RIDGWOOD DISTRICT IMPROVEMENT COMPANY, OR
RIDGWOOD ROAD DISTRICT, OR
RIETH SANITARY DISTRICT, OR
RIETH WATER DISTRICT, OR
RIMROCK WEST IMPROVEMENT DISTRICT, OR

RINK CREEK WATER DISTRICT, OR
RIVER BEND ESTATES SPECIAL ROAD DISTRICT, OR
RIVER FOREST ACRES SPECIAL ROAD DISTRICT, OR
RIVER MEADOWS IMPROVEMENT DISTRICT, OR
RIVER PINES ESTATES SPECIAL ROAD DISTRICT, OR
RIVER ROAD PARK & RECREATION DISTRICT, OR
RIVER ROAD WATER DISTRICT, OR
RIVERBEND RIVERBANK WATER IMPROVEMENT DISTRICT, OR
RIVERDALE R.F.P.D. 11-JT, OR
RIVERGROVE WATER DISTRICT, OR
RIVERSIDE MISSION WATER CONTROL DISTRICT, OR
RIVERSIDE R.F.P.D. #7-406, OR
RIVERSIDE WATER DISTRICT, OR
ROBERTS CREEK WATER DISTRICT, OR
ROCK CREEK DISTRICT IMPROVEMENT, OR
ROCK CREEK WATER DISTRICT, OR
ROCKWOOD WATER P.U.D., OR
ROCKY POINT FIRE & EMS, OR
ROGUE RIVER R.F.P.D., OR
ROGUE RIVER VALLEY IRRIGATION DISTRICT, OR
ROGUE VALLEY SEWER SERVICES, OR
ROGUE VALLEY SEWER, OR
ROGUE VALLEY TRANSPORTATION DISTRICT, OR
ROSEBURG URBAN SANITARY AUTHORITY, OR
ROSEWOOD ESTATES ROAD DISTRICT, OR
ROW RIVER VALLEY WATER DISTRICT, OR
RURAL ROAD ASSESSMENT DISTRICT #3, OR
RURAL ROAD ASSESSMENT DISTRICT #4, OR
SAINT LANDRY PARISH TOURIST COMMISSION
SAINT MARY PARISH REC DISTRICT 2
SAINT MARY PARISH REC DISTRICT 3
SAINT TAMMANY FIRE DISTRICT 4, LA
SALEM AREA MASS TRANSIT DISTRICT, OR
SALEM MASS TRANSIT DISTRICT
SALEM SUBURBAN R.F.P.D., OR
SALISHAN SANITARY DISTRICT, OR
SALMON RIVER PARK SPECIAL ROAD DISTRICT, OR
SALMON RIVER PARK WATER IMPROVEMENT DISTRICT, OR
SALMONBERRY TRAIL INTERGOVERNMENTAL AGENCY, OR
SANDPIPER VILLAGE SPECIAL ROAD DISTRICT, OR
SANDY DRAINAGE IMPROVEMENT COMPANY, OR
SANDY R.F.P.D. #72, OR
SANTA CLARA R.F.P.D., OR
SANTA CLARA WATER DISTRICT, OR
SANTIAM WATER CONTROL DISTRICT, OR
SAUVIE ISLAND DRAINAGE IMPROVEMENT COMPANY, OR
SAUVIE ISLAND VOLUNTEER FIRE DISTRICT #30J, OR
SCAPPOOSE DRAINAGE IMPROVEMENT COMPANY, OR
SCAPPOOSE PUBLIC LIBRARY DISTRICT, OR
SCAPPOOSE R.F.P.D., OR
SCIO R.F.P.D., OR
SCOTTSBURG R.F.P.D., OR
SEAL ROCK R.F.P.D., OR
SEAL ROCK WATER DISTRICT, OR
SEWERAGE AND WATER BOARD OF NEW ORLEANS, LA
SHANGRI-LA WATER DISTRICT, OR
SHASTA VIEW IRRIGATION DISTRICT, OR

SHELLEY ROAD CREST ACRES WATER DISTRICT, OR
SHERIDAN FIRE DISTRICT, OR
SHERMAN COUNTY HEALTH DISTRICT, OR
SHERMAN COUNTY S.W.C.D., OR
SHORELINE SANITARY DISTRICT, OR
SILETZ KEYS SANITARY DISTRICT, OR
SILETZ R.F.P.D., OR
SILVER FALLS LIBRARY DISTRICT, OR
SILVER LAKE IRRIGATION DISTRICT, OR
SILVER LAKE R.F.P.D., OR
SILVER SANDS SPECIAL ROAD DISTRICT, OR
SILVERTON R.F.P.D. NO. 2, OR
SISTERS PARKS & RECREATION DISTRICT, OR
SISTERS-CAMP SHERMAN R.F.P.D., OR
SIUSLAW PUBLIC LIBRARY DISTRICT, OR
SIUSLAW S.W.C.D., OR
SIUSLAW VALLEY FIRE AND RESCUE, OR
SIXES R.F.P.D., OR
SKIPANON WATER CONTROL DISTRICT, OR
SKYLINE VIEW DISTRICT IMPROVEMENT COMPANY, OR
SLEEPY HOLLOW WATER DISTRICT, OR
SMITH DITCH DISTRICT IMPROVEMENT COMPANY, OR
SOUTH CLACKAMAS TRANSPORTATION DISTRICT, OR
SOUTH COUNTY HEALTH DISTRICT, OR
SOUTH FORK WATER BOARD, OR
SOUTH GILLIAM COUNTY CEMETERY DISTRICT, OR
SOUTH GILLIAM COUNTY HEALTH DISTRICT, OR
SOUTH GILLIAM COUNTY R.F.P.D. VI-301, OR
SOUTH LAFOURCHE LEVEE DISTRICT, LA
SOUTH LANE COUNTY FIRE & RESCUE, OR
SOUTH SANTIAM RIVER WATER CONTROL DISTRICT, OR
SOUTH SHERMAN FIRE DISTRICT, OR
SOUTH SUBURBAN SANITARY DISTRICT, OR
SOUTH WASCO PARK & RECREATION DISTRICT, OR
SOUTHERN COOS HEALTH DISTRICT, OR
SOUTHERN CURRY CEMETERY MAINTENANCE DISTRICT, OR
SOUTHVIEW IMPROVEMENT DISTRICT, OR
SOUTHWEST LINCOLN COUNTY WATER DISTRICT, OR
SOUTHWESTERN POLK COUNTY R.F.P.D., OR
SOUTHWOOD PARK WATER DISTRICT, OR
SPECIAL ROAD DISTRICT #1, OR
SPECIAL ROAD DISTRICT #8, OR
SPRING RIVER SPECIAL ROAD DISTRICT, OR
SPRINGFIELD UTILITY BOARD, OR
ST. PAUL R.F.P.D., OR
STANFIELD CEMETERY DISTRICT #6, OR
STANFIELD IRRIGATION DISTRICT, OR
STARR CREEK ROAD DISTRICT, OR
STARWOOD SANITARY DISTRICT, OR
STAYTON FIRE DISTRICT, OR
SUBLIMITY FIRE DISTRICT, OR
SUBURBAN EAST SALEM WATER DISTRICT, OR
SUBURBAN LIGHTING DISTRICT, OR
SUCCOR CREEK DISTRICT IMPROVEMENT COMPANY, OR
SUMMER LAKE IRRIGATION DISTRICT, OR
SUMMERVILLE CEMETERY MAINTENANCE DISTRICT, OR
SUMNER R.F.P.D., OR

SUN MOUNTAIN SPECIAL ROAD DISTRICT, OR
SUNDOWN SANITATION DISTRICT, OR
SUNFOREST ESTATES SPECIAL ROAD DISTRICT, OR
SUNNYSIDE IRRIGATION DISTRICT, OR
SUNRISE WATER AUTHORITY, OR
SUNRIVER SERVICE DISTRICT, OR
SUNSET EMPIRE PARK & RECREATION DISTRICT,
OR
SUNSET EMPIRE TRANSPORTATION DISTRICT, OR
SURFLAND ROAD DISTRICT, OR
SUTHERLIN VALLEY RECREATION DISTRICT, OR
SUTHERLIN WATER CONTROL DISTRICT, OR
SWALLEY IRRIGATION DISTRICT, OR
SWEET HOME CEMETERY MAINTENANCE DISTRICT,
OR
SWEET HOME FIRE & AMBULANCE DISTRICT, OR
SWISSHOME-DEADWOOD R.F.P.D., OR
TABLE ROCK DISTRICT IMPROVEMENT COMPANY,
OR
TALENT IRRIGATION DISTRICT, OR
TANGENT R.F.P.D., OR
TENMILE R.F.P.D., OR
TERREBONNE DOMESTIC WATER DISTRICT, OR
THE DALLES IRRIGATION DISTRICT, OR
THOMAS CREEK-WESTSIDE R.F.P.D., OR
THREE RIVERS RANCH ROAD DISTRICT, OR
THREE SISTERS IRRIGATION DISTRICT, OR
TIGARD TUALATIN AQUATIC DISTRICT, OR
TIGARD WATER DISTRICT, OR
TILLAMOOK BAY FLOOD IMPROVEMENT DISTRICT,
OR
TILLAMOOK COUNTY EMERGENCY
COMMUNICATIONS DISTRICT, OR
TILLAMOOK COUNTY S.W.C.D., OR
TILLAMOOK COUNTY TRANSPORTATION DISTRICT,
OR
TILLAMOOK FIRE DISTRICT, OR
TILLAMOOK P.U.D., OR
TILLER R.F.P.D., OR
TOBIN DITCH DISTRICT IMPROVEMENT COMPANY,
OR
TOLEDO R.F.P.D., OR
TONE WATER DISTRICT, OR
TOOLEY WATER DISTRICT, OR
TRASK DRAINAGE DISTRICT, OR
TRI CITY R.F.P.D. #4, OR
TRI-CITY WATER & SANITARY AUTHORITY, OR
TRI-COUNTY METROPOLITAN TRANSPORTATION
DISTRICT OF OREGON
TRIMET, OR
TUALATIN HILLS PARK & RECREATION DISTRICT
TUALATIN HILLS PARK & RECREATION DISTRICT,
OR
TUALATIN S.W.C.D., OR
TUALATIN VALLEY FIRE & RESCUE
TUALATIN VALLEY FIRE & RESCUE, OR
TUALATIN VALLEY IRRIGATION DISTRICT, OR
TUALATIN VALLEY WATER DISTRICT
TUALATIN VALLEY WATER DISTRICT, OR
TUMALO IRRIGATION DISTRICT, OR
TURNER FIRE DISTRICT, OR
TWIN ROCKS SANITARY DISTRICT, OR
TWO RIVERS NORTH SPECIAL ROAD DISTRICT, OR
TWO RIVERS S.W.C.D., OR
TWO RIVERS SPECIAL ROAD DISTRICT, OR
TYGH VALLEY R.F.P.D., OR

TYGH VALLEY WATER DISTRICT, OR
UMATILLA COUNTY FIRE DISTRICT #1, OR
UMATILLA COUNTY S.W.C.D., OR
UMATILLA COUNTY SPECIAL LIBRARY DISTRICT,
OR
UMATILLA HOSPITAL DISTRICT, OR
UMATILLA R.F.P.D. #7-405, OR
UMATILLA-MORROW RADIO AND DATA DISTRICT,
OR
UMPQUA S.W.C.D., OR
UNION CEMETERY MAINTENANCE DISTRICT, OR
UNION COUNTY SOLID WASTE DISPOSAL DISTRICT,
OR
UNION COUNTY VECTOR CONTROL DISTRICT, OR
UNION GAP SANITARY DISTRICT, OR
UNION GAP WATER DISTRICT, OR
UNION HEALTH DISTRICT, OR
UNION R.F.P.D., OR
UNION S.W.C.D., OR
UNITY COMMUNITY PARK & RECREATION
DISTRICT, OR
UPPER CLEVELAND RAPIDS ROAD DISTRICT, OR
UPPER MCKENZIE R.F.P.D., OR
UPPER WILLAMETTE S.W.C.D., OR
VALE OREGON IRRIGATION DISTRICT, OR
VALE RURAL FIRE PROTECTION DISTRICT, OR
VALLEY ACRES SPECIAL ROAD DISTRICT, OR
VALLEY VIEW CEMETERY MAINTENANCE
DISTRICT, OR
VALLEY VIEW WATER DISTRICT, OR
VANDEVERT ACRES SPECIAL ROAD DISTRICT, OR
VERNONIA R.F.P.D., OR
VINEYARD MOUNTAIN PARK & RECREATION
DISTRICT, OR
VINEYARD MOUNTAIN SPECIAL ROAD DISTRICT,
OR
WALLA WALLA RIVER IRRIGATION DISTRICT, OR
WALLOWA COUNTY HEALTH CARE DISTRICT, OR
WALLOWA LAKE COUNTY SERVICE DISTRICT, OR
WALLOWA LAKE IRRIGATION DISTRICT, OR
WALLOWA LAKE R.F.P.D., OR
WALLOWA S.W.C.D., OR
WALLOWA VALLEY IMPROVEMENT DISTRICT #1,
OR
WAMIC R.F.P.D., OR
WAMIC WATER & SANITARY AUTHORITY, OR
WARMSPRINGS IRRIGATION DISTRICT, OR
WASCO COUNTY S.W.C.D., OR
WATER ENVIRONMENT SERVICES, OR
WATER WONDERLAND IMPROVEMENT DISTRICT,
OR
WATERBURY & ALLEN DITCH IMPROVEMENT
DISTRICT, OR
WATSECO-BARVIEW WATER DISTRICT, OR
WAUNA WATER DISTRICT, OR
WEDDERBURN SANITARY DISTRICT, OR
WEST EAGLE VALLEY WATER CONTROL DISTRICT,
OR
WEST EXTENSION IRRIGATION DISTRICT, OR
WEST LABISH DRAINAGE & WATER CONTROL
IMPROVEMENT DISTRICT, OR
WEST MULTNOMAH S.W.C.D., OR
WEST SIDE R.F.P.D., OR
WEST SLOPE WATER DISTRICT, OR
WEST UMATILLA MOSQUITO CONTROL DISTRICT,
OR

WEST VALLEY FIRE DISTRICT, OR
 WESTERN HEIGHTS SPECIAL ROAD DISTRICT, OR
 WESTERN LANE AMBULANCE DISTRICT, OR
 WESTLAND IRRIGATION DISTRICT, OR
 WESTON ATHENA MEMORIAL HALL PARK &
 RECREATION DISTRICT, OR
 WESTON CEMETERY DISTRICT #2, OR
 WESTPORT FIRE AND RESCUE, OR
 WESTRIDGE WATER SUPPLY CORPORATION, OR
 WESTWOOD HILLS ROAD DISTRICT, OR
 WESTWOOD VILLAGE ROAD DISTRICT, OR
 WHEELER S.W.C.D., OR
 WHITE RIVER HEALTH DISTRICT, OR
 WIARD MEMORIAL PARK DISTRICT, OR
 WICKIUP WATER DISTRICT, OR
 WILLAKENZIE R.F.P.D., OR
 WILLAMALANE PARK & RECREATION DISTRICT, OR
 WILLAMALANE PARK AND RECREATION DISTRICT
 WILLAMETTE HUMANE SOCIETY
 WILLAMETTE RIVER WATER COALITION, OR
 WILLIAMS R.F.P.D., OR
 WILLOW CREEK PARK DISTRICT, OR
 WILLOW DALE WATER DISTRICT, OR
 WILSON RIVER WATER DISTRICT, OR
 WINCHESTER BAY R.F.P.D., OR
 WINCHESTER BAY SANITARY DISTRICT, OR
 WINCHUCK R.F.P.D., OR
 WINSTON-DILLARD R.F.P.D., OR
 WINSTON-DILLARD WATER DISTRICT, OR
 WOLF CREEK R.F.P.D., OR
 WOOD RIVER DISTRICT IMPROVEMENT COMPANY,
 OR
 WOODBURN R.F.P.D. NO. 6, OR
 WOODLAND PARK SPECIAL ROAD DISTRICT, OR
 WOODS ROAD DISTRICT, OR
 WRIGHT CREEK ROAD WATER IMPROVEMENT
 DISTRICT, OR
 WY'EAST FIRE DISTRICT, OR
 YACHATS R.F.P.D., OR
 YAMHILL COUNTY TRANSIT AREA, OR
 YAMHILL FIRE PROTECTION DISTRICT, OR
 YAMHILL SWCD, OR
 YONCALLA PARK & RECREATION DISTRICT, OR
 YOUNGS RIVER-LEWIS & CLARK WATER DISTRICT,
 OR
 ZUMWALT R.F.P.D., OR

K-12 INCLUDING BUT NOT LIMITED TO:

ACADIA PARISH SCHOOL BOARD
 BEAVERTON SCHOOL DISTRICT
 BEND-LA PINE SCHOOL DISTRICT
 BOGALUSA HIGH SCHOOL, LA
 BOSSIER PARISH SCHOOL BOARD
 BROOKING HARBOR SCHOOL DISTRICT
 CADDO PARISH SCHOOL DISTRICT
 CALCASIEU PARISH SCHOOL DISTRICT
 CANBY SCHOOL DISTRICT
 CANYONVILLE CHRISTIAN ACADEMY
 CASCADE SCHOOL DISTRICT
 CASCADES ACADEMY OF CENTRAL OREGON
 CENTENNIAL SCHOOL DISTRICT
 CENTRAL CATHOLIC HIGH SCHOOL
 CENTRAL POINT SCHOOL DISTRICT NO.6
 CENTRAL SCHOOL DISTRICT 13J
 COOS BAY SCHOOL DISTRICT NO.9

CORVALLIS SCHOOL DISTRICT 509J
 COUNTY OF YAMHILL SCHOOL DISTRICT 29
 CULVER SCHOOL DISTRICT
 DALLAS SCHOOL DISTRICT NO.2
 DAVID DOUGLAS SCHOOL DISTRICT
 DAYTON SCHOOL DISTRICT NO.8
 DE LA SALLE N CATHOLIC HS
 DESCHUTES COUNTY SCHOOL DISTRICT NO.6
 DOUGLAS EDUCATIONAL DISTRICT SERVICE
 DUFUR SCHOOL DISTRICT NO.29
 EAST BATON ROUGE PARISH SCHOOL DISTRICT
 ESTACADA SCHOOL DISTRICT NO.10B
 FOREST GROVE SCHOOL DISTRICT
 GEORGE MIDDLE SCHOOL
 GLADSTONE SCHOOL DISTRICT
 GRANTS PASS SCHOOL DISTRICT 7
 GREATER ALBANY PUBLIC SCHOOL DISTRICT
 GRESHAM BARLOW JOINT SCHOOL DISTRICT
 HEAD START OF LANE COUNTY
 HIGH DESERT EDUCATION SERVICE DISTRICT
 HILLSBORO SCHOOL DISTRICT
 HOOD RIVER COUNTY SCHOOL DISTRICT
 JACKSON CO SCHOOL DIST NO.9
 JEFFERSON COUNTY SCHOOL DISTRICT 509-J
 JEFFERSON PARISH SCHOOL DISTRICT
 JEFFERSON SCHOOL DISTRICT
 JUNCTION CITY SCHOOLS, OR
 KLAMATH COUNTY SCHOOL DISTRICT
 KLAMATH FALLS CITY SCHOOLS
 LAFAYETTE PARISH SCHOOL DISTRICT
 LAKE OSWEGO SCHOOL DISTRICT 7J
 LANE COUNTY SCHOOL DISTRICT 4J
 LINCOLN COUNTY SCHOOL DISTRICT
 LINN CO. SCHOOL DIST. 95C
 LIVINGSTON PARISH SCHOOL DISTRICT
 LOST RIVER JR/SR HIGH SCHOOL
 LOWELL SCHOOL DISTRICT NO.71
 MARION COUNTY SCHOOL DISTRICT
 MARION COUNTY SCHOOL DISTRICT 103
 MARIST HIGH SCHOOL, OR
 MCMINNVILLE SCHOOL DISTRICT NOAO
 MEDFORD SCHOOL DISTRICT 549C
 MITCH CHARTER SCHOOL
 MONROE SCHOOL DISTRICT NO.1J
 MORROW COUNTY SCHOOL DIST, OR
 MULTNOMAH EDUCATION SERVICE DISTRICT
 MULTISENSORY LEARNING ACADEMY
 MYRTLE PINT SCHOOL DISTRICT 41
 NEAH-KAH-NIE DISTRICT NO.56
 NEWBERG PUBLIC SCHOOLS
 NESTUCCA VALLEY SCHOOL DISTRICT NO.101
 NOBEL LEARNING COMMUNITIES
 NORTH BEND SCHOOL DISTRICT 13
 NORTH CLACKAMAS SCHOOL DISTRICT
 NORTH DOUGLAS SCHOOL DISTRICT
 NORTH WASCO CITY SCHOOL DISTRICT 21
 NORTHWEST REGIONAL EDUCATION SERVICE
 DISTRICT
 ONTARIO MIDDLE SCHOOL
 OREGON TRAIL SCHOOL DISTRICT NOA6
 ORLEANS PARISH SCHOOL DISTRICT
 PHOENIX-TALENT SCHOOL DISTRICT NOA
 PLEASANT HILL SCHOOL DISTRICT
 PORTLAND JEWISH ACADEMY
 PORTLAND PUBLIC SCHOOLS
 RAPIDES PARISH SCHOOL DISTRICT

REDMOND SCHOOL DISTRICT
REYNOLDS SCHOOL DISTRICT
ROGUE RIVER SCHOOL DISTRICT
ROSEBURG PUBLIC SCHOOLS
SCAPPOOSE SCHOOL DISTRICT 1J
SAINT TAMMANY PARISH SCHOOL BOARD, LA
SEASIDE SCHOOL DISTRICT 10
SHERWOOD SCHOOL DISTRICT 88J
SILVER FALLS SCHOOL DISTRICT 4J
SOUTH LANE SCHOOL DISTRICT 45J3
SOUTHERN OREGON EDUCATION SERVICE
DISTRICT
SPRINGFIELD PUBLIC SCHOOLS
SUTHERLIN SCHOOL DISTRICT
SWEET HOME SCHOOL DISTRICT NO.55
TERREBONNE PARISH SCHOOL DISTRICT
THE CATLIN GABEL SCHOOL
TIGARD-TUALATIN SCHOOL DISTRICT
UMATILLA MORROW ESD
WEST LINN WILSONVILLE SCHOOL DISTRICT
WILLAMETTE EDUCATION SERVICE DISTRICT
WOODBURN SCHOOL DISTRICT
YONCALLA SCHOOL DISTRICT
ACADEMY FOR MATH ENGINEERING & SCIENCE
(AMES), UT
ALIANZA ACADEMY, UT
ALPINE DISTRICT, UT
AMERICAN LEADERSHIP ACADEMY, UT
AMERICAN PREPARATORY ACADEMY, UT
BAER CANYON HIGH SCHOOL FOR SPORTS &
MEDICAL SCIENCES, UT
BEAR RIVER CHARTER SCHOOL, UT
BEAVER SCHOOL DISTRICT, UT
BEEHIVE SCIENCE & TECHNOLOGY ACADEMY
(BSTA) , UT
BOX ELDER SCHOOL DISTRICT, UT
CBA CENTER, UT
CACHE SCHOOL DISTRICT, UT
CANYON RIM ACADEMY, UT
CANYONS DISTRICT, UT
CARBON SCHOOL DISTRICT, UT
CHANNING HALL, UT
CHARTER SCHOOL LEWIS ACADEMY, UT
CITY ACADEMY, UT
DAGGETT SCHOOL DISTRICT, UT
DAVINCI ACADEMY, UT
DAVIS DISTRICT, UT
DUAL IMMERSION ACADEMY, UT
DUCHESNE SCHOOL DISTRICT, UT
EARLY LIGHT ACADEMY AT DAYBREAK, UT
EAST HOLLYWOOD HIGH, UT
EDITH BOWEN LABORATORY SCHOOL, UT
EMERSON ALCOTT ACADEMY, UT
EMERY SCHOOL DISTRICT, UT
ENTHEOS ACADEMY, UT
EXCELSIOR ACADEMY, UT
FAST FORWARD HIGH, UT
FREEDOM ACADEMY, UT
GARFIELD SCHOOL DISTRICT, UT
GATEWAY PREPARATORY ACADEMY, UT
GEORGE WASHINGTON ACADEMY, UT
GOOD FOUNDATION ACADEMY, UT
GRAND SCHOOL DISTRICT, UT
GRANITE DISTRICT, UT
GUADALUPE SCHOOL, UT
HAWTHORN ACADEMY, UT

INTECH COLLEGIATE HIGH SCHOOL, UT
IRON SCHOOL DISTRICT, UT
ITINERIS EARLY COLLEGE HIGH, UT
JOHN HANCOCK CHARTER SCHOOL, UT
JORDAN DISTRICT, UT
JUAB SCHOOL DISTRICT, UT
KANE SCHOOL DISTRICT, UT
KARL G MAESER PREPARATORY ACADEMY, UT
LAKEVIEW ACADEMY, UT
LEGACY PREPARATORY ACADEMY, UT
LIBERTY ACADEMY, UT
LINCOLN ACADEMY, UT
LOGAN SCHOOL DISTRICT, UT
MARIA MONTESSORI ACADEMY, UT
MERIT COLLEGE PREPARATORY ACADEMY, UT
MILLARD SCHOOL DISTRICT, UT
MOAB CHARTER SCHOOL, UT
MONTICELLO ACADEMY, UT
MORGAN SCHOOL DISTRICT, UT
MOUNTAINVILLE ACADEMY, UT
MURRAY SCHOOL DISTRICT, UT
NAVIGATOR POINTE ACADEMY, UT
NEBO SCHOOL DISTRICT, UT
NO UT ACAD FOR MATH ENGINEERING & SCIENCE
(NUAMES), UT
NOAH WEBSTER ACADEMY, UT
NORTH DAVIS PREPARATORY ACADEMY, UT
NORTH SANPETE SCHOOL DISTRICT, UT
NORTH STAR ACADEMY, UT
NORTH SUMMIT SCHOOL DISTRICT, UT
ODYSSEY CHARTER SCHOOL, UT
OGDEN PREPARATORY ACADEMY, UT
OGDEN SCHOOL DISTRICT, UT
OPEN CLASSROOM, UT
OPEN HIGH SCHOOL OF UTAH, UT
OQUIRRH MOUNTAIN CHARTER SCHOOL, UT
PARADIGM HIGH SCHOOL, UT
PARK CITY SCHOOL DISTRICT, UT
PINNACLE CANYON ACADEMY, UT
PIUTE SCHOOL DISTRICT, UT
PROVIDENCE HALL, UT
PROVO SCHOOL DISTRICT, UT
QUAIL RUN PRIMARY SCHOOL, UT
QUEST ACADEMY, UT
RANCHES ACADEMY, UT
REAGAN ACADEMY, UT
RENAISSANCE ACADEMY, UT
RICH SCHOOL DISTRICT, UT
ROCKWELL CHARTER HIGH SCHOOL, UT
SALT LAKE ARTS ACADEMY, UT
SALT LAKE CENTER FOR SCIENCE EDUCATION, UT
SALT LAKE SCHOOL DISTRICT, UT
SALT LAKE SCHOOL FOR THE PERFORMING ARTS,
UT
SAN JUAN SCHOOL DISTRICT, UT
SEVIER SCHOOL DISTRICT, UT
SOLDIER HOLLOW CHARTER SCHOOL, UT
SOUTH SANPETE SCHOOL DISTRICT, UT
SOUTH SUMMIT SCHOOL DISTRICT, UT
SPECTRUM ACADEMY, UT
SUCCESS ACADEMY, UT
SUCCESS SCHOOL, UT
SUMMIT ACADEMY, UT
SUMMIT ACADEMY HIGH SCHOOL, UT
SYRACUSE ARTS ACADEMY, UT
THOMAS EDISON - NORTH, UT

TIMPANOGOS ACADEMY, UT
TINTIC SCHOOL DISTRICT, UT
TOOELE SCHOOL DISTRICT, UT
TUACAHN HIGH SCHOOL FOR THE PERFORMING
ARTS, UT
UINTAH RIVER HIGH, UT
UINTAH SCHOOL DISTRICT, UT
UTAH CONNECTIONS ACADEMY, UT
UTAH COUNTY ACADEMY OF SCIENCE, UT
UTAH ELECTRONIC HIGH SCHOOL, UT
UTAH SCHOOLS FOR DEAF & BLIND, UT
UTAH STATE OFFICE OF EDUCATION, UT
UTAH VIRTUAL ACADEMY, UT
VENTURE ACADEMY, UT
VISTA AT ENTRADA SCHOOL OF PERFORMING
ARTS AND TECHNOLOGY, UT
WALDEN SCHOOL OF LIBERAL ARTS, UT
WASATCH PEAK ACADEMY, UT
WASATCH SCHOOL DISTRICT, UT
WASHINGTON SCHOOL DISTRICT, UT
WAYNE SCHOOL DISTRICT, UT
WEBER SCHOOL DISTRICT, UT
WEILENMANN SCHOOL OF DISCOVERY, UT

HIGHER EDUCATION

ARGOSY UNIVERSITY
BATON ROUGE COMMUNITY COLLEGE, LA
BIRTHINGWAY COLLEGE OF MIDWIFERY
BLUE MOUNTAIN COMMUNITY COLLEGE
BRIGHAM YOUNG UNIVERSITY - HAWAII
CENTRAL OREGON COMMUNITY COLLEGE
CENTENARY COLLEGE OF LOUISIANA
CHEMEKETA COMMUNITY COLLEGE
CLACKAMAS COMMUNITY COLLEGE
COLLEGE OF THE MARSHALL ISLANDS
COLUMBIA GORGE COMMUNITY COLLEGE
CONCORDIA UNIVERSITY
GEORGE FOX UNIVERSITY
KLAMATH COMMUNITY COLLEGE DISTRICT
LANE COMMUNITY COLLEGE
LEWIS AND CLARK COLLEGE
LINFIELD COLLEGE
LINN-BENTON COMMUNITY COLLEGE
LOUISIANA COLLEGE, LA
LOUISIANA STATE UNIVERSITY
LOUISIANA STATE UNIVERSITY HEALTH SERVICES
MARYLHURST UNIVERSITY
MT. HOOD COMMUNITY COLLEGE
MULTNOMAH BIBLE COLLEGE
NATIONAL COLLEGE OF NATURAL MEDICINE
NORTHWEST CHRISTIAN COLLEGE
OREGON HEALTH AND SCIENCE UNIVERSITY
OREGON INSTITUTE OF TECHNOLOGY
OREGON STATE UNIVERSITY
OREGON UNIVERSITY SYSTEM
PACIFIC UNIVERSITY
PIONEER PACIFIC COLLEGE
PORTLAND COMMUNITY COLLEGE
PORTLAND STATE UNIVERSITY
REED COLLEGE
RESEARCH CORPORATION OF THE UNIVERSITY OF
HAWAII
ROGUE COMMUNITY COLLEGE
SOUTHEASTERN LOUISIANA UNIVERSITY
SOUTHERN OREGON UNIVERSITY (OREGON
UNIVERSITY SYSTEM)

SOUTHWESTERN OREGON COMMUNITY COLLEGE
TULANE UNIVERSITY
TILLAMOOK BAY COMMUNITY COLLEGE
UMPQUA COMMUNITY COLLEGE
UNIVERSITY OF HAWAII BOARD OF REGENTS
UNIVERSITY OF HAWAII-HONOLULU COMMUNITY
COLLEGE
UNIVERSITY OF OREGON-GRADUATE SCHOOL
UNIVERSITY OF PORTLAND
UNIVERSITY OF NEW ORLEANS
WESTERN OREGON UNIVERSITY
WESTERN STATES CHIROPRACTIC COLLEGE
WILLAMETTE UNIVERSITY
XAVIER UNIVERSITY
UTAH SYSTEM OF HIGHER EDUCATION, UT
UNIVERSITY OF UTAH, UT
UTAH STATE UNIVERSITY, UT
WEBER STATE UNIVERSITY, UT
SOUTHERN UTAH UNIVERSITY, UT
SNOW COLLEGE, UT
DIXIE STATE COLLEGE, UT
COLLEGE OF EASTERN UTAH, UT
UTAH VALLEY UNIVERSITY, UT
SALT LAKE COMMUNITY COLLEGE, UT
UTAH COLLEGE OF APPLIED TECHNOLOGY, UT

STATE AGENCIES

ADMIN. SERVICES OFFICE
BOARD OF MEDICAL EXAMINERS
HAWAII CHILD SUPPORT ENFORCEMENT AGENCY
HAWAII DEPARTMENT OF TRANSPORTATION
HAWAII HEALTH SYSTEMS CORPORATION
OFFICE OF MEDICAL ASSISTANCE PROGRAMS
OFFICE OF THE STATE TREASURER
OREGON BOARD OF ARCHITECTS
OREGON CHILD DEVELOPMENT COALITION
OREGON DEPARTMENT OF EDUCATION
OREGON DEPARTMENT OF FORESTRY
OREGON DEPT OF TRANSPORTATION
OREGON DEPT. OF EDUCATION
OREGON LOTTERY
OREGON OFFICE OF ENERGY
OREGON STATE BOARD OF NURSING
OREGON STATE DEPT OF CORRECTIONS
OREGON STATE POLICE
OREGON TOURISM COMMISSION
OREGON TRAVEL INFORMATION COUNCIL
SANTIAM CANYON COMMUNICATION CENTER
SEIU LOCAL 503, OPEU
SOH- JUDICIARY CONTRACTS AND PURCH
STATE DEPARTMENT OF DEFENSE, STATE OF
HAWAII
STATE OF HAWAII
STATE OF HAWAII, DEPT. OF EDUCATION
STATE OF LOUISIANA
STATE OF LOUISIANA DEPT. OF EDUCATION
STATE OF LOUISIANA, 26TH JUDICIAL DISTRICT
ATTORNEY
STATE OF UTAH



7145 West Tidwell Road ~ Houston, Texas 77092
(713)-462-7708
www.esc4.net

NOTICE TO OFFEROR

ADDENDUM NO. 1

Solicitation Number 20-08

Request for Proposal (“RFP”)
by

Region 4 Education Service Center (“ESC”)
for

Cyber Security Solutions and Associated Products & Services

SUBMITTAL DEADLINE: Tuesday, April 7, 2020, 10:00 AM CENTRAL TIME

This Addendum No. 1 amends the Request for Proposals (RFP) for Cyber Security Solutions and Associated Products & Services 20-08 (“Addendum”). To the extent of any discrepancy between the original RFP and this Addendum, this Addendum shall prevail.

This Addendum No. 1 is hereby issued to:

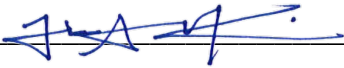
Replace APPENDIX D – Requirements for National Cooperative Contract to be Administered by OMNIA Partners in its entirety with the following attachment

RECEIPT OF ADDENDUM NO. 1 ACKNOWLEDGEMENT

Offeror shall acknowledge this addendum by signing below and include in their proposal response.

Company Name ThunderCat Technology, LLC

Contact Person Jean Kim

Signature  _____

Date 4/9/2020

Crystal Wallace
Region 4 Education Service Center
Business Operations Specialist



7145 West Tidwell Road ~ Houston, Texas 77092
(713)-462-7708
www.esc4.net

NOTICE TO OFFEROR

ADDENDUM NO. 2

Solicitation Number 20-08

Request for Proposal (“RFP”)
by

Region 4 Education Service Center (“ESC”)
for

Cyber Security Solutions and Associated Products and Services

SUBMITTAL DEADLINE: Tuesday, April 14, 2020, 10:00 AM CENTRAL TIME

This Addendum No. 2 amends the Request for Proposals (RFP) for Cyber Security Solutions and Associated Products and Services (“Addendum”). To the extent of any discrepancy between the original RFP and this Addendum, this Addendum shall prevail.

Region 4 Education Service Center (“Region 4 ESC”) requests proposals from qualified suppliers with the intent to enter into a Contract for Cyber Security Solutions and Associated Products and Services. Addendum No. 2 is hereby issued as follows:


1. **Submittal Deadline**: The submittal deadline for this RFP is hereby changed from Tuesday, April 7, 2020 @ 10:00 AM Central Time and extended as indicated below and above:
 - Tuesday, April 14, 2020 @ 10:00 AM Central Time

RECEIPT OF ADDENDUM NO.2 ACKNOWLEDGEMENT

Offeror shall acknowledge this addendum by signing below and include in their proposal response.

Company Name ThunderCat Technology, LLC

Contact Person Jean Kim

Signature  _____

Date 4/9/2020

Crystal Wallace
Region 4 Education Service Center
Business Operations Specialist



7145 West Tidwell Road ~ Houston, Texas 77092
(713)-462-7708
www.esc4.net

NOTICE TO OFFEROR

ADDENDUM NO. 3

Solicitation Number 20-08

Request for Proposal (“RFP”)
by

Region 4 Education Service Center (“ESC”)
for

Cyber Security Solutions and Associated Products and Services

SUBMITTAL DEADLINE: Tuesday, May 5, 2020, 10:00 AM CENTRAL TIME

This Addendum No. 3 amends the Request for Proposals (RFP) for Cyber Security Solutions and Associated Products and Services (“Addendum”). To the extent of any discrepancy between the original RFP and this Addendum, this Addendum shall prevail.

Region 4 Education Service Center (“Region 4 ESC”) requests proposals from qualified suppliers with the intent to enter into a Contract for Cyber Security Solutions and Associated Products and Services. Addendum No. 3 is hereby issued as follows:

- Submittal Deadline**: The submittal deadline for this RFP is hereby changed from Tuesday, April 14, 2020 @ 10:00 AM Central Time and extended as indicated below and above:
 - Tuesday, May 5, 2020 @ 10:00 AM Central Time
- Approval from Region 4 ESC**: Approval of contract award date is hereby changed from June 23, 2020 and extended as indicated below:
 - August 25, 2020 (*tentative and subject to change*)

RECEIPT OF ADDENDUM NO.3 ACKNOWLEDGEMENT

Offeror shall acknowledge this addendum by signing below and include in their proposal response.

Company Name ThunderCat Technology, LLC

Contact Person Jean Kim

Signature  _____

Date 6/11/2020

Crystal Wallace
Region 4 Education Service Center
Business Operations Specialist



7145 West Tidwell Road ~ Houston, Texas 77092

(713)-462-7708

www.esc4.net

NOTICE TO OFFEROR

ADDENDUM NO. 4

Solicitation Number 20-08

Request for Proposal (“RFP”)
by

Region 4 Education Service Center (“ESC”)
for

Cyber Security Solutions and Associated Products and Services

SUBMITTAL DEADLINE: Tuesday, May 5, 2020, 10:00 AM CENTRAL TIME

This Addendum No. 4 amends the Request for Proposals (RFP) for Cyber Security Solutions and Associated Products and Services (“Addendum”). To the extent of any discrepancy between the original RFP and this Addendum, this Addendum shall prevail.

Region 4 Education Service Center (“Region 4 ESC”) requests proposals from qualified suppliers with the intent to enter into a Contract for Cyber Security Solutions and Associated Products and Services. Addendum No. 4 is hereby issued as follows:

1. **Proposal Format:** The submission requirement in Section 5 in the “Instructions to Offerors” in this RFP is hereby revised as follows:
 - The requirement for two (2) bound copies is waived.
 - Offeror must submit their complete response on two (2) electronic copies; pin/flash drives. Offeror must also submit two (2) electronic proposals free of propriety information to be posted, if awarded a Contract.
2. **Required Documents**
 - Any document requiring appearance before a notary shall be waived until a later date or upon Region 4 ESC request.

RECEIPT OF ADDENDUM NO. 4 ACKNOWLEDGEMENT

Offeror shall acknowledge this addendum by signing below and include in their proposal response.

Company Name ThunderCat Technology, LLC

Contact Person Jean Kim

Signature  _____

Date 6/19/2020

Crystal Wallace
Region 4 Education Service Center
Business Operations Specialist



7145 West Tidwell Road ~ Houston, Texas 77092
(713)-462-7708
www.esc4.net

NOTICE TO OFFEROR

ADDENDUM NO. 5

Solicitation Number 20-08

Request for Proposal (“RFP”)
by

Region 4 Education Service Center (“ESC”)
for
Cyber Security Solutions and Associated Products and Services

SUBMITTAL DEADLINE: Thursday, June 18, 2020, 10:00 AM CENTRAL TIME

This Addendum No. 5 amends the Request for Proposals (RFP) for Cyber Security Solutions and Associated Products and Services (“Addendum”). To the extent of any discrepancy between the original RFP and this Addendum, this Addendum shall prevail.

Region 4 Education Service Center (“Region 4 ESC”) requests proposals from qualified suppliers with the intent to enter into a Contract for Cyber Security Solutions and Associated Products and Services. Addendum No. 5 is hereby issued as follows:

1. **Submittal Deadline:** The submittal deadline for this RFP is hereby changed from Tuesday, May 5, 2020 @ 10:00 AM Central Time and extended as indicated below and above:
 - Thursday, June 18, 2020 @ 10:00 AM Central Time

RECEIPT OF ADDENDUM NO. 5 ACKNOWLEDGEMENT

Offeror shall acknowledge this addendum by signing below and include in their proposal response.

Company Name ThunderCat Technology, LLC

Contact Person Jean Kim

Signature  _____

Date 4/24/2020

Crystal Wallace
Region 4 Education Service Center
Business Operations Specialist



7145 West Tidwell Road ~ Houston, Texas 77092
(713)-462-7708
www.esc4.net

NOTICE TO OFFEROR

ADDENDUM NO. 6

Solicitation Number 20-08

Request for Proposal (“RFP”)
by

Region 4 Education Service Center (“ESC”)
for
Cyber Security Solutions and Associated Products and Services

SUBMITTAL DEADLINE: Tuesday, July 14, 2020, 10:00 AM CENTRAL TIME

This Addendum No. 6 amends the Request for Proposals (RFP) for Cyber Security Solutions and Associated Products and Services (“Addendum”). To the extent of any discrepancy between the original RFP and this Addendum, this Addendum shall prevail.

Region 4 Education Service Center (“Region 4 ESC”) requests proposals from qualified suppliers with the intent to enter into a Contract for Cyber Security Solutions and Associated Products and Services. Addendum No. 6 is hereby issued as follows:


- 1. Submittal Deadline:** The submittal deadline for this RFP is hereby changed from Thursday, June 18, 2020 @ 10:00 AM Central Time and extended as indicated below and above:
 - Tuesday, July 14, 2020 @ 10:00 AM Central Time
- 2. Approval from Region 4 ESC:** The contract approval date is hereby changed from Tuesday, June 23, 2020 to:
 - Tuesday, August 25, 2020
- 3. Contract Effective Date:** The contract effective date is hereby changed from August 1, 2020 to:
 - October 1, 2020

RECEIPT OF ADDENDUM NO. 6 ACKNOWLEDGEMENT

Offeror shall acknowledge this addendum by signing below and include in their proposal response.

Company Name ThunderCat Technology, LLC

Contact Person Jean Kim

Signature 

Date 5/19/2020

Crystal Wallace
Region 4 Education Service Center
Business Operations Specialist