



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at wvOASIS.gov. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at WVPurchasing.gov with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header @ 5

List View

General Information | Contact | Default Values | Discount | Document Information | Clarification Request

Procurement Folder: 856640

Procurement Type: Central Contract - Fixed Amt

Vendor ID: VS0000038000

Legal Name: Corvid Cyberdefense, LLC

Alias/DBA: Corvid Technologies LLC

Total Bid: \$340,000.00

Response Date: 05/12/2021

Response Time: 11:46

Responded By User ID: thao.tran

First Name: Thao

Last Name: Tran

Email: thao.tran@corvidtec.com

Phone: 704-799-6944

SO Doc Code: CRFQ

SO Dept: 0231

SO Doc ID: OOT210000005

Published Date: 5/4/21

Close Date: 5/13/21

Close Time: 13:30

Status: Closed

Solicitation Description: Data Center 2.0 Firewall (OT21107)

Total of Header Attachments: 5

Total of All Attachments: 5

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	3.1.1 Palo Alto 5250 Next Gen Firewall, or Equal	2.00000	EA	67500.000000	135000.00

Comm Code	Manufacturer	Specification	Model #
43222501			

Commodity Line Comments: FG-3400E- please see additional specs or the attached data sheet. Delivery arrangements to be made during contract execution.

Extended Description:

3.1.1 Palo Alto 5250 Next Gen Firewall, or Equal

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	3.1.2 Installation Services	1.00000	EA	5000.000000	5000.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Installation should only take 1-2 days. Further implementation may be performed remotely.

Extended Description:

3.1.2 Installation Services

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	3.1.3 Palo Alto Premium Support, or equal	1.00000	YR	50000.000000	50000.00

Comm Code	Manufacturer	Specification	Model #
81112201			

Commodity Line Comments: FortiGate-3400E 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)

Extended Description:

3.1.3 Palo Alto Premium Support, or equal

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	3.1.5 Palo Alto Premium Support, or equal, YR 2	1.00000	YR	50000.000000	50000.00

Comm Code	Manufacturer	Specification	Model #
81112201			

Commodity Line Comments: FortiGate-3400E 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)

Extended Description:

3.1.5 Palo Alto Premium Support, or equal, YR 2

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
5	3.1.5 Palo Alto Premium Support, or equal, YR 3	1.00000	YR	50000.000000	50000.00

Comm Code	Manufacturer	Specification	Model #
81112201			

Commodity Line Comments: FortiGate-3400E 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)

Extended Description:

3.1.5 Palo Alto Premium Support, or equal, YR 3

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
6	3.1.5 Palo Alto Premium Support, or equal, YR 4	1.00000	YR	50000.000000	50000.00

Comm Code	Manufacturer	Specification	Model #
81112201			

Commodity Line Comments: FortiGate-3400E 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)

Extended Description:

3.1.5 Palo Alto Premium Support, or equal, YR 4



Thao Tran
Thao.Tran@corvidtec.com
153 Langtree Campus Drive Ste 401
 Mooresville, NC 28117
(p) 301-905-6330
(f) 704-799-7975

May 12, 2021

Jessica Chambers
Jessica.S.Chambers@wv.gov
2019 Washington Street, East
Charleston, WV 25305

Dear Jessica,

Thank you for the opportunity to present this proposal to the State of West Virginia.

Company Introduction

Corvid Technologies, LLC is a group of over 200 engineers and scientists, about 3/4 with master's degrees or Ph.D.'s, that provide end-to-end solutions including concept development, design and optimization, prototype build, test and manufacture. Geographically, the core of the team is based within the Carolinas, concentrated around the HQ in Mooresville, where our primary SOC is located. Our secondary SOC is located in Alabama.

Corvid Cyberdefense is the cybersecurity division of Corvid Technologies, a provider of complex, technology-based engineering solutions. 25 of our employees are engineers, analysts, and cybersecurity SMEs dedicated to delivering Managed Security Services (MSS). 90% of our staff dedicated to MSS delivery have applicable certifications. These security/cyber certifications include: CISSP, CCNA, CCNA-Wireless, CCNA-Security, PCNSC, PCNSE, GAIC Certified Handler, SANS, Ethical Hacking/Digital Forensics, GCED, GYPC, GCTI, GCIA, CCNA Cyber Ops, Cylance Security Professional, XSOAR Certified, LRSA, LRPA, Comp TIA Security/Network/Server+, A+, CREA, Reverse Engineering. Given our extensive experience within the Department of Defense, several of our staff also have DoD Secret & Top-Secret clearances.

Corvid Cyberdefense has over 175 active customers around the country, handling over 5.7 billion events (Firewall/Endpoint) each quarter. Today we are an award-winning IT security company assisting clients ranging from SMB to Fortune 100, offering advisory, technology, and managed cybersecurity solutions.

Regards,
Thao Tran
Thao Tran
Procurement Specialist



Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

State of West Virginia
 Centralized Request for Quote
 Info Technology

Proc Folder: 856640			Reason for Modification:
Doc Description: Data Center 2.0 Firewall (OT21107)			
Proc Type: Central Contract - Fixed Amt			
Date Issued	Solicitation Closes	Solicitation No	Version
2021-04-01	2021-04-15 13:30	CRFQ 0231 OOT210000005	1

BID RECEIVING LOCATION

BID CLERK
 DEPARTMENT OF ADMINISTRATION
 PURCHASING DIVISION
 2019 WASHINGTON ST E
 CHARLESTON WV 25305
 US

VENDOR

Vendor Customer Code:

Vendor Name :

Address :

Street :

City :

State : **Country :** **Zip :**

Principal Contact :

Vendor Contact Phone: **Extension:**

FOR INFORMATION CONTACT THE BUYER
 Jessica S Chambers
 (304) 558-0246
 jessica.s.chambers@wv.gov

Vendor Signature X **FEIN#** **DATE**

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) for the purchase of two (2) Palo Alto PA-5250 Next Generation Firewalls, or equal, and professional services. These firewalls will be implemented in the WVOT's Data Center 2.0 Project per the terms and conditions and specifications as attached.

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV 25305 US	DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 908 BULLITT ST CHARLESTON WV 25301-1002 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	3.1.1 Palo Alto 5250 Next Gen Firewall, or Equal	2.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222501			

Extended Description:

3.1.1 Palo Alto 5250 Next Gen Firewall, or Equal

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV 25305 US	DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 908 BULLITT ST CHARLESTON WV 25301-1002 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	3.1.2 Installation Services	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:

3.1.2 Installation Services

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV 25305 US	DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 908 BULLITT ST CHARLESTON WV 25301-1002 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	3.1.3 Palo Alto Premium Support, or equal	1.00000	YR		

Comm Code	Manufacturer	Specification	Model #
81112201			

Extended Description:

3.1.3 Palo Alto Premium Support, or equal

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV 25305 US	DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 908 BULLITT ST CHARLESTON WV 25301-1002 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	3.1.5 Palo Alto Premium Support, or equal, YR 2	1.00000	YR		

Comm Code	Manufacturer	Specification	Model #
81112201			

Extended Description:

3.1.5 Palo Alto Premium Support, or equal, YR 2

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV 25305 US	DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 908 BULLITT ST CHARLESTON WV 25301-1002 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	3.1.5 Palo Alto Premium Support, or equal, YR 3	1.00000	YR		

Comm Code	Manufacturer	Specification	Model #
81112201			

Extended Description:
3.1.5 Palo Alto Premium Support, or equal, YR 3

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV 25305 US	DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 908 BULLITT ST CHARLESTON WV 25301-1002 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
6	3.1.5 Palo Alto Premium Support, or equal, YR 4	1.00000	YR		

Comm Code	Manufacturer	Specification	Model #
81112201			

Extended Description:
3.1.5 Palo Alto Premium Support, or equal, YR 4

SCHEDULE OF EVENTS

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	TECHNICAL QUESTION DEADLINE	2021-04-09

INSTRUCTIONS TO VENDORS SUBMITTING BIDS

1. REVIEW DOCUMENTS THOROUGHLY: The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualification of a Vendor's bid. All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid.

2. MANDATORY TERMS: The Solicitation may contain mandatory provisions identified by the use of the words "must," "will," and "shall." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.

3. PREBID MEETING: The item identified below shall apply to this Solicitation.

A pre-bid meeting will not be held prior to bid opening

A **MANDATORY PRE-BID** meeting will be held at the following place and time:

All Vendors submitting a bid must attend the mandatory pre-bid meeting. Failure to attend the mandatory pre-bid meeting shall result in disqualification of the Vendor's bid. No one individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing.

Additionally, the person attending the pre-bid meeting should include the Vendor's E-Mail address, phone number, and Fax number on the attendance sheet. It is the Vendor's responsibility to locate the attendance sheet and provide the required information. Failure to complete the attendance sheet as required may result in disqualification of Vendor's bid.

All Vendors should arrive prior to the starting time for the pre-bid. Vendors who arrive after the starting time but prior to the end of the pre-bid will be permitted to sign in but are charged with knowing all matters discussed at the pre-bid.

Questions submitted at least five business days prior to a scheduled pre-bid will be discussed at the pre-bid meeting if possible. Any discussions or answers to questions at the pre-bid meeting

are preliminary in nature and are non-binding. Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.

4. VENDOR QUESTION DEADLINE: Vendors may submit questions relating to this Solicitation to the Purchasing Division. Questions must be submitted in writing. All questions must be submitted on or before the date listed below and to the address listed below in order to be considered. A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are nonbinding.

Submitted e-mails should have solicitation number in the subject line.

Question Submission Deadline: April 9, 2021 at 9:00 AM (ET)

Submit Questions to: Jessica Chambers

2019 Washington Street, East

Charleston, WV 25305

Fax: (304) 558-4115 (Vendors should not use this fax number for bid submission)

Email: Jessica.S.Chambers@wv.gov

5. VERBAL COMMUNICATION: Any verbal communication between the Vendor and any State personnel is not binding, including verbal communication at the mandatory pre-bid conference. Only information issued in writing and added to the Solicitation by an official written addendum by the Purchasing Division is binding.

6. BID SUBMISSION: All bids must be submitted electronically through wvOASIS or signed and delivered by the Vendor to the Purchasing Division at the address listed below on or before the date and time of the bid opening. Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason. The Purchasing Division will not accept bids, modification of bids, or addendum acknowledgment forms via e-mail. Acceptable delivery methods include electronic submission via wvOASIS, hand delivery, delivery by courier, or facsimile.

The bid delivery address is:

Department of Administration, Purchasing Division

2019 Washington Street East

Charleston, WV 25305-0130

A bid that is not submitted electronically through wvOASIS should contain the information listed below on the face of the envelope or the bid may be rejected by the Purchasing Division.:

SEALED BID:

BUYER: Jessica Chambers

SOLICITATION NO.: CRFQ OOT2100000005

BID OPENING DATE: 4/15/2021

BID OPENING TIME: 1:30 PM (ET)

FAX NUMBER: (304)558-3970

Revised 03/15/2021

The Purchasing Division may prohibit the submission of bids electronically through wvOASIS at its sole discretion. Such a prohibition will be contained and communicated in the wvOASIS system resulting in the Vendor's inability to submit bids through wvOASIS. Submission of a response to a Request for Proposal is not permitted in wvOASIS.

For Request For Proposal ("RFP") Responses Only: In the event that Vendor is responding to a request for proposal, the Vendor shall submit one original technical and one original cost proposal plus _____convenience copies of each to the Purchasing Division at the address shown above. Additionally, the Vendor should identify the bid type as either a technical or cost proposal on the face of each bid envelope submitted in response to a request for proposal as follows:

BID TYPE: (This only applies to CRFP)

Technical

Cost

7. BID OPENING: Bids submitted in response to this Solicitation will be opened at the location identified below on the date and time listed below. Delivery of a bid after the bid opening date and time will result in bid disqualification. For purposes of this Solicitation, a bid is considered delivered when confirmation of delivery is provided by wvOASIS (in the case of electronic submission) or when the bid is time stamped by the official Purchasing Division time clock (in the case of hand delivery).

Bid Opening Date and Time: April 15, 2021 at 1:30 PM (ET)

Bid Opening Location: Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

8. ADDENDUM ACKNOWLEDGEMENT: Changes or revisions to this Solicitation will be made by an official written addendum issued by the Purchasing Division. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing an Addendum Acknowledgment Form, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

9. BID FORMATTING: Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification.

10. ALTERNATE MODEL OR BRAND: Unless the box below is checked, any model, brand, or specification listed in this Solicitation establishes the acceptable level of quality only and is not intended to reflect a preference for, or in any way favor, a particular brand or vendor. Vendors may bid alternates to a listed model or brand provided that the alternate is at least equal to the model or brand and complies with the required specifications. The equality of any alternate being bid shall be determined by the State at its sole discretion. Any Vendor bidding an alternate model or brand should clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the

equality of the alternate items. Failure to provide information for alternate items may be grounds for rejection of a Vendor's bid.

This Solicitation is based upon a standardized commodity established under W. Va. Code § 5A-3-61. Vendors are expected to bid the standardized commodity identified. Failure to bid the standardized commodity will result in your firm's bid being rejected.

11. EXCEPTIONS AND CLARIFICATIONS: The Solicitation contains the specifications that shall form the basis of a contractual agreement. Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid. Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation may result in bid disqualification.

12. COMMUNICATION LIMITATIONS: In accordance with West Virginia Code of State Rules §148-1-6.6, communication with the State of West Virginia or any of its employees regarding this Solicitation during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited without prior Purchasing Division approval. Purchasing Division approval for such communication is implied for all agency delegated and exempt purchases.

13. REGISTRATION: Prior to Contract award, the apparent successful Vendor must be properly registered with the West Virginia Purchasing Division and must have paid the \$125 fee, if applicable.

14. UNIT PRICE: Unit prices shall prevail in cases of a discrepancy in the Vendor's bid.

15. PREFERENCE: Vendor Preference may be requested in purchases of motor vehicles or construction and maintenance equipment and machinery used in highway and other infrastructure projects. Any request for preference must be submitted in writing with the bid, must specifically identify the preference requested with reference to the applicable subsection of West Virginia Code § 5A-3-37, and must include with the bid any information necessary to evaluate and confirm the applicability of the requested preference. A request form to help facilitate the request can be found at:

<http://www.state.wv.us/admin/purchase/vrc/Venpref.pdf>.

15A. RECIPROCAL PREFERENCE: The State of West Virginia applies a reciprocal preference to all solicitations for commodities and printing in accordance with W. Va. Code § 5A-3-37(b). In effect, non-resident vendors receiving a preference in their home states, will see that same preference granted to West Virginia resident vendors bidding against them in West Virginia. Any request for reciprocal preference must include with the bid any information necessary to evaluate and confirm the applicability of the preference. A request form to help facilitate the request can be found at: <http://www.state.wv.us/admin/purchase/vrc/Venpref.pdf>.

16. SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESSES: For any solicitations publicly advertised for bid, in accordance with West Virginia Code §5A-3-37(a)(7) and W. Va. CSR § 148-22-9, any non-resident vendor certified as a small, women-owned, or minority-owned business under W. Va. CSR § 148-22-9 shall be provided the same preference made available to any resident vendor. Any non-resident small, women-owned, or

minority-owned business must identify itself as such in writing, must submit that writing to the Purchasing Division with its bid, and must be properly certified under W. Va. CSR § 148-22-9 prior to contract award to receive the preferences made available to resident vendors. Preference for a non-resident small, women-owned, or minority owned business shall be applied in accordance with W. Va. CSR § 148-22-9.

17. WAIVER OF MINOR IRREGULARITIES: The Director reserves the right to waive minor irregularities in bids or specifications in accordance with West Virginia Code of State Rules § 148-1-4.6.

18. ELECTRONIC FILE ACCESS RESTRICTIONS: Vendor must ensure that its submission in wvOASIS can be accessed and viewed by the Purchasing Division staff immediately upon bid opening. The Purchasing Division will consider any file that cannot be immediately accessed and viewed at the time of the bid opening (such as, encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires, and are therefore unacceptable. A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after bid opening to make a file viewable if those documents are required with the bid. A Vendor may be required to provide document passwords or remove access restrictions to allow the Purchasing Division to print or electronically save documents provided that those documents are viewable by the Purchasing Division prior to obtaining the password or removing the access restriction.

19. NON-RESPONSIBLE: The Purchasing Division Director reserves the right to reject the bid of any vendor as Non-Responsible in accordance with W. Va. Code of State Rules § 148-1-5.3, when the Director determines that the vendor submitting the bid does not have the capability to fully perform, or lacks the integrity and reliability to assure good-faith performance.”

20. ACCEPTANCE/REJECTION: The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules § 148-1-4.5. and § 148-1-6.4.b.”

21. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor’s entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled “confidential,” “proprietary,” “trade secret,” “private,” or labeled with any other claim against public disclosure of the documents, to include any “trade secrets” as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

22. INTERESTED PARTY DISCLOSURE: West Virginia Code § 6D-1-2 requires that the vendor submit to the Purchasing Division a disclosure of interested parties to the contract for all contracts with an actual or estimated value of at least \$1 Million. That disclosure must occur on the form prescribed and approved by the WV Ethics Commission prior to contract award. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

23. WITH THE BID REQUIREMENTS: In instances where these specifications require documentation or other information with the bid, and a vendor fails to provide it with the bid, the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award pursuant to the authority to waive minor irregularities in bids or specifications under W. Va. CSR § 148-1-4.6. This authority does not apply to instances where state law mandates receipt with the bid.

24. E-MAIL NOTIFICATION OF AWARD: The Purchasing Division will attempt to provide bidders with e-mail notification of contract award when a solicitation that the bidder participated in has been awarded. For notification purposes, bidders must provide the Purchasing Division with a valid email address in the bid response. Bidders may also monitor wvOASIS or the Purchasing Division's website to determine when a contract has been awarded.

GENERAL TERMS AND CONDITIONS:

1. CONTRACTUAL AGREEMENT: Issuance of a Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

2. DEFINITIONS: As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

2.1. "Agency" or "Agencies" means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

2.2. "Bid" or "Proposal" means the vendors submitted response to this solicitation.

2.3. "Contract" means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

2.4. "Director" means the Director of the West Virginia Department of Administration, Purchasing Division.

2.5. "Purchasing Division" means the West Virginia Department of Administration, Purchasing Division.

2.6. "Award Document" means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

2.7. "Solicitation" means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

2.8. "State" means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

2.9. "Vendor" or "Vendors" means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

3. CONTRACT TERM; RENEWAL; EXTENSION: The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

Term Contract

Initial Contract Term: This Contract becomes effective on Upon Award and the initial contract term extends until _____.

Renewal Term: This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to Three (3) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

Alternate Renewal Term – This contract may be renewed for _____ successive _____ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

Delivery Order Limitations: In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

Fixed Period Contract: This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within _____ days.

Fixed Period Contract with Renewals: This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within _____ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that maintenance, monitoring, or warranty services will be provided for _____ year(s) thereafter.

One Time Purchase: The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

Other: See attached _____

4. AUTHORITY TO PROCEED: Vendor is authorized to begin performance of this contract on the date of encumbrance listed on the front page of the Award Document unless either the box for “Fixed Period Contract” or “Fixed Period Contract with Renewals” has been checked in Section 3 above. If either “Fixed Period Contract” or “Fixed Period Contract with Renewals” has been checked, Vendor must not begin work until it receives a separate notice to proceed from the State. The notice to proceed will then be incorporated into the contract via change order to memorialize the official date that work commenced.

5. QUANTITIES: The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

Open End Contract: Quantities listed in this Solicitation are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

Service: The scope of the service to be provided will be more clearly defined in the specifications included herewith.

Combined Service and Goods: The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.

One Time Purchase: This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General’s office.

6. EMERGENCY PURCHASES: The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One Time Purchase contract.

7. REQUIRED DOCUMENTS: All of the items checked below must be provided to the Purchasing Division by the Vendor as specified below.

BID BOND (Construction Only): Pursuant to the requirements contained in W. Va. Code § 5-22-1(c), All Vendors submitting a bid on a construction project shall furnish a valid bid bond in the amount of five percent (5%) of the total amount of the bid protecting the State of West Virginia. The bid bond must be submitted with the bid.

PERFORMANCE BOND: The apparent successful Vendor shall provide a performance bond in the amount of 100% of the contract. The performance bond must be received by the Purchasing Division prior to Contract award.

LABOR/MATERIAL PAYMENT BOND: The apparent successful Vendor shall provide a labor/material payment bond in the amount of 100% of the Contract value. The labor/material payment bond must be delivered to the Purchasing Division prior to Contract award.

In lieu of the Bid Bond, Performance Bond, and Labor/Material Payment Bond, the Vendor may provide certified checks, cashier's checks, or irrevocable letters of credit. Any certified check, cashier's check, or irrevocable letter of credit provided in lieu of a bond must be of the same amount and delivered on the same schedule as the bond it replaces. A letter of credit submitted in lieu of a performance and labor/material payment bond will only be allowed for projects under \$100,000. Personal or business checks are not acceptable. Notwithstanding the foregoing, West Virginia Code § 5-22-1 (d) mandates that a vendor provide a performance and labor/material payment bond for construction projects. Accordingly, substitutions for the performance and labor/material payment bonds for construction projects is not permitted.

MAINTENANCE BOND: The apparent successful Vendor shall provide a two (2) year maintenance bond covering the roofing system. The maintenance bond must be issued and delivered to the Purchasing Division prior to Contract award.

LICENSE(S) / CERTIFICATIONS / PERMITS: In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits upon request and in a form acceptable to the State. The request may be prior to or after contract award at the State's sole discretion.

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications regardless of whether or not that requirement is listed above.

8. INSURANCE: The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below and must include the State as an additional insured on each policy prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether or not that insurance requirement is listed in this section.

Vendor must maintain:

Commercial General Liability Insurance in at least an amount of: \$1,000,000.00 per occurrence.

Automobile Liability Insurance in at least an amount of: _____ per occurrence.

Professional/Malpractice/Errors and Omission Insurance in at least an amount of: \$1,000,000.00 per occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

Commercial Crime and Third Party Fidelity Insurance in an amount of: _____ per occurrence.

Cyber Liability Insurance in an amount of: \$1,000,000.00 per occurrence.

Builders Risk Insurance in an amount equal to 100% of the amount of the Contract.

Pollution Insurance in an amount of: _____ per occurrence.

Aircraft Liability in an amount of: _____ per occurrence.

Notwithstanding anything contained in this section to the contrary, the Director of the Purchasing Division reserves the right to waive the requirement that the State be named as an additional insured on one or more of the Vendor's insurance policies if the Director finds that doing so is in the State's best interest.

9. WORKERS' COMPENSATION INSURANCE: The apparent successful Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

10. [Reserved]

11. LIQUIDATED DAMAGES: This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

_____ for _____

Liquidated Damages Contained in the Specifications

12. ACCEPTANCE: Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

13. PRICING: The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.

14. PAYMENT IN ARREARS: Payment in advance is prohibited under this Contract. Payment may only be made after the delivery and acceptance of goods or services. The Vendor shall submit invoices, in arrears.

15. PAYMENT METHODS: Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

16. TAXES: The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

17. ADDITIONAL FEES: Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

18. FUNDING: This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available.

19. CANCELLATION: The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.b.

20. TIME: Time is of the essence with regard to all matters of time and performance in this Contract.

21. APPLICABLE LAW: This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code or West Virginia Code of State Rules is void and of no effect.

22. COMPLIANCE WITH LAWS: Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

23. ARBITRATION: Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

24. MODIFICATIONS: This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

25. WAIVER: The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

26. SUBSEQUENT FORMS: The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

27. ASSIGNMENT: Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

28. WARRANTY: The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

29. STATE EMPLOYEES: State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

30. PRIVACY, SECURITY, AND CONFIDENTIALITY: The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in <http://www.state.wv.us/admin/purchase/privacy/default.html>.

31. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

32. LICENSING: In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

33. ANTITRUST: In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

34. VENDOR CERTIFICATIONS: By signing its bid or entering into this Contract, Vendor certifies (1) that its bid or offer was made without prior understanding, agreement, or connection with any corporation, firm, limited liability company, partnership, person or entity submitting a bid or offer for the same material, supplies, equipment or services; (2) that its bid or offer is in all respects fair and without collusion or fraud; (3) that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; and (4) that it has reviewed this Solicitation in its entirety; understands the requirements, terms and conditions, and other information contained herein.

Vendor's signature on its bid or offer also affirms that neither it nor its representatives have any interest, nor shall acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency. The individual signing this bid or offer on behalf of Vendor certifies that he or she is authorized by the Vendor to execute this bid or offer or any documents related thereto on Vendor's behalf; that he or she is authorized to bind the Vendor in a contractual relationship; and that, to the best of his or her knowledge, the Vendor has properly registered with any State agency that may require registration.

35. VENDOR RELATIONSHIP: The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

36. INDEMNIFICATION: The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

37. PURCHASING AFFIDAVIT: In accordance with West Virginia Code §§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State, Vendors are required to sign, notarize, and submit the Purchasing Affidavit to the Purchasing Division affirming under oath that it is not in default on any monetary obligation owed to the state or a political subdivision of the state.

38. ADDITIONAL AGENCY AND LOCAL GOVERNMENT USE: This Contract may be utilized by other agencies, spending units, and political subdivisions of the State of West Virginia; county, municipal, and other local government bodies; and school districts (“Other Government Entities”), provided that both the Other Government Entity and the Vendor agree. Any extension of this Contract to the aforementioned Other Government Entities must be on the same prices, terms, and conditions as those offered and agreed to in this Contract, provided that such extension is in compliance with the applicable laws, rules, and ordinances of the Other Government Entity. A refusal to extend this Contract to the Other Government Entities shall not impact or influence the award of this Contract in any manner.

39. CONFLICT OF INTEREST: Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

40. REPORTS: Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at purchasing.requisitions@wv.gov.

41. BACKGROUND CHECK: In accordance with W. Va. Code § 15-2D-3, the Director of the Division of Protective Services shall require any service provider whose employees are regularly employed on the grounds or in the buildings of the Capitol complex or who have access to sensitive or critical information to submit to a fingerprint-based state and federal background inquiry through the state repository. The service provider is responsible for any costs associated with the fingerprint-based state and federal background inquiry.

After the contract for such services has been approved, but before any such employees are permitted to be on the grounds or in the buildings of the Capitol complex or have access to sensitive or critical information, the service provider shall submit a list of all persons who will be physically present and working at the Capitol complex to the Director of the Division of Protective Services for purposes of verifying compliance with this provision. The State reserves the right to prohibit a service provider’s employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check.

Revised 03/15/2021

Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

42. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS: Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code § 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code § 5A-3-56. As used in this section:

- a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.
- b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open heath, basic oxygen, electric furnace, Bessemer or other steel making process. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:
- c. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars (\$2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or
- d. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

43. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL: In Accordance with W. Va. Code § 5-19-1 et seq., and W. Va. CSR § 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars (\$50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a

“substantial labor surplus area”, as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

44. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE: W. Va. Code § 6D-1-2 requires that for contracts with an actual or estimated value of at least \$1 million, the vendor must submit to the Agency a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-award interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

45. PROHIBITION AGAINST USED OR REFURBISHED: Unless expressly permitted in the solicitation published by the State, Vendor must provide new, unused commodities, and is prohibited from supplying used or refurbished commodities, in fulfilling its responsibilities under this Contract.

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

Thao Tran, Procurement Specialist

(Name, Title)

Thao Tran, Procurement Specialist

(Printed Name and Title)

153 Langtree Campus Drive Suite 401 Mooresville, NC 28117

(Address)

704-799-6944

(Phone Number) / (Fax Number)

thao.tran@corvidtec.com

(email address)

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

Corvid Cyberdefense, LLC

(Company)



Matt Hurley, Chief Operating Officer

(Authorized Signature) (Representative Name, Title)

Matt Hurley, Chief Operating Officer

(Printed Name and Title of Authorized Representative)

5/11/2021

(Date)

703-731-5325

704-799-7975

(Phone Number) (Fax Number)

REQUEST FOR QUOTATION
Next-Gen Firewalls for DC2.0 (OT21107)

SPECIFICATIONS

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) for the purchase of two (2) Palo Alto PA-5250 Next Generation Firewalls, or equal, and professional services. These firewalls will be implemented in the WVOT's Data Center 2.0 Project.
2. **DEFINITIONS:** The terms listed below shall have the meanings assigned to them below. Additional definitions can be found in section 2 of the General Terms and Conditions.
 - 2.1 **"Contract Item"** means firewall appliances as more fully described by these specifications.
 - 2.2 **"Pricing Page"** means the pages, contained in wvOASIS or attached as Exhibit A, upon which Vendor should list its proposed price for the Contract Items.
 - 2.3 **"Solicitation"** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.
 - 2.4 **"GB"** means gigabyte which is a multiple of the unit byte for digital information.
 - 2.5 **"Gbps"** means gigabits per second, a data transfer speed measurement for high-speed networks such as gigabit ethernet.
 - 2.6 **"FIPS 140-2"** stands for Federal Information Processing Standard (FIPS) Publication 140-2 which is a U.S. government computer security standard used to approve cryptographic modules.
 - 2.7 **"Mbps"** means megabits per second which is a unit of measurement for bandwidth and throughput on a network.
 - 2.8 **"NBD"** stands for next business day.
 - 2.9 **"RMA"** means Return Material Authorization
 - 2.10 **"OEM"** means original equipment manufacturer.
 - 2.11 **"VLAN"** means Virtual Local Area Network.
 - 2.12 **"DNS"** means Domain Name Servers which is the Internet's system for converting alphabetic names into numeric IP addresses.
 - 2.13 **"DMZ"** means Demilitarized Zone which is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.

REQUEST FOR QUOTATION
Next-Gen Firewalls for DC2.0 (OT21107)

3. GENERAL REQUIREMENTS:

3.1 Mandatory Contract Item Requirements: Contract Item must meet or exceed the mandatory requirements listed below.

3.1.1 Two (2) Palo Alto PA-5250 Next-Generation Firewall or equal

3.1.1.1 Must be FIPS 140-2 validated. Vendor must provide the certificate number of the module validated if requested. The link to provide the certificate can be found here.

<https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search>

3.1.1.2 Must receive software updates from designated servers located in the US.

3.1.1.3 Must have a minimum Firewall Throughput of 35 Gbps

3.1.1.4 Must have a minimum Threat Prevention Throughput of ten (10) Gbps.

3.1.1.5 Must be able to use in an Active/Passive configuration to ensure High Availability.

3.1.1.6 System must have audit logs that document security-related events.

3.1.1.7 System must lock administrator accounts after no more than three unsuccessful attempts to logon with an invalid password.

3.1.1.8 System must be configurable to require multi-factor authentication for remote device management.

3.1.1.9 System must not display passwords in clear text during login.

3.1.1.10 Must have an Intrusion Prevention Service that provides the latest defenses against network-based threats.

3.1.1.11 Must have a DNS Filter that blocks DNS requests to known botnet command and control addresses. Vendor must maintain a database of known botnet command and control addresses.

3.1.1.12 Must have Antivirus protection that covers automated content updates and also malware and heuristic detection engines.

REQUEST FOR QUOTATION
Next-Gen Firewalls for DC2.0 (OT21107)

- 3.1.1.13 Must have Web Application Firewall (WAF) to protect against SQL injection, cross-site scripting, web robot patterns, and suspicious URLs.
- 3.1.1.14 Must have the ability to identify infected hosts that try to connect to malicious domains.
- 3.1.1.15 Must have redundant power supplies.
- 3.1.1.16 Must have a rack mounting kit and any cables necessary to configure the firewalls in an active/standby state.
- 3.1.1.17 Vendor must include any and all licenses required to meet the mandatory specifications.
- 3.1.1.18 Must be capable of being centrally managed via state-used Panorama Version 9.16
- 3.1.1.19 Must have 5TB of Cortex Data Lake Storage, or equivalent 5TB of storage that can be configured for log storage.
- 3.1.1.20 Must have a minimum of four (4) SFP+ form factor, SR 10GB optical transceiver, short reach 300m, duplex LC, IEEE 802.3ae 10GBASE-SR compliant.
- 3.1.1.21 Vendor must be an authorized reseller of all equipment bid and provide proof of authorization from OEM. All equipment must be new and genuine. Refurbished and/or gray market equipment will not be accepted.

3.1.2 Initial Configuration Professional Services

- 3.1.2.1 Vendor must perform physical installation of all devices, transceivers, or modules.
- 3.1.2.2 Vendor must configure all licensed features.
- 3.1.2.3 Vendor must configure the devices into a high-availability cluster.
- 3.1.2.4 Vendor must provision existing VLANs used to segment the agency networks.

REQUEST FOR QUOTATION
Next-Gen Firewalls for DC2.0 (OT21107)

3.1.3 Palo Alto Premium Support or Equal

3.1.3.1 Must have 24x7x365 technical support.

3.1.3.2 Technical Support must be provided by U.S. Citizens located in the United States. No offshore access is permitted.

3.1.3.3 Must receive software updates and patches from the vendor's servers located within the United States.

3.1.3.4 Must be able to escalate case severity level when higher priority is required. Severity will be determined at the discretion of the State.

3.1.3.5 Must have a Next Business Day or sooner RMA option.

3.1.4 Vendor must sign and agree to the State of WV Cloud Addendum, attached to this solicitation.

3.1.5 Vendor should include pricing for Optional Annual Renewals Years 2, 3, and 4 for maintenance and support. Optional Annual Renewal Years will be initiated by the Agency, agreed to by the Vendor, and executed via formal Change Order issued by the WV Purchasing Division.

4. CONTRACT AWARD:

4.1 Contract Award: The Contract is intended to provide Agencies with a purchase price for the Contract Items. The Contract shall be awarded to the Vendor that provides the Contract Items meeting the required specifications for the lowest overall total cost as shown on the Pricing Pages.

4.2 Pricing Page: Vendor should complete the Pricing Page by completing Exhibit A. Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

5. PAYMENT:

5.1 Payment: Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.

6. DELIVERY AND RETURN:

REQUEST FOR QUOTATION
Next-Gen Firewalls for DC2.0 (OT21107)

6.1 Shipment and Delivery: Vendor shall ship the Contract Items immediately after being awarded this Contract and receiving a purchase order or notice to proceed. Vendor shall deliver the Contract Items within 15 calendar days after receiving a purchase order or notice to proceed. Contract Items must be delivered to Agency at 908 Bullitt Street, Charleston, WV 25301.

6.2 Late Delivery: The Agency placing the order under this Contract must be notified in writing if the shipment of the Contract Items will be delayed for any reason. Any delay in delivery that could cause harm to an Agency will be grounds for cancellation of the Contract, and/or obtaining the Contract Items from a third party.

Any Agency seeking to obtain the Contract Items from a third party under this provision must first obtain approval of the Purchasing Division.

6.3 Delivery Payment/Risk of Loss: Vendor shall deliver the Contract Items F.O.B. destination to the Agency's location.

6.4 Return of Unacceptable Items: If the Agency deems the Contract Items to be unacceptable, the Contract Items shall be returned to Vendor at Vendor's expense and with no restocking charge. Vendor shall either make arrangements for the return within five (5) days of being notified that items are unacceptable, or permit the Agency to arrange for the return and reimburse Agency for delivery expenses. If the original packaging cannot be utilized for the return, Vendor will supply the Agency with appropriate return packaging upon request. All returns of unacceptable items shall be F.O.B. the Agency's location. The returned product shall either be replaced, or the Agency shall receive a full credit or refund for the purchase price, at the Agency's discretion.

6.5 Return Due to Agency Error: Items ordered in error by the Agency will be returned for credit within 30 days of receipt, F.O.B. Vendor's location. Vendor shall not charge a restocking fee if returned products are in a resalable condition. Items shall be deemed to be in a resalable condition if they are unused and in the original packaging. Any restocking fee for items not in a resalable condition shall be the lower of the Vendor's customary restocking fee or 5% of the total invoiced value of the returned items.

7 VENDOR DEFAULT:

7.1 The following shall be considered a vendor default under this Contract.

7.1.1 Failure to provide Contract Items in accordance with the requirements contained herein.

7.1.2 Failure to comply with other specifications and requirements contained herein.

7.1.3 Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.

7.1.4 Failure to remedy deficient performance upon request.

REQUEST FOR QUOTATION
Next-Gen Firewalls for DC2.0 (OT21107)

7.2 The following remedies shall be available to Agency upon default.

7.2.1 Immediate cancellation of the Contract.

7.2.2 Immediate cancellation of one or more release orders issued under this Contract.

7.2.3 Any other remedies available in law or equity.

Software as a Service Addendum

1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at <https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN>.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

Public Jurisdiction means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

Public Jurisdiction Data means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

Public Jurisdiction Identified Contact means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

Restricted data means personal data and non-public data.

Security Incident means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

Service Provider means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

Software-as-a-Service (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection and Privacy: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

- a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

- b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.
- c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.
- d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.
- e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.
- f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.
- g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.
- h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.
- i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to *store* public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

4. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

- a) Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.
- b) Security Incident Reporting Requirements: The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.
- c) Breach Reporting Requirements: Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and the public jurisdiction point of contact for general contract oversight/administration.

5. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

- a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

- b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.
- c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.
- d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
- e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any

type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

6. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

- a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.
- b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.
- c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:
 - 10 days after the effective date of termination, if the termination is in accordance with the contract period
 - 30 days after the effective date of termination, if the termination is for convenience
 - 60 days after the effective date of termination, if the termination is for cause

After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

- d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.
- e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

8. Background Checks: The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

of the contract, including subcontractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

9. Oversight of Authorized Persons: During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

10. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

11. Data Protection Self-Assessment: The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

12. Data Center Audit: The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

13. Change Control and Advance Notice: The service provider shall give 30 days, advance notice (to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics.

14. Security:

- a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; (3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

- b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.
- c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

15. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

17. Responsibilities: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

18. Subcontractor Compliance: The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

24. Subscription Terms: Service provider grants to a public jurisdiction a license to:

- a. Access and use the service for its business purposes;
- b. For SaaS, use underlying software as embodied or used in the service; and
- c. View, copy, upload, download (where applicable), and use service provider's documentation.

25. Equitable Relief: Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

Name of Agency: _____

Name of Vendor: Corvid Cyberdefense, LLC

Signature: _____

Signature:  _____

Title: _____

Title: Chief Operating Officer

Date: _____

Date: 5/11/2021

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: Corvid Cybedeense, LLC.

Name of Agency: WVOT

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
Yes
No
2. If yes to #1, does the restricted information include personal data?
Yes
No
3. If yes to #1, does the restricted information include non-public data?
Yes
No
4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
Yes
No
5. Provide name and email address for the Department privacy officer:

Name: Jennelle Jones

Email address: Jennelle.H.Jones@wv.gov

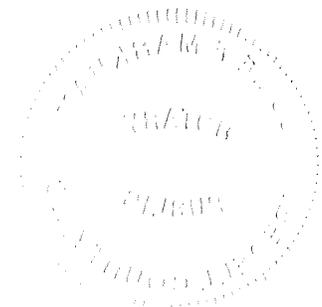
Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

Name: John Britton

Email address: john.britton@corvidtec.com

Phone Number: 704-799-6944



STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

ALL CONTRACTS: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (*W. Va. Code §61-5-3*) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: Corvid Cyberdefense, LLC.

Authorized Signature:  Date: 5/11/2021

State of NORTH CAROLINA

County of IREDELL, to-wit:

Taken, subscribed, and sworn to before me this 11th day of MAY, 2021.

My Commission expires MARCH 11, 2021.

AFFIX SEAL HERE

NOTARY PUBLIC


JULIE F. MARKHAM
Purchasing Affidavit (Revised 01/19/2018)



ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: _____

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

<input checked="" type="checkbox"/> Addendum No. 1	<input type="checkbox"/> Addendum No. 6
<input checked="" type="checkbox"/> Addendum No. 2	<input type="checkbox"/> Addendum No. 7
<input checked="" type="checkbox"/> Addendum No. 3	<input type="checkbox"/> Addendum No. 8
<input type="checkbox"/> Addendum No. 4	<input type="checkbox"/> Addendum No. 9
<input type="checkbox"/> Addendum No. 5	<input type="checkbox"/> Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Corvid Cyberdefense, LLC

Company



Authorized Signature

5/11/2021

Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.

Revised 6/8/2012



Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

State of West Virginia
 Centralized Request for Quote
 Info Technology

Proc Folder: 856640		Reason for Modification:	
Doc Description: Data Center 2.0 Firewall (OT21107)		Addendum No. 03 is being issued to address all technical questions received.	
Proc Type: Central Contract - Fixed Amt		No other changes.	
Date Issued	Solicitation Closes	Solicitation No	Version
2021-05-04	2021-05-13 13:30	CRFQ 0231 OOT2100000005	4

BID RECEIVING LOCATION

BID CLERK
 DEPARTMENT OF ADMINISTRATION
 PURCHASING DIVISION
 2019 WASHINGTON ST E
 CHARLESTON WV 25305
 US

VENDOR

Vendor Customer Code: VS0000038000
Vendor Name : Corvid Cyberdefense, LLC
Address : 153
Street : Langtree Campus Drive Ste 401
City : Mooresville
State : North Carolina **Country :** USA **Zip :** 28117
Principal Contact : Matt Hurley
Vendor Contact Phone: 703-731-5325 **Extension:**

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers
 (304) 558-0246
 jessica.s.chambers@wv.gov

Vendor
 Signature X

FEIN# 47-2954825

DATE 5/12/2021

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) for the purchase of two (2) Palo Alto PA-5250 Next Generation Firewalls, or equal, and professional services. These firewalls will be implemented in the WVOT's Data Center 2.0 Project per the terms and conditions and specifications as attached.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US		DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 908 BULLITT ST CHARLESTON WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	3.1.1 Palo Alto 5250 Next Gen Firewall, or Equal	2.00000	EA	\$67,500.00	\$135,000.00

Comm Code	Manufacturer	Specification	Model #
43222501	Fortinet	Fortigate	3400E

Extended Description:
3.1.1 Palo Alto 5250 Next Gen Firewall, or Equal

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US		DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 908 BULLITT ST CHARLESTON WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	3.1.2 Installation Services	1.00000	EA	1	\$5,000.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:
3.1.2 Installation Services

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US		DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 908 BULLITT ST CHARLESTON WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	3.1.3 Palo Alto Premium Support, or equal	1.00000	YR	1	\$50,000.00

Comm Code	Manufacturer	Specification	Model #
81112201	Fortinet	Fortigate	Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)

Extended Description:

3.1.3 Palo Alto Premium Support, or equal

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US		DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 908 BULLITT ST CHARLESTON WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	3.1.5 Palo Alto Premium Support, or equal, YR 2	1.00000	YR	1	\$50,000.00

Comm Code	Manufacturer	Specification	Model #
81112201	Fortinet	Fortigate	Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)

Extended Description:

3.1.5 Palo Alto Premium Support, or equal, YR 2

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US		DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 908 BULLITT ST CHARLESTON WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	3.1.5 Palo Alto Premium Support, or equal, YR 3	1.00000	YR	1	50,000.00

Comm Code	Manufacturer	Specification	Model #
81112201	Fortinet	Fortigate	

Extended Description:

3.1.5 Palo Alto Premium Support, or equal, YR 3

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US		DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 908 BULLITT ST CHARLESTON WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
6	3.1.5 Palo Alto Premium Support, or equal, YR 4	1.00000	YR	1	\$50,00.00

Comm Code	Manufacturer	Specification	Model #
81112201	Fortinet	Fortigate	Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)

Extended Description:

3.1.5 Palo Alto Premium Support, or equal, YR 4

SCHEDULE OF EVENTS

Line	Event	Event Date
1	TECHNICAL QUESTION DEADLINE	2021-04-09

	Document Phase	Document Description	Page
OOT210000005	Final	Data Center 2.0 Firewall (OT21107)	5

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions



Certificate of Authorized Reseller

Date: 05/10/2021

Fortinet, Inc. operates through a channel of independent distributors and resellers. Therefore, Fortinet hereby confirms that: Corvid Cyberdefense

Having its registered place of business at:
153 Langtree Campus Dr, Mooresville, North Carolina 28117, United States;

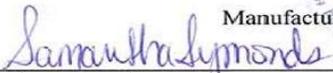
is currently an authorized FortiPartner and is currently authorized throughout US to sell Fortinet products as a partner with the following designations:

- Level of Engagement: Advocate
- Business Model: Integrator

This certificate is issued as of the date shown above, and is valid for 180 days from this date.

Provided the FortiPartner identified above has purchased applicable support services from Fortinet and the applicable support services have been effectively registered and contracted with Fortinet, Fortinet agrees and undertakes that Fortinet would provide support for the applicable Fortinet products according to the terms of the support agreement, available at <https://support.fortinet.com>. Fortinet Products are shipped subject to the terms of its then-current End User License Agreement, available at <http://www.fortinet.com/doc/legal/EULA.pdf>, which sets forth Fortinet's warranty.

This certificate is subject to the FortiPartner maintaining its FortiPartner Agreement with Fortinet and to Fortinet's FortiPartner guidelines. Fortinet's partner program and its guidelines are available for review at http://www.fortinet.com/partners/partner_program/fpp.html. Notwithstanding anything to the contrary herein, authorized FortiPartners do not represent Fortinet and can not make statements that are binding on behalf of Fortinet.


Samantha Symonds
Vice President of Legal and Compliance, Americas


Manufacturer Confirmation

FORTINET, INC.
899 Kifer Road
Sunnyvale, CA 94086

Telephone: +1-866-868-3678
Email: sales@fortinet.com
Website: www.fortinet.com

DATA SHEET

FortiGate® 3400E Series

FG-3400E/-DC and 3401E/-DC

**Next Generation Firewall
Segmentation
Secure Web Gateway
IPS
Mobile Security**



The FortiGate 3400E series delivers high performance next generation firewall (NGFW) capabilities for large enterprises and service providers. With multiple high-speed interfaces, high-port density, and high-throughput, ideal deployments are at the enterprise edge, hybrid data center core, and across internal segments. Leverage industry-leading IPS, SSL inspection, and advanced threat protection to optimize your network performance. Fortinet’s Security-Driven Networking approach provides tight network integration to the new security generation.

Security

- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services

Performance

- Delivers industry’s best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

Certification

- Independently tested and validated best security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

Networking

- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

Management

- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Security Fabric’s Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

Security Fabric

- Enables Fortinet and Fabric-ready partners’ products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation

Firewall	IPS	NGFW	Threat Protection	Interfaces
240 Gbps	44 Gbps	34 Gbps	25 Gbps	Multiple GE RJ45, 25 GE SFP28 / 10 GE SFP+ / GE SFP and 100 GE QSFP28 / 40 GE QSFP+ slots

Refer to specification table for details

DEPLOYMENT



Next Generation Firewall (NGFW)

- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, and applications across the entire attack surface, and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS security effectiveness, low latency, and optimized network performance
- Automatically block threats on decrypted traffic using the industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric



Segmentation

- Segmentation that adapts to any network topology, delivering end-to-end security from the branch level to data centers and extending to multiple clouds
- Reduce security risks by improving network visibility from the components of the Fortinet Security Fabric, which adapt access permissions to current levels of trust and enforce access control effectively and efficiently
- Delivers defense in depth security powered by high-performance L7 inspection and remediation by Fortinet's SPU, while delivering third party validated TCO of per protected Mbps
- Protects critical business applications and helps implement any compliance requirements without network redesigns



Secure Web Gateway (SWG)

- Secure web access from both internal and external risks, even for encrypted traffic at high performance
- Enhanced user experience with dynamic web and video caching
- Block and control web access based on user or user groups across URL's and domains
- Prevent data loss and discover user activity to known and unknown cloud applications
- Block DNS requests against malicious domains
- Multi-layered advanced protection against zero-day malware threats delivered over the web



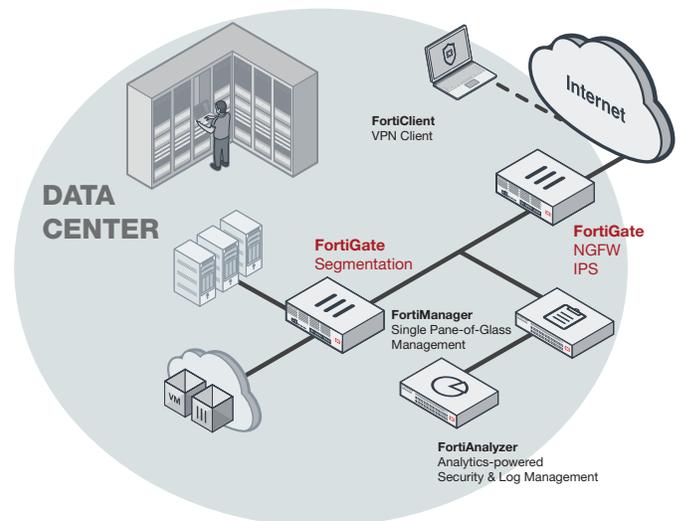
IPS

- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric



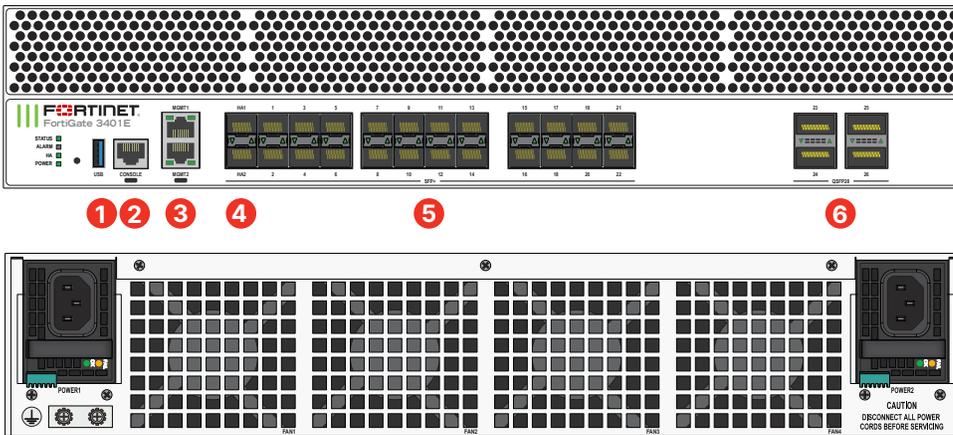
Mobile Security for 4G, 5G, and IOT

- SPU accelerated, high performance CGNAT and IPv4 and IPv6 traffic, for 4G SGI LAN and 5G N6 security
- RAN Access Security with highly scalable and best performing IPsec aggregation and control security gateway (SecGW)
- User plane security enabled by full Threat Protection and visibility into GTP-U inspection
- 4G and 5G security for user and data plane traffic SCTP, GTP-U/C and SIP that provides protection against attacks
- 4G and 5G cores IoT signaling storm protection
- High-speed interfaces to enable deployment flexibility



HARDWARE

FortiGate 3400E/-DC and 3401E/-DC



Interfaces

1. 1x USB Management Port
2. 1x Console Port
3. 2x GE RJ45 Management Ports
4. 2x 25 GE SFP28 / 10 GE SFP+ / GE SFP HA Slots
5. 22x 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots
6. 4x 100 GE QSFP28 / 40 GE QSFP+ Slots

Hardware Features



Powered by SPU

- Fortinet's custom SPU processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today's wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- SPU processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck



Network Processor

Fortinet's new, breakthrough SPU NP6 network processor works inline with FortiOS functions delivering:

- Superior firewall performance for IPv4/IPv6, SCTP and multicast traffic with ultra-low latency
- VPN, CAPWAP and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

Content Processor

Fortinet's ninth generation custom SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection.

High-Speed Connectivity

High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 3400E provides multiple 100 GE QSFP28 slots, simplifying network designs without relying on additional devices to bridge desired connectivity.



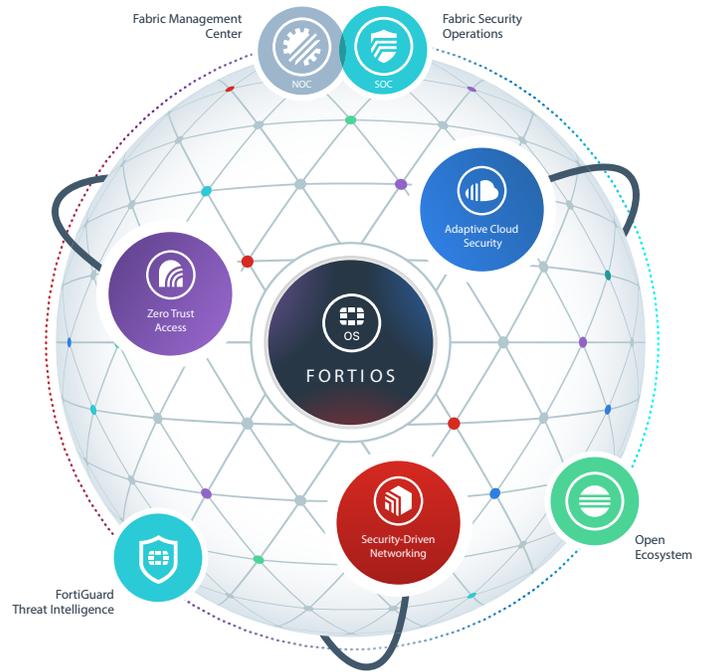
FORTINET SECURITY FABRIC

Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad:** Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints, and users
- **Integrated:** Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest ecosystem
- **Automated:** Context aware, self-healing network and security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.



FortiOS™ Operating System

FortiOS, Fortinet's leading operating system enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoint, and clouds. The organically built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across hybrid deployment models of Hardware, Software, and Software As-a-Service with SASE and ZTNA, among others.

SERVICES

FortiGuard™ Security Services

FortiGuard Labs offer real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.

FortiCare™ Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1,000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.



SPECIFICATIONS

FORTIGATE	3400E/-DC	3401E/-DC
Interfaces and Modules		
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots		4
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots		24
GE RJ45 Management Ports		2
USB Ports (Client / Server)		1 / 1
Console Port		1
Onboard Storage	0	2x 2 TB SSD
Included Transceivers	2x SFP+ (SR 10 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput ²	44 Gbps	
NGFW Throughput ^{2,4}	34 Gbps	
Threat Protection Throughput ^{2,5}	25 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	240 / 238 / 150 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	240 / 238 / 150 Gbps	
Firewall Latency (64 byte, UDP)	3.33 µs	
Firewall Throughput (Packet per Second)	225 Mpps	
Concurrent Sessions (TCP)	50 Million	
New Sessions/Second (TCP)	850,000	
Firewall Policies	200,000	
IPsec VPN Throughput (512 byte) ¹	140 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	40,000	
Client-to-Gateway IPsec VPN Tunnels	200,000	
SSL-VPN Throughput	11 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30,000	
SSL Inspection Throughput (IPS, avg. HTTPS) ³	30 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) ³	14,000	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	4.9 Million	
Application Control Throughput (HTTP 64K) ²	86 Gbps	
CAPWAP Throughput (HTTP 64K)	57 Gbps	
Virtual Domains (Default / Maximum)	10 / 500	
Maximum Number of FortiSwitches Supported	300	
Maximum Number of FortiAPs (Total / Tunnel)	4,096 / 2,048	
Maximum Number of FortiTokens	20,000	
High Availability Configurations	Active, Active-Active, Passive, Clustering	

FORTIGATE	3400E/-DC	3401E/-DC
Dimensions and Power		
Height x Width x Length (inches)	3.5 x 17.44 x 21.89	
Height x Width x Length (mm)	88.9 x 443 x 556	
Weight	42.9 lbs (19.5 kg)	44.3 lbs (20.1 kg)
Form Factor	Rack Mount, 2 RU	
AC Power Supply	100–240V AC, 50–60 Hz	
Power Consumption (Average / Maximum)	513 W / 728 W	519 W / 750 W
AC Current (Maximum)	12A@120V, 9A@240V	
Heat Dissipation	2,484 BTU/h	2,560 BTU/h
DC Power Supply	-48V DC	
DC Current (Maximum)	17.8A	
Redundant Power Supplies	Yes, Hot swappable	
Operating Environment and Certifications		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	63 dBA	
Forced Airflow	Front to Back	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, USGv6/IPv6	

Note: All performance values are “up to” and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

4. NGFW performance is measured with Firewall, IPS, and Application Control enabled.
5. Threat Protection performance is measured with Firewall, IPS, Application Control, URL filtering, and Malware Protection with sandboxing enabled.



ORDERING INFORMATION

Product	SKU	Description
FortiGate 3400E	FG-3400E	4× 100 GE QSFP28 slots and 24× 25 GE SFP28 slots (including 22x ports, 2x HA ports), 2x GE RJ45 Management ports, SPU NP6 and CP9 hardware accelerated, and 2 AC power supplies.
FortiGate 3400E-DC	FG-3400E-DC	4× 100 GE QSFP28 slots and 24× 25 GE SFP28 slots (including 22x ports, 2x HA ports), 2x GE RJ45 Management ports, SPU NP6 and CP9 hardware accelerated, and 2 DC power supplies.
FortiGate 3401E	FG-3401E	4× 100 GE QSFP28 slots and 24× 25 GE SFP28 slots (including 22x ports, 2x HA ports), 2x GE RJ45 Management ports, SPU NP6 and CP9 hardware accelerated, 4 TB SSD onboard storage, and 2 AC power supplies.
FortiGate 3401E-DC	FG-3401E-DC	4× 100 GE QSFP28 slots and 24× 25 GE SFP28 slots (including 22x ports, 2x HA ports), 2x GE RJ45 Management ports, SPU NP6 and CP9 hardware accelerated, 4 TB SSD onboard storage, and 2 DC power supplies.
Optional Accessories/Spares	SKU	Description
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1200D, FG-1500D/DC, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D/-DC, FG-3100D/-DC, FG-3200D/-DC, FG-3400/3401E, FG-3600/3601E, FG-3700D/-DC, FG-3700DX, FG-3810D/-DC and FG-3950B/-DC.
AC Power Supply	SP-FG3800D-PS	AC power supply for FG-3400/3401E, FG-3600/3601E, FG-3700D, FG-3700D-NEBS, FG-3700DX, FG-3810D and FG-3815D.
DC Power Supply	SP-FG3800D-DC-PS	DC power supply for FG-3400/3401E-DC, FG-3700D-DC, FG-3700D-DC-NEBS, FG-3810D-DC, FG-3815D-DC.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Active Direct Attach Cable, 10m / 32.8 ft	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots.
25 GE SFP28 Transceiver Module, Short Range	FN-TRAN-SFP28-SR	25 GE SFP28 transceiver module, short range for all systems with SFP28 slots.
25 GE SFP28 Transceiver Module, Long Range	FG-TRAN-SFP28-LR	25 GE SFP28 transceiver module, long range for all systems with SFP28 slots.
40 GE QSFP+ Transceiver Module, Short Range	FN-TRAN-QSFP+SR	40 GE QSFP+ transceiver module, short range for all systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Short Range BiDi	FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ transceiver module, short range BiDi for all systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Long Range	FN-TRAN-QSFP+LR	40 GE QSFP+ transceiver module, long range for all systems with QSFP+ slots.
100 GE QSFP28 Transceivers, Short Range	FN-TRAN-QSFP28-SR	100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 slots.
100 GE QSFP28 Transceivers, Long Range	FN-TRAN-QSFP28-LR	100 GE QSFP28 transceivers, 4 channel parallel fiber, long range for all systems with QSFP28 slots.
100 GE QSFP28 Transceivers, CWDM4	FN-TRAN-QSFP28-CWDM4	100 GE QSFP28 transceivers, LC connectors, 2KM for all systems with QSFP28 slots.



BUNDLES



FortiGuard Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Bundles	360 Protection	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	ASE ¹	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web and Video ² Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard IoT Detection Service	•	•		
FortiGuard Industrial Service	•	•		
FortiConverter Service	•	•		
SD-WAN Orchestrator Entitlement	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
Fortinet SOCaaS	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 7.0



Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.