



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](http://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](http://WVPurchasing.gov) with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

## Header 2

## General Information

Contact

Default Values

Discount

Document Information

Procurement Folder: 591150

Procurement Type: Central Master Agreement

Vendor ID: 000000180127



Legal Name: INSIGHT PUBLIC SECTOR INC

Alias/DBA:

Total Bid: \$20.56

Response Date: 07/30/2019



Response Time: 11:25

SO Doc Code: CRFQ

SO Dept: 0210

SO Doc ID: ISC2000000002

Published Date: 7/22/19

Close Date: 7/30/19

Close Time: 13:30

Status: Closed

Solicitation Description: Addendum 1-EndPoint Detection and Response Software - OT1912

Total of Header Attachments: 2

Total of All Attachments: 2



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

**State of West Virginia  
 Solicitation Response**

**Proc Folder :** 591150

**Solicitation Description :** Addendum 1-EndPoint Detection and Response Software - OT1912

**Proc Type :** Central Master Agreement

Date issued	Solicitation Closes	Solicitation Response	Version
	2019-07-30 13:30:00	SR 0210 ESR07301900000000465	1

<b>VENDOR</b>
000000180127 INSIGHT PUBLIC SECTOR INC

**Solicitation Number:** CRFQ 0210 ISC2000000002

**Total Bid :** \$20.56                      **Response Date:** 2019-07-30                      **Response Time:** 11:25:41

**Comments:** Discount has already been figured into quoted price. no additional discounts for early payment.

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

<b>Signature on File</b>	<b>FEIN #</b>	<b>DATE</b>
--------------------------	---------------	-------------

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Overall Total for Contract Items 1 & 2 with Opt Renewals	1.00000	LS	\$20.560000	\$20.56

Comm Code	Manufacturer	Specification	Model #
43233204			

<b>Extended Description :</b>	<p>4.1.1 Contract Item 1: Containment &amp; Remediation</p> <p>4.1.1.1 The Vendor must provide a software and/or service that is capable of supporting a minimum of 2,000 endpoints throughout the State of West Virginia</p>
-------------------------------	---



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

State of West Virginia  
 Request for Quotation  
 21 - Info Technology

Proc Folder: 591150

Doc Description: EndPoint Detection and Response Software - OT19125

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-07-10	2019-07-30 13:30:00	CRFQ 0210 ISC2000000002	1

**BID RECEIVING LOCATION**

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

**VENDOR**

Vendor Name, Address and Telephone Number:

Insight Public Sector, Inc.  
 6820 S. Harl Ave.  
 Tempe, AZ 85283  
 501-505-4155

**FOR INFORMATION CONTACT THE BUYER**

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

Signature X

FEIN # 36-3949000

DATE July 29, 2019

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 WV Office of Technology to establish a contract for an End Point Detection and Response Software to support approximately two thousand (2,000) endpoints across the state of West Virginia but can be managed centrally. This service will assist in the continuous monitoring and response to advanced cyber security threats 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 WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Overall Total for Contract Items 1 & 2 with Opt Renewals	1.00000	LS		

Comm Code	Manufacturer	Specification	Model #
43233204			

**Extended Description :**

4.1.1 Contract Item 1: Containment & Remediation

4.1.1.1 The Vendor must provide a software and/or service that is capable of supporting a minimum of 2,000 endpoints throughout the State of West Virginia

For more details see attached specifications.

## 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 person attending the pre-bid meeting may represent more than one Vendor.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. The State will not accept any other form of proof or documentation to verify 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: July 18, 2019 at 9:00 AM (EDT)

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](mailto: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 ISC2000000002  
BID OPENING DATE: 7/30/2019  
BID OPENING TIME: 1:30 PM (EDT)  
FAX NUMBER: (304)558-3970



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 an Expression or Interest or 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: July 30 2019 at 1:30 PM (EDT)

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

Revised 06/05/2019

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 should 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. 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.

## 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 extends for a period of one (1) year(s).

**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. NOTICE TO PROCEED:** Vendor shall begin performance of this Contract immediately upon receiving notice to proceed unless otherwise instructed by the Agency. Unless otherwise specified, the fully executed Award Document will be considered notice to proceed.

**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 prior to Contract award, in a form acceptable to the Purchasing Division.

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications prior to Contract award 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: \$1,000,000.00 per occurrence.

**Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: \_\_\_\_\_ per occurrence.

**Commercial Crime and Third Party Fidelity Insurance** in an amount of: \_\_\_\_\_ per occurrence.

**Cyber Liability Insurance** in an amount of: \_\_\_\_\_ 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](mailto: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 06/05/2019

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 of 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.

**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.

Crystal McBride  
\_\_\_\_\_  
(Name, Title)  
Crystal McBride - Account Executive  
\_\_\_\_\_  
(Printed Name and Title)  
6820 S. Harl Ave. Tempe, AZ 85283  
\_\_\_\_\_  
(Address)  
501-505-4155 / 480-760-9488  
\_\_\_\_\_  
(Phone Number) / (Fax Number)  
crystal.mcbride@insight.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.

Insight Public Sector, Inc.  
\_\_\_\_\_  
(Company)  
  
\_\_\_\_\_  
(Authorized Signature) (Representative Name, Title)

Erica Falchetti - Capture Manager  
\_\_\_\_\_  
(Printed Name and Title of Authorized Representative)

July 29, 2019  
\_\_\_\_\_  
(Date)

480-333-3071 / 480-760-9488  
\_\_\_\_\_  
(Phone Number) (Fax Number)

**REQUEST FOR QUOTATION**  
EndPoint Detection and Response Software

---

**SPECIFICATIONS**

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of The WV Office of Technology to establish a contract for an EndPoint Detection and Response Software to support approximately two thousand (2,000) endpoints across the state of West Virginia but can be managed centrally. This service will assist in the continuous monitoring and response to advanced cyber security threats.
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 **“Business Hours”** means Monday - Friday 8:00 AM to 5:00 PM EST excluding weekends and Federal and State holidays, which are as follows:
    - New Year’s Day (January 1)
    - Martin Luther King Day (Third Monday in January)
    - President’s Day (Third Monday in February)
    - Memorial Day (Last Monday in May)
    - West Virginia Day (June 20)
    - Independence Day (July 4)
    - Labor Day (First Monday in September)
    - Columbus Day (Second Monday in October)
    - Veterans Day (November 11)
    - Thanksgiving (Fourth Thursday in November)
    - Day After Thanksgiving (Fourth Friday in November)
    - Christmas Day (December 25)
  - 2.2 **“Contract Services”** means an EndPoint Detection and Response Service to support approximately 2,000 endpoints across the state of WV, as more fully described in these specifications.
  - 2.3 **“EDR”** means EndPoint Detection and Response.
  - 2.4 **“Endpoints”** means an Internet-capable computer hardware device on a TCP/IP network, including desktop computers, laptops, tablets, thin clients, and servers.
  - 2.5 **“FTI”** means an Federal Tax Information.
  - 2.6 **“Pricing Page”** means the pages, contained in wvOASIS or attached hereto as Exhibit A, upon which Vendor should list its proposed price for the Contract Services.

**REQUEST FOR QUOTATION**  
EndPoint Detection and Response Software

---

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.

3. **QUALIFICATIONS:** Vendor, or Vendor’s staff if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:

3.1 The Vendor must be compliant with Internal Revenue Service (IRS) 1075, Section 9.3.1.12 – Remote Access requirements.

3.1.1 IRS 1075, Section 9.3.1.12 states that *“FTI cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore - outside of the United States territories, embassies, or military installations. Further, FTI may not be received, processed, stored, transmitted, or disposed of by IT systems located offshore.”*

3.2 The Vendor must have the ability to provide at a minimum 3-tiered levels of support. Documentation detailing the Vendor’s tiered level support must be available upon request. The levels of support must consist of following:

3.2.1 A Customer Service Tier; Initial contact that will provide tier one support to include basic troubleshooting.

3.2.2 An Engineering Tier; If tier one troubleshooting is unable to resolve the issue at hand, then it needs to be able to be escalated to an engineer level support.

3.2.3 An Onsite Support Tier; To include any and all subject matter experts applicable to the problem that cannot be fixed remotely.

3.3 The Vendor must provide upon request, examples of at least five (5) successful implementations of their EDR service over last three (3) years.

3.4 The Vendor must provide upon request a dedicated Project Manager and Project Management services during the implementation of the proposed service, including a project plan.

3.4.1 The project plan must include but is not limited to the Work Breakdown Structure, a change management plan, a communication plan, and weekly status report.

4. **MANDATORY REQUIREMENTS:**

4.1 **Mandatory Contract Services Requirements and Deliverables:** Contract Services must meet or exceed the mandatory requirements listed below.

4.1.1 **Contract Item: Endpoint Detection and Response Software**

**REQUEST FOR QUOTATION**  
**EndPoint Detection and Response Software**

---

**4.1.1.1 Containment & Remediation**

**4.1.1.2** The Vendor must provide a software and/or service that is capable of supporting a minimum of two thousand (2,000) endpoints throughout the State of West Virginia

**4.1.1.3** The Vendor must provide a software and/or service that can be centrally managed by a West Virginia Office of Technology Administrator.

**4.1.1.4** The Vendor must provide a software and/or service that shall feature the following:

**4.1.1.4.1** Automatically restrict potentially malicious activity to within an isolation container.

**4.1.1.4.2** Automatically isolate applications interacting with untrusted content from more trusted portions of the device outside the container.

**4.1.1.4.3** Automatically detect and isolate potentially malicious code behavior.

**4.1.1.4.4** Continuously detect, and isolate threats based on machine learning, behavioral analytics, and custom detection rules.

**4.1.1.4.5** Automatically capture necessary event details on all malicious activity, including but not limited to ports and protocols in use, running executables and services, and browser plugins occurring within the isolation container to support retrospective post-event analysis, threat analysis, and situational awareness.

**4.1.1.4.6** Be configurable to control the ability of applications running within the isolation container to access only specified system resources.

**4.1.1.4.7** Provide the ability to restrict execution of high-risk applications and computer processing activities to an isolated environment.

**REQUEST FOR QUOTATION**  
**EndPoint Detection and Response Software**

---

- 4.1.1.4.8 Automatically eliminate and report all isolation container artifacts of compromise and intrusion remnants.
  - 4.1.1.4.9 Provide continual verification of the integrity of the isolation container to ensure there is no unauthorized/malicious access or persistent modification.
  - 4.1.1.4.10 Automatically report potentially malicious events detected within the isolation container and provide actionable information.
  - 4.1.1.4.11 Be capable of containing operating system kernel-level vulnerability exploitation.
  - 4.1.1.4.12 Provide options for configurable automated or manual remediation actions in response to detected potentially malicious events.
- 4.1.1.5 Reporting & Monitoring**
- 4.1.1.6 The Vendor must provide a software or service that shall interoperate with event monitoring and correlation systems to facilitate aggregated situational awareness.
  - 4.1.1.7 The software shall support open standards for automated threat information sharing.
  - 4.1.1.8 The software shall provide integrated and customizable search with, at minimum, the ability to search data from all systems for information relevant to an incident investigation or risk analysis.
  - 4.1.1.9 The software shall have the ability to execute manual and scheduled scans of specified systems for indicators derived from threat intelligence or other sources.

**REQUEST FOR QUOTATION**  
**EndPoint Detection and Response Software**

---

- 4.1.1.10 The software shall provide integrated analytics (including visualization) and support the creation of custom analytics, in order to identify anomalous endpoint behaviors, support incident investigation, and perform event analysis.
- 4.1.1.11 The software shall allow administrative functions to be delegated to users based on roles/permissions and or groupings of endpoints they are responsible for managing.
- 4.1.1.12 The software shall support delegation (i.e., user-specified) of who can access/view collected endpoint data.
- 4.1.1.13 The software shall have the capability to be tuned/configured to reduce alerts resulting from false positives.
- 4.1.1.14 The software shall provide configurable alerting based upon administrator defined criteria.
- 4.1.1.15 The software shall send alerts at administrator-definable intervals.
- 4.1.1.16 The software shall provide the ability to automatically discover and alert on previously unknown external and/or internal hardware/peripheral devices (such as storage) connected to endpoints for the purpose of retrospective/post-event analysis.
- 4.1.1.17 The software shall generate reports based on pre-saved user-defined formats and datasets to facilitate rapid analysis, decision making, and follow-up actions following events.
- 4.1.1.18 The software shall provide time stamping of all collected data and events based on a single time standard (e.g., coordinated universal time).
- 4.1.1.19 The software shall have the ability to pull locally stored data from specified endpoints in near real time to support high priority hunt and forensic operations.
- 4.1.1.20 The software shall provide automated analysis and visualization of an attack; including production of an event timeline and initial assessment of severity/impact.

**REQUEST FOR QUOTATION**  
EndPoint Detection and Response Software

---

**4.1.2 Technical Details**

**4.1.2.1** The Vendor must provide the minimum supported platforms including: Windows operating system, Linux operating system, and all virtual environments including but not limited to VMWare, Azure, and Hyper-V.

**4.1.2.2** The software shall not impair authorized system operations nor shall it degrade managed system performance in any way, which may adversely impact a system's primary business/mission functions. The following authorize system operations include but not limited to:

**4.1.2.2.1** Patching, Scanning, Business software usage,

**4.1.2.2.2** The following Information Assurance Tools/Initiatives include but not limited to:

**4.1.2.2.2.1** Secure host baseline, and assured compliance assessment software.

**4.1.2.3** The software shall allow for patching and update of containerized applications through a means of automated verification (e.g., integration with automated patch management infrastructure/processes).

**4.1.2.4** All software components shall have the ability to be automatically deployed and configured based on predefined configurations.

**4.1.2.5** The software shall securely store and transmit data in a manner that ensures the confidentiality, integrity, availability, and source authenticity of the data.

**4.1.2.6** The software shall encrypt all data in transit or data at rest with Federal Information Processing Standards (FIPS) 140-2 compliant cryptographic modules.

**4.1.3 Optional Renewals**

**4.1.3.1** Vendor should include, as part of its bid, pricing for optional renewal years 2, 3, and 4. These optional renewal years will be agreed upon by both parties and initiated by the Agency via Change Order. The contract will be awarded on the initial year's cost only.



**REQUEST FOR QUOTATION**  
EndPoint Detection and Response Software

---

**5. CONTRACT AWARD:**

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

**Contract will be evaluated on all lines but only awarded on first year.**

Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

Vendor should provide with their bid a copy of any and all Software Terms and Conditions or licenses that the State of West Virginia or the Agency will have to agree to or accept as a part of this solicitation. This information will be required before contract is issued.

Vendor should include a copy of any Maintenance Terms and Conditions or Licenses that the State of West Virginia or the Agency will be required to agree to and accept as a part of this solicitation. This information will be required before contract is issued.

**5.2 Pricing Page:** Vendor should complete the Pricing Page, Exhibit "A", by inserting the unit cost of the items listed; extended cost; and an overall total to reflect Total Cost of the listed items. See pricing page example. 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.

**Pricing Page Example**

$$\text{Estimated Quantity} \times \text{Unit Cost} = \text{Extended Cost}$$

The Pricing Pages contain a list of the Contract Items and estimated purchase volume. The estimated purchase volume for each item represents the approximate volume of anticipated purchases only. No future use of the Contract or any individual item is guaranteed or implied.

The Vendor can request an electronic copy of the Pricing Pages for bid purposes by sending an email request to the following address: [Jessica.S.Chambers@wv.gov](mailto:Jessica.S.Chambers@wv.gov).

**6. PERFORMANCE:** Vendor and Agency shall agree upon a schedule for performance of Contract Services and Contract Services Deliverables, unless such a schedule is already included herein by Agency. In the event that this Contract is designated as an open-end contract, Vendor shall perform in accordance with the release orders that may be issued against this Contract.

**REQUEST FOR QUOTATION**  
EndPoint Detection and Response Software

---

7. **PAYMENT:** Agency shall pay flat fee for the unit cost, as shown on the Pricing Pages, for all Contract Services performed and accepted under this Contract. Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.
8. **TRAVEL:** Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on Vendor's bid, but such costs will not be paid by the Agency separately.
9. **FACILITIES ACCESS:** Performance of Contract Services may require access cards and/or keys to gain entrance to Agency's facilities. In the event that access cards and/or keys are required:
  - 9.1 Vendor must identify principal service personnel which will be issued access cards and/or keys to perform service.
  - 9.2 Vendor will be responsible for controlling cards and keys and will pay replacement fee, if the cards or keys become lost or stolen.
  - 9.3 Vendor shall notify Agency immediately of any lost, stolen, or missing card or key.
  - 9.4 Anyone performing under this Contract will be subject to Agency's security protocol and procedures.
  - 9.5 Vendor shall inform all staff of Agency's security protocol and procedures.
10. **VENDOR DEFAULT:**
  - 10.1 The following shall be considered a vendor default under this Contract.
    - 10.1.1 Failure to perform Contract Services in accordance with the requirements contained herein.
    - 10.1.2 Failure to comply with other specifications and requirements contained herein.
    - 10.1.3 Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.
    - 10.1.4 Failure to remedy deficient performance upon request.
  - 10.2 The following remedies shall be available to Agency upon default.
    - 10.2.1 Immediate cancellation of the Contract.
    - 10.2.2 Immediate cancellation of one or more release orders issued under this Contract.

**REQUEST FOR QUOTATION**  
EndPoint Detection and Response Software

---

10.2.3 Any other remedies available in law or equity.

**11. MISCELLANEOUS:**

**11.1 Contract Manager:** During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

<b>Contract Manager:</b>	Erica Falchetti
<b>Telephone Number:</b>	480-333-3071
<b>Fax Number:</b>	480-760-9488
<b>Email Address:</b>	erica.falchetti@insight.com

**EXHIBIT A – Pricing Page**  
**EndPoint Detection and Response Services - OT19125**  
**Note to Vendors: The Pricing Page is locked with the exception of Unit Cost column.**

Line Items	Description	Unit of Measure	Estimated Quantity	Unit Cost	Extended Cost
4.1	Contract Item: Endpoint Detection and Response Software for approximately 2,000 EndPoints	LS	1		\$ 41,120.00 -
4.1	Optional Renewal Year 2 Maintenance: Contract Item: Endpoint Detection and Response Software	LS	1		\$ 43,176.00 -
4.1	Optional Renewal Year 3 Maintenance: Contract Item: Endpoint Detection and Response Software	LS	1		\$ 45,334.00 -
4.1	Optional Renewal Year 4 Maintenance: Contract Item: Endpoint Detection and Response Software	LS	1		\$ 47,600.00 -
<b>Total Overall Cost</b>					<b>\$ 177,230.00 -</b>

Please note: This information is being captured for auditing purposes

Contract will be evaluated on all lines but only awarded on first year. Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the WV Purchasing Division as Change Orders for subsequent years.



Vendor Signature:

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 exceeds 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: Insight Public Sector, Inc.

Authorized Signature: *Cira J. Delle* Date: July 29, 2019

State of Arizona

County of Maricopa, to-wit:

Taken, subscribed, and sworn to before me this 29<sup>th</sup> day of July, 2019.

My Commission expires April 7, 2021.

AFFIX SEAL HERE

NOTARY PUBLIC *Kayla Martin*



*Purchasing Affidavit (Revised 01/19/2018)*



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

State of West Virginia  
 Request for Quotation  
 21 - Info Technology

Proc Folder: 591150

Doc Description: Addendum 1-EndPoint Detection and Response Software - OT1912

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-07-22	2019-07-30 13:30:00	CRFQ 0210 ISC2000000002	2

**BID RECEIVING LOCATION**

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

**VENDOR**

Vendor Name, Address and Telephone Number:

Insight Public Sector, Inc.  
 6820 S. Hari Ave  
 Tempe, AZ 85283  
 501-505-4155

**FOR INFORMATION CONTACT THE BUYER**

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

Signature X *Gina I. Chetti*

FEIN # 36-3949000

DATE July 29, 2019

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

**ADDITIONAL INFORMATION:**

Addendum

Addendum No.01 issued to publish and distribute the attached information to the vendor community.

\*\*\*\*\*

The West Virginia Purchasing Division is soliciting bids on behalf of The WV Office of Technology to establish a contract for an End Point Detection and Response Software to support approximately two thousand (2,000) endpoints across the state of West Virginia but can be managed centrally. This service will assist in the continuous monitoring and response to advanced cyber security threats 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 WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Overall Total for Contract Items 1 & 2 with Opt Renewals	1.00000	LS		

Comm Code	Manufacturer	Specification	Model #
43233204			

**Extended Description :**

4.1.1 Contract Item 1: Containment & Remediation

4.1.1.1 The Vendor must provide a software and/or service that is capable of supporting a minimum of 2,000 endpoints throughout the State of West Virginia

For more details see attached specifications.

SOLICITATION NUMBER: CRFQ ISC2000000002

Addendum Number: No.01

---

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

**Applicable Addendum Category:**

- Modify bid opening date and time
- Modify specifications of product or service being sought
- Attachment of vendor questions and responses
- Attachment of pre-bid sign-in sheet
- Correction of error
- Other

**Description of Modification to Solicitation:**

Addendum issued to publish and distribute the attached documentation to the vendor community.

1. The purpose of this addendum is to address all technical questions received.

No additional changes.

**Additional Documentation:** Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

**Terms and Conditions:**

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.
2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, 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.



# ATTACHMENT A

Technical Questions  
CRFQ ISC2000000002

1. Are there any details available regarding 'Endpoint Detection and Response Software'? Any specific metrics regarding detection and/or response? Details listed in 4.1.1.4.1 thru 4.1.1.4.10 are limited, at best.

**Agency Answer:**

The State would like a solution that performs the functions listed in Section 4.1.1.4.1 thru 4.1.1.4.10 automatically, without direct, manual interaction from staff.

2. Are there any details available on the 'Scoring Matrix' to be used in evaluating proposals? Price, references, ability to meet all technical requirements, gartner, etc?

**Agency Answer:**

Lowest price that meets all the mandatory requirements of the solicitation.

3. Will implementation and professional services be required at the time of this bid or after contract award? Any details specific to this?

**Agency Answer:**

Implementation should be included in the total bid cost

4. Would the West Virginia Department of Administration extend the due date out to August 13, 2019?

**Agency Answer:**

No.

5. Are the 2,000 endpoints strictly laptops and desktops? Are there any mobile devices mixed in?

**Agency Answer:**

The EndPoints are servers

6. Will the number of endpoints grow beyond 2,000?

**Agency Answer:**

Not at this time

7. What is the mixture of Windows and Linux based endpoints?

**Agency Answer:**

85% Windows; 10% Linux; 5% Other

8. Will EDR for the 2000 endpoints include any servers or is this just for workstations?

**Agency Answer:**

All the endpoints are servers

a. How many Windows servers are included in the 2000 endpoints?

Approximately 85% of the licenses

b. How many Linux servers are included in the 2000 endpoints?

Approximately 10% of the licenses

**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 type="checkbox"/> Addendum No. 2            | <input type="checkbox"/> Addendum No. 7  |
| <input 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.

Insight Public Sector, Inc.

Company



Authorized Signature

July 29, 2019

Date

**NOTE:** This addendum acknowledgment should be submitted with the bid to expedite document processing.  
Revised 6/8/2012

**SOLD-TO PARTY**      10781998  
 STATE OF WEST VIRGINIA  
 DEPARTMENT OF ADMINISTRATION  
 2019 WASHINGTON ST E  
 CHARLESTON WV 25305-2214

**SHIP-TO PARTY**  
 STATE OF WEST VIRGINIA  
 DEPARTMENT OF ADMINISTRATION  
 2019 WASHINGTON ST E  
 CHARLESTON WV 25305-2214

Quotation	
Quotation Number :	221404196
Document Date :	29-JUL-2019
PO Number :	
PO Release :	
Sales Rep :	Crystal McBride
Email :	CMCBRIDE@INSIGHT.COM
Telephone :	5015054155

**We deliver according to the following terms:**

**Payment Terms** : Net 30 days  
**Ship Via** : Electronic Delivery  
**Terms of Delivery** : FOB DESTINATION  
**Currency** : USD

Material	Material Description	Quantity	Unit Price	Extended Price
<a href="#">CEDSEPNEWAG1K2499</a>	Symantec Complete Endpoint Defense Suite with SEP - Initial Hybrid Subscription (1 year) + Support - 1 device - academic, volume, GO V - 1000-2499 licenses Coverage Dates: 29-JUL-2019 - 29-JUL-2020 OPEN MARKET	2,000	20.56	41,120.00
			Product Subtotal	41,120.00
			TAX	0.00
			<b>Total</b>	<b>41,120.00</b>

Lease & Financing options available from Insight Global Finance for your equipment & software acquisitions. Contact your Insight account executive for a quote.

**PURCHASE ORDER REQUIREMENTS:**  
 Quote Number:221404196

Purchase Order Number: \_\_\_\_\_

Authorized by/Title: \_\_\_\_\_ (please print)

Authorized Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Thank you for considering Insight. Please contact us with any questions or for additional information about Insight's complete IT solution offering.

Sincerely,

Crystal McBride  
 5015054155  
 CMCBRIDE@INSIGHT.COM

---

For years 2, 3 and 4 Symantec has agreed that the price will not exceed a 5% annual increase, this is a ceiling price not an automatic increase.

Year 1 – \$41,120; Year 2 – \$43,176; Year 3 – \$45,334; Year 4 – 47,600

Insight Global Finance has a wide variety of flexible financing options and technology refresh solutions. Contact your Insight representative for an innovative approach to maximizing your technology and developing a strategy to manage your financial options.

The U.S. government has imposed tariffs on technology-related goods. Many of Insight's OEM and distribution partners have notified Insight that these tariffs will result in frequent and significant price increases. Some of our major partners have already provided Insight with cost increases, in some instances multiple times per day, while other providers are still assessing their situations. Due to the situation it is possible this quote may be subject to cost changes for Insight which will necessitate changes to the quoted pricing, or withdrawal of the quote.

This purchase is subject to Insight's online Terms of Sale unless you have a separate purchase agreement signed by both your company and Insight, in which case, that separate agreement will govern. Insight's online Terms of Sale can be found at: [http://www.insight.com/en\\_US/help/terms-of-sale-products-ips.html](http://www.insight.com/en_US/help/terms-of-sale-products-ips.html)



**Symantec Response to the Request for Quote**  
**to**  
**State of West Virginia**  
**for**  
**EndPoint Detection and Response Software**  
**Symantec - Complete Endpoint Defense**

**07-30-2019**

Please note that this proposal and any other Symantec related information provided to you or your organization (You) are the sole property and confidential information of Symantec and are submitted for the sole purpose of assisting You in deciding whether to enter into a contractual agreement with Symantec for the products or services described in the proposal. Please contact your Symantec representative if You have any questions about the content of this proposal or to obtain our express written permission if Your organization would like to use the Symantec information for any other purpose. Symantec endeavors to include only correct information in this proposal; however, any warranties provided by Symantec will be included in Symantec's confirmed order form. Symantec shall not be liable for any errors or omissions, and this information is provided "as-is".

Your review of this proposal does not create a binding agreement between you and Symantec, except with respect to your obligation to protect the confidential information in the proposal. If included, Symantec's standard terms and conditions governing the use of product or delivery of services described in this proposal are provided for your convenient reference, however Symantec reserves the right to negotiate mutually agreeable terms and conditions upon award of a contract resulting from this proposal.

The data subject to this restriction are contained in all pages marked with the following legend: Use or disclosure of data contained on this page is subject to the restriction on the coversheet of this proposal.

Copyright © Symantec Corporation. All Rights Reserved.



Table of Contents

<b>Proposed Solution .....</b>	<b>6</b>
<b>RESPONSE TO MANDATORY REQUIREMENTS.....</b>	<b>9</b>
4.1 Mandatory Contract Services Requirements and Deliverables:.....	9
4.1.1 Contract Item: Endpoint Detection and Response Software .....	9
4.1.2 Technical Details .....	14
4.1.3 Optional Renewals .....	17



## Executive Summary

---

### *Symantec – A Trusted Security Leader*

Partnering with a trusted security leader that is also the largest cybersecurity company in the world is critical today in light of cyber threats that advance faster and faster in innovation and complexity, from industrial espionage to cybercrime, hacktivism, state-sponsored cyber threats, insider threats, terrorist-backed cyber threats, and newly emerging threats.

#### According to the Symantec Internet Security Threat Report 2019

Partnering with a trusted security leader that is also the largest cybersecurity company in the world is critical today in light of cyber threats that advance faster and faster in innovation and complexity, from industrial espionage to cybercrime, hacktivism, state-sponsored cyber threats, insider threats, terrorist-backed cyber threats, and newly emerging threats.

**The 2019 Internet Security Threat Report (ISTR)** reveals that faced with diminishing returns from cryptojacking, cyber criminals are doubling down on alternative methods, such as formjacking, to make money. On average, 4,800 unique websites are compromised by formjacking attacks every month. Symantec blocked more than 3.7 million formjacking attempts on endpoints in 2018, with nearly a third of all detections occurring during the busiest online shopping period of the year – November and December. Highlights of the report include:

- Nearly one in ten targeted attack groups now use malware, up 25 percent
- Cloud resources are increasingly targeted with over 70 million records stolen or leaked
- Enterprise ransomware infections jumped by 12 percent
- Attackers enhance tactics such as spear phishing, hijacking, and malicious email attachments
- More attackers showed interest in compromising industrial control systems

Symantec owns the largest civilian cyber threat collection network in the world and operates the most comprehensive collection of cyber security threat intelligence through the Symantec Global Intelligence Network (GIN). The Symantec GIN records events from 123 million attack sensors worldwide, blocks 142 million threats daily, and monitors threat activities in more than 157 countries via a set of tightly integrated technologies and services.

#### ***Solution Overview***

##### Endpoint Detection and Response

Enterprises are increasingly under threat from sophisticated attacks. These Advanced Persistent Threats (APTs) use stealthy techniques to evade detection and bypass traditional security defenses. In fact, research has found that threats dwell in a customer's environment an average of 190 days. These APTs use stealthy techniques to evade detection and bypass traditional security defenses. Once an advanced attack gains access to a customer environment the attacker has many tools to evade detection and begin to exploit valuable resources and data. Security teams face multiple challenges when attempting to detect and fully expose the extent of an advanced attack including manual searches through large and disparate data sources, lack of visibility into critical control points, alert fatigue from false positives, and difficulty identifying and fixing impacted endpoints.

Security teams face the following challenges when attempting to detect and fully expose the extent of an advanced attack:

- Large amounts lack visibility into critical control points where Indicators of Compromise (IoCs) can be found
- Large numbers of alerts and false positives make investigation time-consuming
- Once an attack is confirmed security teams find it difficult to identify all the impacted endpoints to take protective action

Symantec Endpoint Detection and Response (EDR) exposes persistent attacks with precision detections and global threat intelligence, minimizing false positives and helping to ensure high levels of productivity for security teams. Symantec EDR exposes advanced attacks with precision machine learning and global threat intelligence minimizing false positives and helps ensure high levels of productivity for security teams. Symantec EDR capabilities allow incident responders to quickly search, identify and contain all impacted endpoints while investigating threats using a choice of on-premises and cloud-based sandboxing. Also, Symantec EDR enhances investigator productivity with automated incident playbook rules and user behavior analytics that brings the skills and best practices of the most experienced security analysts to any organization, resulting in significantly lower costs. Symantec empowers security teams to:

**Detect** and expose attack methods at the endpoint and using AI-driven cloud analytics.

**Investigate** and contain via proactive threat hunting and forensic analysis with advanced investigation tools.

**Resolve** by deleting malicious files and associated artifacts on all impacted endpoints; black and whitelist files

**Automate and Integrate** by unifying investigator views, and orchestrate data and work flows



### Detect Stealthy Threats

Get alerted to threats that 'hide in plain sight'



### Hunt and Investigate IoCs

Find suspicious objects, inspect, convict and contain



### Rapidly Fix Endpoints

Remediate impacted endpoints with one-click



### Automate and Integrate

Enhance productivity for analysts at every level

## Why State of West Virginia can trust Symantec

Organizations with sensitive data to protect have many reasons to trust Symantec. With 385,000 customers worldwide, Symantec is the world's largest cybersecurity company. For example, our customers include some of the world's largest government agencies and financial institutions who are constant targets of professional cyber-crime organizations, well-funded nation states, hacktivists, and insider threats.

More organizations trust Symantec than any other cybersecurity company because we are the world leader in protecting sensitive data, whether on premises or in the cloud, on mobile, desktop, or Internet of Things (IoT) devices, whether in use, at rest, or in transit, whether encrypted or not, whether you have a large security staff or none at all – with Symantec, you are protected. This is

because of the breadth of our products and services – we can solve all of your most critical security needs.

As we continue to build on the capabilities established during our 30+ years of protecting highly sensitive information, we are creating the world's leading integrated cyber defense program to help our customers solve their biggest cybersecurity challenges:

- Staying ahead of advanced threats
- Securing the mobile workforce
- Helping customers securely embrace the cloud

It's easy for any company to claim that they are a leader. However, the most prominent industry analysts consistently rank Symantec as a global leader in security innovation. For instance, for 15 years running, Gartner has named Symantec a global leader in Endpoint Protection. For 13 years running, Gartner has named Symantec a global leader in Managed Security Services. For 10 years running, Gartner has named Symantec a global leader in Data Loss Prevention. In independent third party testing, other Symantec products have won awards and been independently validated as best in their class.

Symantec's leadership does not happen by accident. Our innovation is driven by our scale, product breadth, and massive engineering and research investment. We have 3,000 cybersecurity engineers and continuously learn from our research and real world experience. That experience includes protecting 64,000 data centers, 175,000 endpoints, 12,000+ cloud apps, scanning 2 billion emails daily, categorizing 1 billion web requests daily, processing 4 million previously unseen threats daily, and the largest civilian global intelligence network in the world. All of this gives us unmatched telemetry and insight, which fuels our innovation and leadership.

We are so convinced of the effectiveness of our products and services that we use and depend on them to protect our highly sensitive information. This proposal explains the numerous, compelling benefits of deploying the solutions in your enterprise that we and 385,000 other organizations use in ours. Your Symantec team looks forward to working with you and to address your most pressing challenges. Our goal is to enable you to protect your enterprise — no matter where it is, and no matter how the threat landscape evolves.

## Proposed Solution

---

After carefully reviewing your business objectives, Symantec is pleased to recommend the following solution. Symantec is confident that this solution meets stringent State of West Virginia requirements and successfully addresses its most pressing challenges. The following information details how Symantec can help State of West Virginia realize the many benefits of this comprehensive and compelling solution.

### Symantec Endpoint Detection and Response

Symantec Endpoint and Detection and Response (EDR) detects and exposes attackers in their environment—no new agent required. Supported by deep endpoint visibility, precisely detect and actively hunt threats to quickly expose and fully resolve them, no matter how persistent. EDR instantly detect advanced attack methods using behavioral policies continually updated by Symantec researchers. EDR detects new attack patterns in minutes, and alert responders to attacks in progress, with analytics continuously trained by global telemetry, and quickly analyze attack chains and remediates impacted systems using risk-scored history of endpoint activity.

Symantec EDR supports 'zero trust' threat hunting with advanced forensics tools that use full memory scans and metadata acquisition to find injections, process hollowing, shellcode, and more. Symantec EDR speeds threat hunting and response with deep visibility, precision analytics, and workflow automation. Symantec EDR detects, hunts, isolates, and eliminates intrusions across all endpoints using AI-driven analytics, investigation playbooks, and unequaled threat intelligence.

### Increase Investigator Productivity

Symantec EDR increases investigator productivity by prioritizing incidents by risk. And Symantec EDR automatically generates incidents for targeted attacks identified through Symantec's Target Attack Analytics and Dynamic Adversary Intelligence. EDR enables users to create custom investigation flows and automate repetitive manual tasks and automatically sandbox suspicious files for quick conviction and blacklisting – with no complex scripting required.

In addition, investigators can take advantage of Endpoint Activity Recording to hunt for Indicators of Attack and perform endpoint analysis. Symantec EDR supports continuous and on-demand retrieval for a wide range of events including session, process, module load point modifications, file and folder operations, registry changes and network connection activity. EDR streamlines SOC operations and lower costs with prebuilt apps for SIEM, orchestration, and ticketing systems. EDR provides visual graphs and alerts to simplify how security analysts work with large amounts of cyber data.

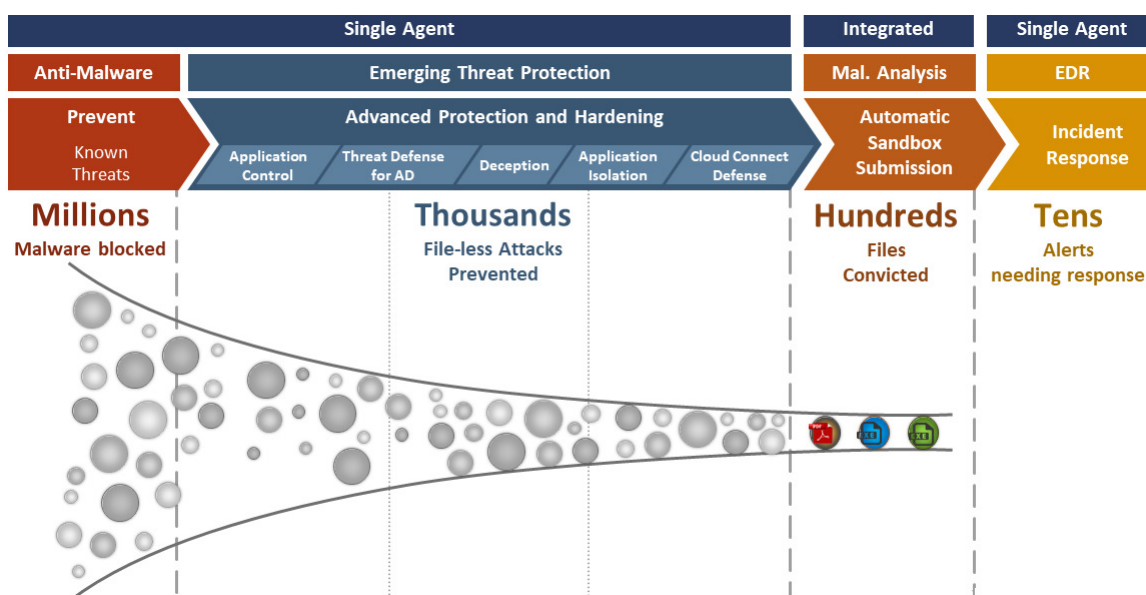
According to Symantec Internet Safety and Threat Report (ISTR), more than 20% of the malware is VM-aware which means they evade detection in a traditional sandbox. Symantec EDR can detect such VM-aware threats by employing advanced techniques that include mimicking human behavior and if necessary, using physical servers for detonation.

### Cloud-based Attack Analytics and Endpoint Advanced Attack Detections

Symantec EDR includes Targeted Attack Analytics (TAA). TAA parses global activity, the good and the bad, across all enterprises that comprise our telemetry set. Our cloud-based artificial intelligence algorithms and advanced machine learning adapts to new attack techniques automatically. TAA creates a real-time incident—with a detailed analysis of the attacker, techniques, impacted machines, and remediation guidance—and streams it to the EDR console. This approach streamlines the efforts of incident responders and enhances productivity for the entire security team (TAA is provided at no additional cost to Symantec customers using Advanced Threat Protection 3.1 or higher).

Symantec EDR also leverages endpoint behavioral polices, continually updated by Symantec researchers, to detect advanced attack methods instantly at the endpoint (over 330 currently available).

These detections detail activity that may indicate attacks in progress including file and registry changes, suspicious network and processes activity and use of specific Windows API's that can be used to start a malicious thread within an existing process.



### Hunt for Anomalies Across Endpoints

Symantec EDR simplifies the hunt for attackers within the environment by providing an across the board view of software, memory, user, and network baseline activity. When attackers operate in the environment, their malware and user activity stand out as anomalies or outliers.

Symantec EDR exposes outliers across the environment including:

- Software outliers – Expose endpoints that have uncommon software, build discrepancies, unpatched or old operating system (OS) releases
- Memory outliers – Detect memory-resident outliers using forensic examination of process memory, file and OS object, and system settings
- User outliers – User behavior analytics detect attackers acting as legitimate users performing unusual activity
- Network outliers – Leverage statistical analysis to identify anomalous IP addresses, reputation lookups identify IP addresses and domains associated with data exfiltration

These outlier detections are provided via cloud-based service and are available using built-in playbooks that produce specific reports on wide variety of anomalous activity.

### MITRE ATT&CK Event Enrichment and Cyber Analytics

Symantec EDR provides tools to detect and visualize the attack lifecycle based on the MITRE ATT&CK framework. The EDR tool describes attack methods based on the standard tactics and techniques in the ATT&CK matrix. In addition, quick filters make it easy for investigators to narrow results to one or more phases of the MITRE ATT&CK lifecycle including initial access, persistence, lateral movement and command and control.

Critically, Symantec EDR supports MITRE Cyber Analytics through automated investigation playbooks. MITRE recommends organizations implement a zero-trust approach to forensic collection and investigation by interrogating autorun differences, suspicious run locations, potential DDL injections and SMB event monitoring. Symantec EDR makes it easy to run

scheduled sweeps across endpoints to determine if any attacks can be detected using common knowledge of the MITRE community of adversary models.

### **Complete and Rapid Endpoint Repair**

Symantec EDR supports rapid remediation of impacted endpoints including file deletion, blacklisting and endpoint quarantine. Using powerful eraser capabilities built into Symantec Endpoint Protection (SEP), responders can take action from a single console and with one click apply a fix across multiple endpoints.

### **Automate Skilled Investigator Practices**

Symantec EDR supports playbooks that automate the complex, multi-step investigation workflows of security analysts. Built-in playbooks quickly expose suspicious behaviors, unknown threats, lateral movement and policy violations. The security team can view the playbooks to learn expert hunting and investigation techniques. In addition, Investigators can create their own playbooks to automate best practices and document specific threat hunting scenarios.

# RESPONSE TO MANDATORY REQUIREMENTS

---

## **4.1 Mandatory Contract Services Requirements and Deliverables:**

Contract Services must meet or exceed the mandatory requirements listed below.

### **4.1.1 Contract Item: Endpoint Detection and Response Software**

#### 4.1.1.1 Containment & Remediation

Symantec Complete Endpoint Defense is a bundled solution by Symantec that meets and exceeds the needs of the State of West Virginia as defined below. This solution has been rated by Gartner as the leader in vision and ability to execute in the most recent Gartner MQ report and is the only solution to have maintained a spot in the leaders' quadrant for over 10 years.

In the proposed solution below, Symantec will provide the ability for the State of West Virginia to:

- Leverage Symantec's Endpoint Detection and Response capabilities to automatically detect and respond to events
- Leverage Symantec's industry leading Application Isolation and Application Control functionality
- Leverage Symantec's Threat Protection for AD component - which monitors for malicious AD traffic, uses AI to provide false responses, and provides targeted alerts for unauthorized privilege escalation attempts.

Symantec enjoys the privilege of being the largest cyber-security company in the world with the broadest scope of products. Our Threat protection tools are the life of Symantec and have teams of researchers working globally to analyze threats and ensure protections are in place before they are needed. Symantec enjoys the opportunity to work with the State of West Virginia in securing its endpoints.

4.1.1.2 The Vendor must provide a software and/or service that is capable of supporting a minimum of two thousand (2,000) endpoints throughout the State of West Virginia

The Symantec solution proposed below has deployments ranging from under 500 endpoints to well over 100,000 endpoints.

4.1.1.3 The Vendor must provide a software and/or service that can be centrally managed by a West Virginia Office of Technology Administrator.

Symantec provides the ability for the products listed below to be managed on-premise, full cloud, or in a hybrid mode. In each mode, all clients can be seamlessly managed no matter where they may travel globally.

4.1.1.4 The Vendor must provide a software and/or service that shall feature the following:

4.1.1.4.1 Automatically restrict potentially malicious activity to within an isolation container.

Symantec's Complete Endpoint Defense has multiple defense mechanisms that will land malicious activity into isolation containers, including but not limited to:

Cynic Sandbox - new files that are blocked from running/quarantined on a system can be automatically submitted to Symantec's Cynic sandbox where the file is executed in virtual and bare metal systems to determine what activity was intended and provides a response back with all attempted changes and network connections for event correlation, SEIM aggregation, or further discovery.

SEP Isolation - If a file is determined to be unknown but not malicious, SEP can isolate a file/process away from the OS into three distinctive buckets based on policy. High Isolation ensures that the file/process can be used but can make zero impact to the system. Medium Isolation allows the utilization of some protected system resources but not modification. Lastly low isolation allows for the configuration of some trusted updaters or resources that are allowed to be modified. Policies can be set to trigger based off of known publishers, reputation in the Symantec Global Intelligence Network, prevalence in the environment, or days available.

SEP Emulator - Before Cynic Sandbox or SEP Isolation is utilized, SEP Emulator will unpack unknown, obfuscated files to determine their risk level and share this information with other in use engines to determine if the file should be allowed, isolated, quarantined, or deleted.

#### 4.1.1.4.2 Automatically isolate applications interacting with untrusted content from more trusted portions of the device outside the container.

Symantec Complete Endpoint Defense includes a feature from Symantec called Application Isolation. This feature allows Symantec to dynamically identify apps that may pose a risk to the environment and then isolate into High, Medium, and Low risk containers as mentioned in answer 4.1.1.4.1. Such examples of isolation policy could dictate that all unknown files are placed into high isolation until further identified, or that any file signed by the State of West Virginia and that has a good reputation can be trusted.

The levels of isolation can be set dynamically by file elements, prevalence in the environment, age, publisher, etc. A drift analysis is also available as an automated report to help administrators keep tabs on trusted applications in the environment that might have changed over time since initial policy creation.

#### 4.1.1.4.3 Automatically detect and isolate potentially malicious code behavior.

Symantec Complete Endpoint Defense is capable of isolating files or systems as needed. Symantec will can automatically quarantine files/process based on behavior and, if primary actions fail, can enforce a complete endpoint quarantine where the system is denied network access except to defined IT tools. Symantec also provides the ability for runbooks/playbooks to be generated for automatic enforcement using the MITRE framework as a means to define infection attempts.

#### 4.1.1.4.4. Continuously detect, and isolate threats based on machine learning, behavioral analytics, and custom detection rules.

Symantec Complete Endpoint Defense meets this need across the board. Symantec has the highest rated Endpoint solution by third party reviews, such as the Gartner Magic Quadrant, and is the longest leader in the space being the only Endpoint platform to hold MQ Leader status since the report's inception. Symantec Complete Endpoint Defense includes such engines as AML (Advanced Machine Learning), SONAR (heuristics and analytics), Bloodhound (AI and heuristics), Cynic (cloud sandbox), and Application Isolation (for risky behaviors or file types).

#### 4.1.1.4.5 Automatically capture necessary event details on all malicious activity, including but not limited to ports and protocols in use, running executables and services, and browser plugins occurring within the isolation container to support retrospective post-event analysis, threat analysis, and situational awareness.

Symantec Complete Endpoint Defense has a complete EDR console available for user that captures these details and more. Each discovered incident automatically reviews the attack to see if it is originating from a known attacker and alerts to the type (determined attacker, nation state, activist, etc.), automatically sandboxes unknown executable files, alerts to discovered IOCs, and displays items such as ports/protocols, active connections, signed in user, originating processes, etc.



More importantly a Flight Data Recorder is available on the system to see every action that was taken within a defined period (example: recording set for last 7 days). IOCs that come from any event will automatically be searched for and correlated. Triggering events are marked for easy discovery with bright red text stating "Triggering Event" and all events are attempted to be mapped to the MITRE framework to assist in expediting responses.

4.1.1.4.6 Be configurable to control the ability of applications running within the isolation container to access only specified system resources.

Symantec Complete Endpoint Defense fully meets this need with the feature Application Isolation. The Application Isolation feature provides a predefined High, Medium, and Low isolation container. Administrators can easily change the level of access and trust for each container by policy. Policy can be modified granularly by group so that high risk clients can be as aggressive with the protection as deemed necessary by administrators.

4.1.1.4.7 Provide the ability to restrict execution of high-risk applications and computer processing activities to an isolated environment.

Symantec Complete Endpoint Defense includes the features of Application Control and Application Isolation. Together these features can define what applications should be allowed to run on a system and in turn either block unknown apps from running or force isolation of unlisted applications.

Symantec's Application Isolation and Application Control feature is built on the same base engine as Symantec Critical System Protection which has hosted a capture the flag event at Black Hat with no winners to date.

4.1.1.4.8 Automatically eliminate and report all isolation container artifacts of compromise and intrusion remnants.

Symantec Complete Endpoint Defense does not retain artifacts by default unless told to quarantine items or to submit them to the EDR service for outside inspection.

4.1.1.4.9 Provide continual verification of the integrity of the isolation container to ensure there is no unauthorized/malicious access or persistent modification.

Symantec Complete Endpoint Defense does not persist isolation containers. If an event is determined that could attempt to escape isolation the container and its contained process/content are stopped and a new container will be created for the next process/event as needed.

4.1.1.4.10 Automatically report potentially malicious events detected within the isolation container and provide actionable information.

Symantec Complete Endpoint Defense will report all malicious and suspicious events by default. To Symantec it is critically important that such items be logged and stored if needed for further investigation. Similarly, Symantec strongly encourages the use of sys-logging to ensure that endpoint data is being used to trigger alerts and security responses from other tools in the environment.

4.1.1.4.11 Be capable of containing operating system kernel-level vulnerability exploitation.

Symantec Complete Endpoint Defense has multiple channels monitoring for such events and has a track record for exceeding standard protection norms. One such example would be our defense of WannaCry and Petya\NotPetya in which Symantec customers enjoyed a global 0% infection rate.

- 4.1.1.4.12 Provide options for configurable automated or manual remediation actions in response to detected potentially malicious events.

Symantec Complete Endpoint Defense's EDR platform allows for automated playbooks to be developed to take defined actions when an event or series of events occurs. Such an example could be that if a file is discovered as potentially malicious or a known IOC, the device can be removed from the network and put in an isolation zone until the morning when security administrators have a chance to manually remediate the system.

All of Symantec's automated response capabilities can also be triggered manually by security administrators even without a corresponding Symantec alert.

#### 4.1.1.5 Reporting & Monitoring

- 4.1.1.6 The Vendor must provide a software or service that shall interoperate with event monitoring and correlation systems to facilitate aggregated situational awareness.

Symantec fully supports syslog via its tools and encourages the use of this feature as well as our open APIs to integrate Symantec products with other items in the existing security stack.

- 4.1.1.7 The software shall support open standards for automated threat information sharing.

SIEM integrations are fully supported via both syslog feeds and the RESTful API data feed with external services, such as threat feeds.

- 4.1.1.8 The software shall provide integrated and customizable search with, at minimum, the ability to search data from all systems for information relevant to an incident investigation or risk analysis.

Symantec EDR will automatically correlate event data for any threat it detects in the environment. Above this, investigators/administrators will have the ability to manually search for IOCs (via hash, STIX/TAXII report, etc.) and allow the EDR tool to correlate systems with like indicators. For each system, the running process and network connections can be viewed for each system as well as full process trees.

In addition to this each event is evaluated against the MITRE framework to ensure that an accurate timeline of attempted incursions is provided.

- 4.1.1.9 The software shall have the ability to execute manual and scheduled scans of specified systems for indicators derived from threat intelligence or other sources.

Symantec supports Daily, Weekly and Monthly scan thresholds to look for known malware and to analyze systems for new anomalies. Playbooks can be built on these scans to ensure that an initial response is given in line with the State of West Virginia's expectations.

- 4.1.1.10 The software shall provide integrated analytics (including visualization) and support the creation of custom analytics, in order to identify anomalous endpoint behaviors, support incident investigation, and perform event analysis.

Symantec Endpoint Detection and Response provides threat maps of incidents that allow modification of how elements are viewed. Below this, investigators will find a time sorted forensic print out of each event and all available meta data (example: MITRE Framework placing, Triggering Event status, parent process, active user, etc.). If there are any correlations with other incidents, the incident and its response will be listed for consideration. Furthermore, Symantec EDR receives threat intelligence from our Global Intelligence Network and will educate incident responders if items appear to be a targeted attack and/or originate from a known organization (nation-state, crime unit, activists, etc.)

4.1.1.11 The software shall allow administrative functions to be delegated to users based on roles/permissions and or groupings of endpoints they are responsible for managing.

Symantec provides full Role Based Access Controls for its systems as well as audit functionality to ensure each action is logged and recorded for accountability.

4.1.1.12 The software shall support delegation (i.e., user-specified) of who can access/view collected endpoint data.

Symantec provides full Role Based Access Controls for its systems. Granular access can be provided to particular groups/units inside of the organization.

4.1.1.13 The software shall have the capability to be tuned/configured to reduce alerts resulting from false positives.

Symantec allows for events and notifications to be tuned to help focus investigators on useful events.

4.1.1.14 The software shall provide configurable alerting based upon administrator defined criteria.

Symantec fully supports notifications and alerts from inside of the product, but also highly recommends the use of syslog to integrate Symantec event details with other security tools.

4.1.1.15 The software shall send alerts at administrator-definable intervals.

Symantec supports alert thresholds being defined. For example - if 10 new pieces of malware are found in under a minute and administrator may be notified immediately however if 10 new pieces of malware were found over the course of a day and all were remediated a daily report would be sent at the defined time.

4.1.1.16 The software shall provide the ability to automatically discover and alert on previously unknown external and/or internal hardware/peripheral devices (such as storage) connected to endpoints for the purpose of retrospective/post-event analysis.

Symantec supports the ability to log all plugged in devices. An additional option with this feature is to also log file names that are written to peripheral devices. Content inspection can be integrated with Symantec DLP if this becomes a consideration for the State in the future.

4.1.1.17 The software shall generate reports based on pre-saved userdefined formats and datasets to facilitate rapid analysis, decision making, and follow-up actions following events.

Symantec reports can be tuned to provide desired content for easier analysis. Similarly, notifications can be set to alert on user defined thresholds. For instance, one administrator may want to be defined if a number of systems go offline at one time and another administrator may only care if malicious/suspicious detections have occurred.

4.1.1.18 The software shall provide time stamping of all collected data and events based on a single time standard (e.g., coordinated universal time).

Symantec meets this requirement fully across all product sets. Having a single time standard is critical to incident remediation.

4.1.1.19 The software shall have the ability to pull locally stored data from specified endpoints in near real time to support high priority hunt and forensic operations.

Symantec Endpoint Detection and Response has the ability to pull full endpoint recordings from the system as well as the ability to pull individual file items from a system to a no-execution zone where forensic teams can access the file and move for the benefit of their investigation.

4.1.1.20 The software shall provide automated analysis and visualization of an attack; including production of an event timeline and initial assessment of severity/impact.

Symantec Endpoint Detection and response provides a visual and forensic output for all incidents.

- The incident map provides objects for URLs, Systems, and files/objects that make up the incident. Each object can be moved on the map to help with sorting and investigation.

- The forensic print out is a chronological report for each event in the process with data elements surrounding each event. Each event can be opened to review associated details. The forensic team can build custom views to help ease incident remediation and pull out data elements for easier inspection - such as if an item is a triggering even, unknown to Symantec, or made a network connection.

## 4.1.2 Technical Details

4.1.2.1 The Vendor must provide the minimum supported platforms including: Windows operating system, Linux operating system, and all virtual environments including but not limited to VMWare, Azure, and Hyper-V.

Client Workstation and Server System Requirements

Windows® Operating Systems

- Windows Vista (32-bit, 64-bit)
- Windows 7 (32-bit, 64-bit; RTM and SP1)
- Windows Embedded 7 Standard, POSReady, and Enterprise (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows Embedded 8 Standard (32-bit and 64-bit)
- Windows 8.1 (32-bit, 64-bit), including Windows To Go
- Windows 8.1 update for April 2014 (32-bit, 64-bit)
- Windows 8.1 update for August 2014 (32-bit, 64-bit)
- Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (32-bit, 64-bit)
- Windows 10 (32-bit, 64-bit)
- Windows 10 November Update (2015) (32-bit, 64-bit)
- Windows 10 Anniversary Update (2016) (32-bit, 64-bit)
- Windows Server 2008 (32-bit, 64-bit; R2, SP1, and SP2)
- Windows Small Business Server 2008 (64-bit)
- Windows Essential Business Server 2008 (64-bit)
- Windows Small Business Server 2011 (64-bit)
- Windows Server 2012

- Windows Server 2012 R2
- Windows Server 2012 R2 update for April 2014
- Windows Server 2012 R2 update for August 2014
- Windows Server 2016

#### Windows Hardware Requirements

- 1.9 GHz CPU or higher
- 1 GB of RAM (2 GB recommended)
- 530 MB of free space on the hard disk

#### Macintosh® Operating Systems

- Mac OS X 10.10, 10.11, macOS 10.12, 10.13

#### Mac Hardware Requirements

- 64-bit Intel Core 2 Duo or later
- 2 GB of RAM
- 500 MB of free space on the hard disk

#### Virtual Environments

- Microsoft Azure
- Amazon WorkSpaces
- VMware WS 5.0, GSX 3.2, ESX 2.5 or later
- VMware ESXi 4.1 – 5.5
- VMware ESX 6.0
- Microsoft Virtual Server 2005
- Microsoft Enterprise Desktop Virtualization (MED-V)
- Microsoft Windows Server 2008, 2012, and 2012 R2 Hyper-V
- Citrix XenServer 5.6 or later
- Oracle Cloud
- Virtual Box by Oracle

#### Linux Operating System (32-bit and 64-bit versions)

- Amazon Linux
- CentOS 6U3, 6U4, 6U5, 6U6, 7, 7U1, 7U2, 7U3; 32-bit and 64-bit
- Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit

- Fedora 16, 17; 32-bit and 64-bit
- Oracle Linux (OEL) 6U2, 6U4, 6U5, 7, 7.1, 7.2, 7.3
- Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U8, 7 - 7.3
- SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP3; 32-bit and 64-bit; 12
- SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP3; 32-bit and 64-bit
- Ubuntu 12.04, 14.04, 16.04; 32-bit and 64-bit

#### Linux Hardware Requirements

- Intel Pentium 4 (2 GHz CPU or higher)
- 1 GB of RAM
- 7 GB of free space on the hard disk

The EDR on-premise appliance is a Virtual Appliance requiring:

- 12 cores
- 48 GB memory
- 500GB disk

4.1.2.2 The software shall not impair authorized system operations nor shall it degrade managed system performance in any way, which may adversely impact a system's primary business/mission functions. The following authorize system operations include but not limited to:

4.1.2.2.1 Patching, Scanning, Business software usage,

By default, Symantec products do not typically interfere with patching software or known business applications. In the event of any issues, Symantec offers centralized whitelisting to allow permitted business and patching applications to run without impact. Scanning solutions without an installed agent soliciting the traffic will also need to be whitelisted as out of the box Symantec will block most unsolicited inbound traffic.

4.1.2.2.2 The following Information Assurance Tools/Initiatives include but not limited to:

Symantec has a broad knowledge of other security and assurance tools and makes every effort to ensure compatibility if possible. In some cases, items like Vulnerability scanners will need to be explicitly whitelisted due to the nature of the product (unsolicited traffic checking known vulnerabilities). In most cases, Symantec can be deployed along other security tools with little to no configuration.

4.1.2.2.2.1 Secure host baseline, and assured compliance assessment software.

As part of the proposed solution, Symantec offers features around Host Integrity Monitoring that can check to ensure systems are compliant with the expected configuration. Symantec also works with other tools that may exist in this space such as ForeScout, Cisco, BigFix, and more.

4.1.2.3 The software shall allow for patching and update of containerized applications through a means of automated verification (e.g., integration with automated patch management infrastructure/processes).

Symantec fully meets this requirement. Isolated applications are not allowed to make changes to the system, but defined applications (such as SCCM for example) can be allowed to modify isolated applications.

4.1.2.4 All software components shall have the ability to be automatically deployed and configured based on predefined configurations.

Symantec provides several deployment options such as:

- A Symantec hosted deployment wizard
- Ability to push clients via software deployment tools (SCCM, Tanium, ITMS, etc.)
- Ability to force install of clients via GPO.

Defined policy baselines are included in the client to ensure it is protected automatically after install. As part of the installation process clients will attempt to check in and verify that the bundled policy is still the current policy. If not, updates are made to ensure a consistent experience from the start.

4.1.2.5 The software shall securely store and transmit data in a manner that ensures the confidentiality, integrity, availability, and source authenticity of the data.

By default, Symantec solutions are installed with TLS enabled and enforced. Manual intervention is required to deprecate this security.

4.1.2.6 The software shall encrypt all data in transit or data at rest with Federal Information Processing Standards (FIPS) 140-2 compliant cryptographic modules.

Symantec supports FIPS 140-2 compliance for client/server communication.

### **4.1.3 Optional Renewals**

4.1.3.1 Vendor should include, as part of its bid, pricing for optional renewal years 2, 3, and 4. These optional renewal years will be agreed upon by both parties and initiated by the Agency via Change Order. The contract will be awarded on the initial year's cost only.

As referenced in Exhibit A Pricing page, for years 2, 3 and 4 the Symantec price will not exceed an annual increase of 5%. This is shown as a ceiling price not an automatic increase.

## About Symantec

Symantec Corporation, founded in 1982, is the world's largest pure-play cybersecurity company. With 11,000 employees and operations in 46 countries, organizations across the world look to Symantec for strategic, integrated solutions to defend against the most sophisticated attacks across their endpoints, email, cloud environments, the web, and networks. Symantec protects 15,000 enterprises worldwide, enabling them to take full advantage of cloud services without compromising the security of the people, data, applications, and infrastructure that drive their business. Our advanced technology portfolio is powered by the world's largest civilian threat intelligence network, enabling us to see and protect against the most advanced threats.

Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. We are solely focused on helping organizations of all sizes, governments, and individuals secure their most important data wherever it lives.

Symantec's individual product technologies are unsurpassed with multiple products being named as leaders by industry analysts, such as Gartner, Forrester and others. Symantec was recently named as the 'top-right' leader in Zero Trust

(<https://resource.elq.symantec.com/LP=6476?cid=70138000001Ffr9AA>), validating Symantec as the unrivaled leader in cybersecurity efficacy.

In addition to Symantec's enterprise leadership in cybersecurity, the Symantec product family protects a global community of over 50 million people and families with Symantec's Norton and LifeLock product suites, securing their digital lives at home and across all their devices.



### Integrated Cyber Defense

Having superior products isn't sufficient to address the evolution of cyber threats. The complexity of managing many disparate tools drives up the cost of a cybersecurity strategy. Products must integrate and work in unison to form a unified cyber defense strategy.

#### Symantec's approach is different and superior

Our Cyber Defense Platform unifies cybersecurity products, services, and partners. The Cyber Defense Platform drives down the cost and complexity of cybersecurity, while protecting enterprises against ever increasingly sophisticated threats.

Symantec understands that many organizations intentionally use a mix of Symantec and 3rd party products that aren't integrated. To solve this, our Integrated Cyber Defense Exchange (ICDx) standardizes the interfaces between Symantec's portfolio of enterprise security solutions and a diverse ecosystem of hundreds of 3rd party technology partners.

#### Benefits of Integrated Cyber Defense

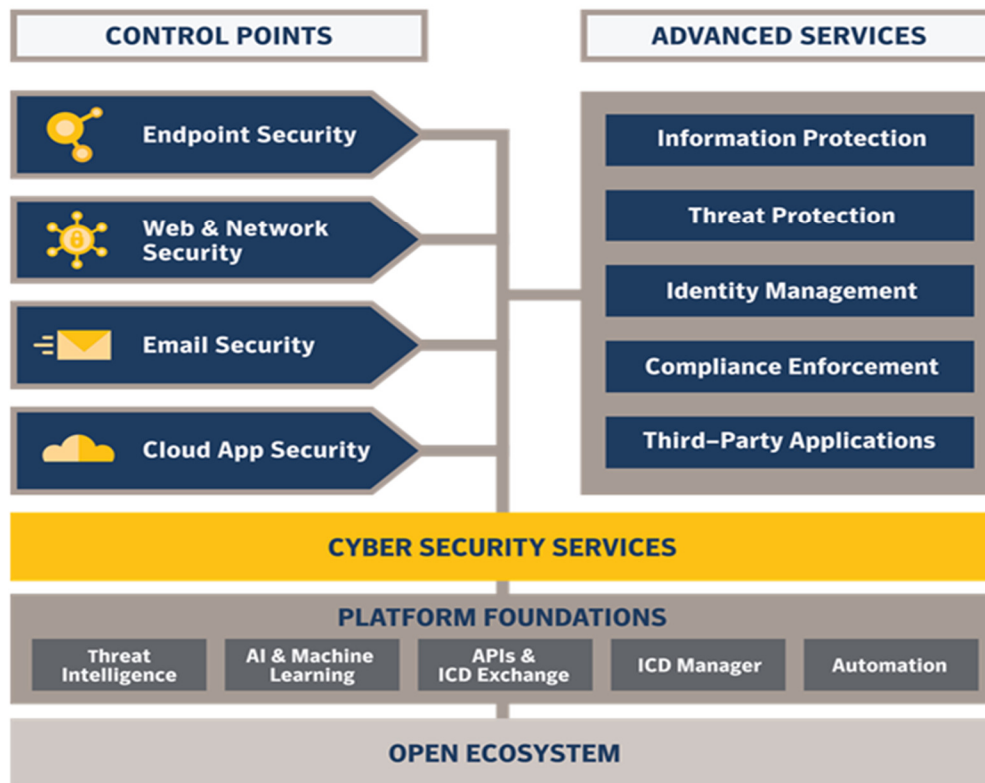
- **Simplifies Operations and Reduces Costs** by integrating tools and consolidating controls
- **Reduces Organizational Risk** by hardening security and covering new exposure points
- **Speeds Cyber Response** by integrating cross-organization workflows

The foundational component of the Platform is an Integrated Cyber Defense Exchange (ICDx), which combines information protection, threat protection, identity management, compliance and other advanced services, powered by shared intelligence and automation across endpoints, networks, applications, and clouds.

The ICD Platform gives Symantec customers a single point of integration that only requires simple configurations within an easy to use console in order to centralize, normalize, archive, filter and forward events from all supported Symantec and 3rd party products. ICDx integrates data, such as Indicators of Compromise (IoC) for a range of control points including Endpoint Security, Web & Network Security, Email Security, and Cloud App Security.



# Integrated Cyber Defense Platform



## Innovation Driving Growth

To maintain its industry leadership and protect customers in the face of ever evolving threats, Symantec embraces a global research and development (R&D) strategy to drive organic innovation. More than 3,000 engineers and researchers throughout the company pursue advanced projects to translate R&D into customer solutions by creating new technologies and integrating our unique set of technology assets. Symantec focuses on short, medium, and long-term applied research, develops new products in emerging areas, participates in government-funded research projects, drives industry standards, and partners with universities to conduct research supporting Symantec's strategy. This has resulted in Symantec holding over 2,000 patents.

## Corporate Responsibility

Symantec is committed to conducting business with respect and attention to ethical operation, a diverse and inclusive workforce, the environment, and positive societal impact. We share our progress in delivering on this commitment in our corporate responsibility report, [Securing a Sustainable Future](#). We have developed this report using the [Global Reporting Initiative \(GRI\)](#) Sustainability Reporting Standards at the "Core in Accordance" level. The report describes how we are taking action to address our priority issues and serves as our annual Communication on Progress (COP) as a signatory to the United Nations Global Compact.

Confidence in a connected world.



**Symantec™**

