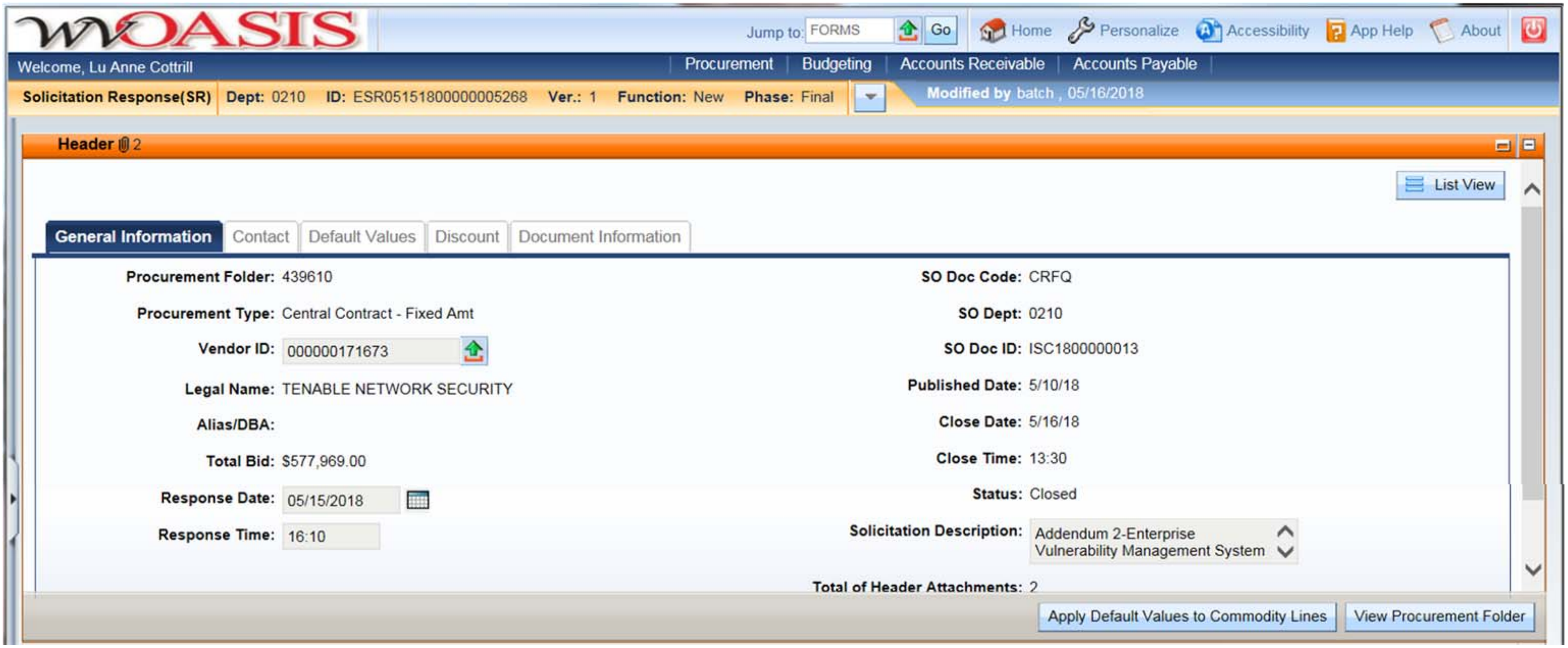
West Virginia
Purchasing Division

2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970

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



Welcome, Lu Anne Cottrill

Solicitation Response(SR) **Dept:** 0210 **ID:** ESR05151800000005268 **Ver.:** 1 **Function:** New **Phase:** Final

Modified by batch , 05/16/2018

Procurement Folder: 439610

Procurement Type: Central Contract - Fixed Amt

Vendor ID: 000000171673

Legal Name: TENABLE NETWORK SECURITY

Alias/DBA:

Total Bid: $577,969.00

Response Date: 05/15/2018

Response Time: 16:10

SO Doc Code: CRFQ

SO Dept: 0210

SO Doc ID: ISC1800000013

Published Date: 5/10/18

Close Date: 5/16/18

Close Time: 13:30

Status: Closed

Solicitation Description: Addendum 2-Enterprise Vulnerability Management System

Total of Header Attachments: 2

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

State of West Virginia
Solicitation Response

Proc Folder : 439610

Solicitation Description : Addendum 2-Enterprise Vulnerability Management System (EVMS)

Proc Type : Central Contract - Fixed Amt

Date issued	Solicitation Closes	Solicitation Response	Version
	2018-05-16 13:30:00	SR 0210 ESR05151800000005268	1

VENDOR

000000171673

TENABLE NETWORK SECURITY

Solicitation Number: CRFQ 0210 ISC1800000013

Total Bid : $577,969.00 **Response Date:** 2018-05-15 **Response Time:** 16:10:07

Comments: Tenable does not sell direct, we partner with VARs, who could possibly be able to negotiate any additional payment term discounts during the negotiation phase. The pricing included herein is via a VAR quote, with associated discount pricing, less than our MSRP pricing.

FOR INFORMATION CONTACT THE BUYER

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

Signature on File **FEIN #** **DATE**

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	Enterprise Vulnerability Management System (EVMS), License	1.00000	EA	$139,705.000000	$139,705.00

Comm Code	Manufacturer	Specification	Model #
43233701			

Extended Description : 3.1.1-3.1.4.9 Enterprise Vulnerability Management System (EVMS), Annual License Service - 1 Year - 25,000 assets - Warranty Included

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Central Management Appliance	1.00000	EA	$9,299.000000	$9,299.00

Comm Code	Manufacturer	Specification	Model #
43210000			

Extended Description : 3.1.5-3.1.5.1.4 Central Management Appliance per specifications.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	System Deployment	1.00000	EA	$9,850.000000	$9,850.00

Comm Code	Manufacturer	Specification	Model #
81111500			

Extended Description : 3.1.6-3.1.6.3.1 System Deployment

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	License Optional Renewal Year 2	1.00000	EA	$139,705.000000	$139,705.00

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description : 3.1.8 Optional Renewal Year 2

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
5	License Optional Renewal Year 3	1.00000	EA	$139,705.000000	$139,705.00

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description :	3.1.8 Optional Renewal Year 3

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
6	License Optional Renewal Year 4	1.00000	EA	$139,705.000000	$139,705.00

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description :	3.1.8 Optional Renewal Year 4

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

State of West Virginia
Request for Quotation
21 — Info Technology

Proc Folder: 439610

Doc Description: Enterprise Vulnerability Management System (EVMS)

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2018-04-19	2018-05-10 13:30:00	CRFQ 0210 ISC1800000013	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:

Tenable Public Sector LLC
7021 Columbia Gateway Drive, Suite 500
Columbia, MD 21046

Contact: Stan Sharrow, ssharrow@tenable.com, 412-527-2193

FOR INFORMATION CONTACT THE BUYER

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

Signature X **FEIN #** 35-2597619 **DATE** 05/10/2018

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

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

State of West Virginia
Request for Quotation
21 — Info Technology

Proc Folder: 439610

Doc Description: Addendum 1-Enterprise Vulnerability Management System (EVMS)

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2018-05-10	2018-05-16 13:30:00	CRFQ 0210 ISC1800000013	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:

Tenable Public Sector LLC
7021 Columbia Gateway Drive, Suite 500
Columbia, MD 21046

Contact: Stan Sharrow, ssharrow@tenable.com, 412-527-2193

FOR INFORMATION CONTACT THE BUYER

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

Signature X **FEIN #** 35-2597619 **DATE** 05/16/2018

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

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

State of West Virginia
Request for Quotation
21 — Info Technology

Proc Folder: 439610

Doc Description: Addendum 2-Enterprise Vulnerability Management System (EVMS)

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2018-05-10	2018-05-16 13:30:00	CRFQ 0210 ISC1800000013	3

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:

Tenable Public Sector LLC
7021 Columbia Gateway Drive, Suite 500
Columbia, MD 21046

Contact: Stan Sharrow, ssharrow@tenable.com, 412-527-2193

FOR INFORMATION CONTACT THE BUYER

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

Signature X FEIN # 35-2597619 DATE 05/16/2018

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

ADDITIONAL INFORMATION:

Addendum

Addendum No.02 issued to publish and distribute the attached information to the vendor community.

****

The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) to establish a contract for the purchase of an Enterprise Vulnerability Management System (EVMS), consisting of an annual software license, central management appliance, and system deployment 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	Enterprise Vulnerability Management System (EVMS), License	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233701			

Extended Description :

3.1.1-3.1.4.9 Enterprise Vulnerability Management System (EVMS), Annual License Service - 1 Year - 25,000 assets - Warranty Included

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
2	Central Management Appliance	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43210000			

Extended Description :

3.1.5-3.1.5.1.4 Central Management Appliance per specifications.

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
3	System Deployment	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81111500			

Extended Description :
3.1.6-3.1.6.3.1 System Deployment

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
4	License Optional Renewal Year 2	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description :
3.1.8 Optional Renewal Year 2

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
5	License Optional Renewal Year 3	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description :

3.1.8 Optional Renewal Year 3

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
6	License Optional Renewal Year 4	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description :

3.1.8 Optional Renewal Year 4

SOLICITATION NUMBER: CRFQ ISC1800000013
Addendum Number: No.02

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 an additional technical question 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

Revised 6/8/2012

Q: What is the breakdown of the 25,000 IPs. Internal vs external IPs. (For Example: 15,000 Internal IPs, 10,000 External IPs)

A: The 25,000 are internal addresses.

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)

[x] Addendum No. 1

[x] Addendum No. 2

[ ] Addendum No. 3

[ ] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] 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.

Tenable Public Sector, LLC
Company

DocuSigned by:
John C. Huffard, Jr.
745494F7C8D04DE...
Authorized Signature

May 10, 2018
Date

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

Revised 6/8/2012

ADDITIONAL INFORMATION:

: The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) to establish a contract for the purchase of an Enterprise Vulnerability Management System (EVMS), consisting of an annual software license, central management appliance, and system deployment per the terms and conditions and specifications as attached.

INVOICE TO	SHIP TO
	IS&C - CHIEF FINANCIAL OFFICER
DEPARTMENT OF ADMINISTRATION	DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV 25305	CHARLESTON WV 25305
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Enterprise Vulnerability Management System (EVMS), License	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233701			

Extended Description :

3.1.1-3.1.4.9 Enterprise Vulnerability Management System (EVMS), Annual License Service - 1 Year - 25,000 assets - Warranty Included

INVOICE TO	SHIP TO
	IS&C - CHIEF FINANCIAL OFFICER
DEPARTMENT OF ADMINISTRATION	DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV 25305	CHARLESTON WV 25305
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Central Management Appliance	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43210000			

Extended Description :

3.1.5-3.1.5.1.4 Central Management Appliance per specifications.

INVOICE TO	SHIP TO
	IS&C - CHIEF FINANCIAL OFFICER
DEPARTMENT OF ADMINISTRATION	DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV 25305	CHARLESTON WV 25305
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	System Deployment	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81111500			

Extended Description :

3.1.6-3.1.6.3.1 System Deployment

INVOICE TO	SHIP TO
	IS&C - CHIEF FINANCIAL OFFICER
DEPARTMENT OF ADMINISTRATION	DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV 25305	CHARLESTON WV 25305
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	License Optional Renewal Year 2	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description :

3.1.8 Optional Renewal Year 2

INVOICE TO	SHIP TO
	IS&C - CHIEF FINANCIAL OFFICER
DEPARTMENT OF ADMINISTRATION	DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV 25305	CHARLESTON WV 25305
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	License Optional Renewal Year 3	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description :

3.1.8 Optional Renewal Year 3

INVOICE TO	SHIP TO
	IS&C - CHIEF FINANCIAL OFFICER
DEPARTMENT OF ADMINISTRATION	DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV 25305	CHARLESTON WV 25305
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
6	License Optional Renewal Year 4	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
81112200			

Extended Description :

3.1.8 Optional Renewal Year 4

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

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

□ 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: May 4, 2018 at 9:00 AM (EST)

Submit Questions to: Jessica Chambers
2019 Washington Street, East
Charleston, WV 25305
Fax: (304) 558-4115 (Vendors should not use this fax number for bid submission)
Email: Jessica.S.Chambers@wv.gov

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

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

The bid delivery address is:
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

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

SEALED BID:
BUYER: Jessica Chambers
SOLICITATION NO.: CRFQ ISC1800000013
BID OPENING DATE: 5/10/2018
BID OPENING TIME: 1:30 PM (EST)
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: May 10, 2018 at 1:30 PM (EST)

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

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 only be granted upon written request and only in accordance with the West Virginia Code § 5A-3-37 and the West Virginia Code of State Rules. A Vendor Preference Certificate form has been attached hereto to allow Vendor to apply for the preference. Vendor's failure to submit the Vendor Preference Certificate form with its bid will result in denial of Vendor Preference. Vendor Preference does not apply to construction projects.

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: W. Va. Code § 6D-1-2 requires that for contracts with an actual or estimated value of at least $100,000, the vendor must submit to the Purchasing Division a disclosure of interested parties to the contract, prior to contract award. That disclosure must occur on the form prescribed and approved by the WV Ethics Commission. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. "Interested parties" means: (1) A business entity performing work or service pursuant to, or in furtherance of, the applicable contract, including specifically sub-contractors; (2) the person(s) who have an ownership interest equal to or greater than 25% in the business entity performing work or service pursuant to, or in furtherance of, the applicable contract; and (3) the person or business entity, if any, that served as a compensated broker or intermediary to actively facilitate the applicable contract or negotiated the terms of the applicable contract with the state agency: Provided, That subdivision (2) shall be inapplicable if a business entity is a publicly traded company: Provided, however, That subdivision (3) shall not include persons or business entities performing legal services related to the negotiation or drafting of the applicable contract.

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: Initial Contract Term: This Contract becomes effective on ______________________ and extends for a period of _____________________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 ___________________ 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 30 calendar days. Upon completion of the work covered by the preceding sentence, the vendor agrees that maintenance, monitoring, or warranty services will be provided for three (3) 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 _________________. The performance bond must be received by the Purchasing Division prior to Contract award. On construction contracts, the performance bond must be 100% of the Contract value.

□ **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 entitled Licensing, of the General Terms and Conditions, 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 prior to Contract award. Subsequent to contract award, and prior to the insurance expiration date, 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 mandated herein, including but not limited to, policy cancelation, policy reduction, or change in insurers. The insurance coverages identified below must be maintained throughout the life of this contract. 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

☑ **Automobile Liability Insurance** in at least an amount of: $1,000,000.00

□ **Professional/Malpractice/Errors and Omission Insurance** in at least an amount of:

□ **Commercial Crime and Third Party Fidelity Insurance** in an amount of:

□ **Cyber Liability Insurance** in an amount of:

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

□

□

□

□

□

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.

14. PAYMENT: 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. PURCHASING CARD ACCEPTANCE: The State of West Virginia currently utilizes a Purchasing Card program, administered under contract by a banking institution, to process payment for goods and services. The Vendor must accept the State of West Virginia's Purchasing Card for payment of all orders under this Contract unless the box below is checked.

□ Vendor is not required to accept the State of West Virginia's Purchasing Card as payment for all goods and services.

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. Notwithstanding the foregoing, Purchasing Division approval may or may not be required on certain agency delegated or exempt purchases.

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. BANKRUPTCY: In the event the Vendor files for bankruptcy protection, the State of West Virginia may deem this Contract null and void, and terminate this Contract without notice.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. PURCHASING AFFIDAVIT: In accordance with West Virginia Code § 5-22-1(i), the contracting public entity shall not award a contract for a construction project 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. Accordingly, prior to contract award, 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.

39. 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"). 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. If the Vendor does not wish to extend the prices, terms, and conditions of its bid and subsequent contract to the Other Government Entities, the Vendor must clearly indicate such refusal in its bid. A refusal to extend this Contract to the Other Government Entities shall not impact or influence the award of this Contract in any manner.

40. 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.

41. 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.

42. 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.

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

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

a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.

b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open heath, basic oxygen, electric furnace, Bessemer or other steel making process. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:

c. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars ($2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or

d. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

44. 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.

45. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE: W. Va. Code § 6D-1-2 requires that for contracts with an actual or estimated value of at least $100,000, 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. "Interested parties" means: (1) A business entity performing work or service pursuant to, or in furtherance of, the applicable contract, including specifically sub-contractors; (2) the person(s) who have an ownership interest equal to or greater than 25% in the business entity performing work or service pursuant to, or in furtherance of, the applicable contract; and (3) the person or business entity, if any, that served as a compensated broker or intermediary to actively facilitate the applicable contract or negotiated the terms of the applicable contract with the state agency: Provided, That subdivision (2) shall be inapplicable if a business entity is a publicly traded company: Provided, however, That subdivision (3) shall not include persons or business entities performing legal services related to the negotiation or drafting of the applicable contract. The Agency shall submit a copy of the disclosure to the Ethics Commission within 15 days after receiving the supplemental disclosure of interested parties.

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.

(Name, Title)
Stan Sharrow, Territory Sales Manager
(Printed Name and Title)
7201 Columbia Gateway Drive, Columbia, MD 21046
(Address)
Phone: 412-527-2193 Fax: 410-510-1889
(Phone Number) / (Fax Number)
ssharrow@tenable.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.

Tenable Public Sector LLC
(Company)

John C. Hufford, Jr. President
(Authorized Signature) (Representative Name, Title)

(Printed Name and Title of Authorized Representative)

May 10, 2018
(Date)

410 872 0555
(Phone Number) (Fax Number)

REQUEST FOR QUOTATION
Enterprise Vulnerability Management System – OT18175

SPECIFICATIONS

1 Purpose and Scope: The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) to establish a contract for the purchase of an Enterprise Vulnerability Management System (EVMS), consisting of an annual software license, central management appliance, and system deployment.

2 Definitions: The terms listed below shall have the meanings assigned to them below. Additional definitions can be found in section 2 of the General Terms and Conditions.

2.1 **"Contract Item"** means an annual license purchase of Enterprise Vulnerability Management System (EVMS) as more fully described by these specifications.

2.2 **"Pricing Page"** means the pages, contained in wvOASIS or attached as Exhibit A, upon which Vendor should list its proposed price for the Contract Items.

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

2.4 **"Host"** means a single, active asset, regardless of the number of associated IP addresses.

2.5 **"CVSS"** means Common Vulnerability Scoring System, a framework for rating the severity of security vulnerabilities in software.

2.6 **"SCAP"** refers to NIST's Security Content Automation Protocol, a method for using specific standards to enable the automated vulnerability management, measurement, and policy compliance evaluation systems deployed in an organization.

2.7 **"DAST"** means Dynamic Application Security Testing, a scan designed to detect conditions indicative of a security vulnerability in an application in its running state.

2.8 **"NVD"** means National Vulnerability Database, the US government repository of standards-based vulnerability management data represented using SCAP.

2.9 **"CERT"** is a division of SEI that provides a collection of internet security information related to incidents and Vulnerabilities. The CERT Knowledgebase houses the public

Vulnerability Notes Database as well as the Vulnerability Card Catalog and the Special Communications Database.

2.10 "CVE" means Common Vulnerabilities and Exposures (CVE), it is a catalog of known security threats.

2.11 "SANS" is an Institute that provides a vulnerability database that supports the CIS Critical Security Controls.

2.12 "Kerberos" is a computer network authentication protocol that works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

2.13 "API" means Application Program Interface (API), it is a set of routines, protocols, and tools for building software applications.

2.14 "Common Criteria" is an international standard (ISO/IEC 15408) for computer security certification.

2.15 "Software-as-a-Service" is a software application delivery model where a software vendor develops a web-native software application and hosts and operates (either independently or through a third-party) the application for use by its customers over the Internet.

3 GENERAL REQUIREMENTS:

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

3.1.1 Specification Validation: Vendor must provide service/application capabilities and features documentation. This documentation is preferred with the bid but must be submitted upon request.

3.1.2 The Enterprise Vulnerability Management System (EVMS) must provide full-feature vulnerability management capabilities to include, but not limited to, the specifications outlined below.

3.1.3 The State will operationally utilize the EVMS application. The EVMS will not be provided as a managed service. The State will hold responsibility for leveraging the application to carry out vulnerability management activities.

3.1.4 Enterprise Vulnerability Management System

3.1.4.1 Enterprise Vulnerability Management System (EVMS) must adhere to the following architecture, performance, scalability and licensing functionality requirements:

3.1.4.1.1 The license must provide full functionality of the service for up to 25,000 individual hosts. The 25,000 does not apply to inactive IP addresses.

3.1.4.1.2 The license must provide capability to select which hosts are covered by the service, irrespective of network or subnet.

3.1.4.1.3 The license must include discovery scanning (device enumeration) for an unlimited number of internal network IP addresses.

3.1.4.1.4 The license must include internal and external scanner device license(s) at no additional cost.

3.1.4.1.5 Minimum supported platforms for scanner hosts must include: Windows operating system, Linux operating system, virtual environments such as VMWare, Azure, Hyper-V, etc.

3.1.4.1.6 Must include internal network scanning in a distributed environment across multiple subnets.

3.1.4.1.7 Must include multiple deployment options to include: agent-based, agentless, internal network scans and external network scan capabilities.

3.1.4.2 EVMS must adhere to the following risk and remediation management requirements:

3.1.4.2.1 Must include an advanced risk scoring algorithm.

3.1.4.2.2 Risk scoring must be based on CVSS scoring, asset exploitability and susceptibility to known malware kits.

3.1.4.2.3 Risk scoring must integrate organization determined variables, such as asset criticality (critical business assets).

3.1.4.2.4 Capable of both quantitative and qualitative metrics.

3.1.4.2.5 Able to provide remediation information to include: engineer level instructions and cross linking to external database for patches, downloads, and references.

3.1.4.2.6 Support identification and management of vulnerability exceptions, to include an approval workflow.

3.1.4.3 EVMS must adhere to the following management requirements:

3.1.4.3.1 Include the following asset management functions: asset grouping, asset import, asset categorization, asset definition, and dynamic & static tagging.

3.1.4.3.2 Support data query based upon asset management functions.

3.1.4.3.3 Support role-based access control with both pre-defined and custom roles.

3.1.4.3.4 Support role-based access approval permissions to be assigned for vulnerability exclusions or exceptions.

3.1.4.3.5 Support credential management for authenticated scans.

3.1.4.3.6 Support automatic and manual update options for both the EVMS and for vulnerability and configuration updates.

3.1.4.3.7 Support workflow automation to include: scan scheduling, scan event and vulnerability alerts, and report generation and distribution.

3.1.4.4 EVMS must adhere to the following scanning requirements:

3.1.4.4.1 Capable of asset discovery/mapping scans, including operating system fingerprinting.

3.1.4.4.2 Capable of both unauthenticated and authenticated scans.

3.1.4.4.3 Capable of configuration assessment scans in accordance with NIST Security Content Automation Protocol (SCAP).

3.1.4.4.4 Capable of database configuration scans.

3.1.4.4.5 Support DAST system scan data through native or import capabilities.

3.1.4.4.6 Identify known exploits and malware kits associated with detected vulnerabilities.

3.1.4.4.7 Include customizable, pre-configured scan templates.

3.1.4.4.8 Include the ability to scan against a specific vulnerability.

3.1.4.4.9 Include capability for scheduled scans, unsafe scan checks and scan blackout capabilities on a per-scan basis.

3.1.4.4.10 Support a policy editor for custom configuration policy scans.

3.1.4.4.11 Provide a log or feedback mechanism in the event scan failure.

3.1.4.5 EVMS must adhere to the following reporting requirements:

3.1.4.5.1 Capable of aggregated reporting, leveraging the data from multiple scan engines.

3.1.4.5.2 Include pre-configured, customizable report templates to include compliance, risk prioritization and executive-level reports.

3.1.4.5.3 Capable of scheduled reports and report distribution within the system and via email.

3.1.4.5.4 Support vulnerability asset management variable report filtering.

3.1.4.5.5 Supply reference IDs from vulnerability databases including NVD and CVE.

3.1.4.5.6 Support the following report formats: HTML, PDF, CSV, or XML.

3.1.4.6 EVMS must adhere to the following integration requirements:

3.1.4.6.1 Support integration with the patch management solutions, System Center Configuration Manager (SCCM) and Windows Server Update Services (WSUS).

3.1.4.6.2 Support bi-directional API. API usage shall not require additional fees.

3.1.4.6.3 Support integration with virtual environments, to include tracking virtual assets that may have a shared IP address and/or MAC address.

3.1.4.7 The Vendor must provide EVMS support and maintenance for troubleshooting and errors as part of the licensed service.

3.1.4.7.1 Support and maintenance must be provided to include escalation, and multilevel support services. Support response time of four (4) hours or less is required.

3.1.4.7.2 Support and maintenance must be available Monday – Friday, from 8AM – 5PM EST.

3.1.4.8 For any components of this system that use SaaS or cloud services, the vendor must adhere to the following requirements:

3.1.4.8.1 Meet or exceed all applicable controls of NIST Special Publication 800-53, Rev 4, for a moderate/moderate/moderate categorized information system.

3.1.4.8.2 Provide strict data protection to all data transmitted, processed, and stored in the service, to include, at a minimum, data-in-transit and data-at-rest encryption.

3.1.4.8.3 The cloud environment (primary and redundant sites) must reside in the continental United States.

3.1.4.8.4 Agree to provide a cloud exit plan detailing the functionality, capability, and support to extract all stored data from the service in a non-proprietary format. The cloud lock-in protection cannot include additional fees or charges for data extraction.

3.1.4.8.5 Agree to include the method(s) of data destruction and how validation of data destruction will be provided to the State in the cloud exit plan.

3.1.4.8.6 Be willing to participate in a vendor assurance program, which can include, but not limited to, providing FedRAMP or Cloud Security Alliance documentation, for security and privacy protection validation.

3.1.4.9 The vendor must recognize the State as the data owner for all data transmitted, processed, and stored in the service. As such, the data cannot be shared or utilized in any manner by the vendor without prior written approval.

3.1.5 Central Management Appliance

3.1.5.1 The vendor will provide the central management appliance hardware to be physically installed by the State, but configured by the Vendor – in accordance with all State security procedures – with the following requirements:

3.1.5.1.1 The specifications of the appliance must be aligned with the size of an environment of 25,000+ assets.

3.1.5.1.2 The appliance must include all standard data connection and power cables.

3.1.5.1.3 The appliance must include, at minimum, a 3-year warranty.

3.1.5.1.4 The vendor must provide a knowledge transfer concerning implementation, configuration, recommended maintenance actions, and troubleshooting guidance concerning the appliance.

3.1.6 System Deployment

3.1.6.1 Required Installation and Configuration support services will consist of a support engagement for conducting initial configuration and implementation support functions. The support engagement can be conducted in-person or remotely, leveraging voice, email and teleconference communication methods.

3.1.6.2 A Statement of Work (SOW) between the State and the Vendor will be drafted and agreed upon after the Contract is awarded. At a minimum, the SOW will address how the system will be initiated and configured for full operation, and support requirements that:

3.1.6.2.1 Provide the deliverable of a deployment project plan designed to ensure a sound architecture of the system.

3.1.6.2.2 Provide technical support during the deployment and initial configuration of the system.

3.1.6.2.3 Provide the deliverables of all documentation pertaining to the service to include installation, operation, maintenance, troubleshooting and support manuals.

3.1.6.3 Training Services.

3.1.6.3.1 Provide two (2) training seats for application administration, configuration, & operations training. The training can be a single course or multiple courses, but must encompass both basic and advanced functionality of the application. The training must be a live training environment, but can be web-delivered and each training seat can be scheduled independently.

3.1.7 Notice to Proceed will be issued via Change Order upon System Acceptance, thereby activating the license service period and appliance warranty. System Acceptance will be provided after a successful test of the service for no less than 30 days. Once Change Order has been issued, the State will pay the Vendor for the first year's value of this contract.

3.1.8 Vendor should include, as part of its bid, pricing for optional renewal years 2, 3, and 4 for maintenance and support of system. The contract will be awarded on the initial year's cost only.

4 CONTRACT AWARD:

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

4.2 Pricing Page: Vendor should enter the unit cost for each line item in wvOASIS. Quantities have been provided and Vendors must provide their best lump sum price for each line item. Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

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

5 PAYMENT:

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

6 DELIVERY AND RETURN:

6.1 Shipment and Delivery: Vendor shall ship the Contract Items immediately after being awarded this Contract and receiving a purchase order or notice to proceed. Vendor shall deliver the Contract Items within the timeframe specified in the SOW. Contract Items must be delivered to Agency as specified on Purchase Order.

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

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

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

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

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

7 VENDOR DEFAULT:

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

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

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

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

7.1.4 Failure to remedy deficient performance upon request.

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

7.2.1 Immediate cancellation of the Contract.

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

7.2.3 Any other remedies available in law or equity.

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

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

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

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

DEFINITIONS:

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

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

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

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

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: Tenable Public Sector LLC

Authorized Signature: ______________________ Date: 5/10/18

State of Maryland

County of Howard, to-wit:

Taken, subscribed, and sworn to before me this 10th day of May, 2018.

My Commission expires May 31, 2021.

AFFIX SEAL HERE

NOTARY PUBLIC Kelly K

KELLY KALINOWSKI
Notary Public
Anne Arundel County
Maryland
My Commission Expires May 31, 2021

WV-10
Approved / Revised
09/15/17

State of West Virginia

VENDOR PREFERENCE CERTIFICATE

Certification and application is hereby made for Preference in accordance with ***West Virginia Code***, §5A-3-37. (Does not apply to construction contracts). ***West Virginia Code***, §5A-3-37, provides an opportunity for qualifying vendors to request (at the time of bid) preference for their residency status. Such preference is an evaluation method only and will be applied only to the cost bid in accordance with the ***West Virginia Code***. This certificate for application is to be used to request such preference. The Purchasing Division will make the determination of the Vendor Preference, if applicable.

1. □ **Application is made for 2.5% vendor preference for the reason checked:**
Bidder is an individual resident vendor and has resided continuously in West Virginia, or bidder is a partnership, association or corporation resident vendor and has maintained its headquarters or principal place of business continuously in West Virginia, for four (4) years immediately preceding the date of this certification; **or,**

□ Bidder is a resident vendor partnership, association, or corporation with at least eighty percent of ownership interest of bidder held by another entity that meets the applicable four year residency requirement; **or,**

□ Bidder is a nonresident vendor which has an affiliate or subsidiary which employs a minimum of one hundred state residents and which has maintained its headquarters or principal place of business within West Virginia continuously for the four (4) years immediately preceding the date of this certification; **or,**

2. □ **Application is made for 2.5% vendor preference for the reason checked:**
Bidder is a resident vendor who certifies that, during the life of the contract, on average at least 75% of the employees working on the project being bid are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or,**

3. □ **Application is made for 2.5% vendor preference for the reason checked:**
Bidder is a nonresident vendor that employs a minimum of one hundred state residents, or a nonresident vendor which has an affiliate or subsidiary which maintains its headquarters or principal place of business within West Virginia and employs a minimum of one hundred state residents, and for purposes of producing or distributing the commodities or completing the project which is the subject of the bidder's bid and continuously over the entire term of the project, on average at least seventy-five percent of the bidder's employees or the bidder's affiliate's or subsidiary's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years and the vendor's bid; **or,**

4. □ **Application is made for 5% vendor preference for the reason checked:**
Bidder meets either the requirement of both subdivisions (1) and (2) or subdivision (1) and (3) as stated above; **or,**

5. □ **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**
Bidder is an individual resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard and has resided in West Virginia continuously for the four years immediately preceding the date on which the bid is submitted; **or,**

6. □ **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**
Bidder is a resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard, if, for purposes of producing or distributing the commodities or completing the project which is the subject of the vendor's bid and continuously over the entire term of the project, on average at least seventy-five percent of the vendor's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years.

7. **Application is made for preference as a non-resident small, women- and minority-owned business, in accordance with *West Virginia Code* §5A-3-59 and *West Virginia Code of State Rules.***
□ Bidder has been or expects to be approved prior to contract award by the Purchasing Division as a certified small, women- and minority-owned business.

Bidder understands if the Secretary of Revenue determines that a Bidder receiving preference has failed to continue to meet the requirements for such preference, the Secretary may order the Director of Purchasing to: (a) rescind the contract or purchase order; or (b) assess a penalty against such Bidder in an amount not to exceed 5% of the bid amount and that such penalty will be paid to the contracting agency or deducted from any unpaid balance on the contract or purchase order.

By submission of this certificate, Bidder agrees to disclose any reasonably requested information to the Purchasing Division and authorizes the Department of Revenue to disclose to the Director of Purchasing appropriate information verifying that Bidder has paid the required business taxes, provided that such information does not contain the amounts of taxes paid nor any other information deemed by the Tax Commissioner to be confidential.

Bidder hereby certifies that this certificate is true and accurate in all respects; and that if a contract is issued to Bidder and if anything contained within this certificate changes during the term of the contract, Bidder will notify the Purchasing Division in writing immediately.

Bidder: Tenable Public Sector LLC

Signed:

Date: May 10, 2018

Title: President

**Check any combination of preference consideration(s) indicated above, which you are entitled to receive.*

West Virginia Ethics Commission

Disclosure of Interested Parties to Contracts

Pursuant to *W. Va. Code* § 6D-1-2, a state agency may not enter into a contract, or a series of related contracts, that has/have an actual or estimated value of $100,000 or more until the business entity submits to the contracting state agency a Disclosure of Interested Parties to the applicable contract. In addition, the business entity awarded a contract is obligated to submit a supplemental Disclosure of Interested Parties reflecting any new or differing interested parties to the contract within 30 days following the completion or termination of the applicable contract.

For purposes of complying with these requirements, the following definitions apply:

"Business entity" means any entity recognized by law through which business is conducted, including a sole proprietorship, partnership or corporation.

"Interested party" or *"Interested parties"* means:

(1) A business entity performing work or service pursuant to, or in furtherance of, the applicable contract, including specifically sub-contractors;
(2) the person(s) who have an ownership interest equal to or greater than 25% in the business entity performing work or service pursuant to, or in furtherance of, the applicable contract. (This subdivision does not apply to a publicly traded company); and
(3) the person or business entity, if any, that served as a compensated broker or intermediary to actively facilitate the applicable contract or negotiated the terms of the applicable contract with the state agency. (This subdivision does not apply to persons or business entities performing legal services related to the negotiation or drafting of the applicable contract.)

"State agency" means a board, commission, office, department or other agency in the executive, judicial or legislative branch of state government, including publicly funded institutions of higher education: Provided, that for purposes of W. Va. Code § 6D-1-2, the West Virginia Investment Management Board shall not be deemed a state agency nor subject to the requirements of that provision.

The contracting business entity must complete this form and submit it to the contracting state agency prior to contract award and to complete another form within 30 days of contract completion or termination.

This form was created by the State of West Virginia Ethics Commission, 210 Brooks Street, Suite 300, Charleston, WV 25301-1804. Telephone: (304)558-0664; fax: (304)558-2169; e-mail: ethics@wv.gov; website: www.ethics.wv.gov.

Revised October 7, 2017

West Virginia Ethics Commission

Disclosure of Interested Parties to Contracts

(Required by *W. Va. Code* § 6D-1-2)

Contracting Business Entity: Tenable Public Sector LLC **Address:** 7201 Columbia Gateway Drive
Suite 500

Authorized Agent: ____________ **Address:** Columbia, MD 21046

Contract Number: CRFQ 0210 ISC1800000013 **Contract Description:** EVMS

Governmental agency awarding contract: West Virginia Office of Technology (WVOT)

□ **Check here if this is a Supplemental Disclosure**

List the Names of Interested Parties to the contract which are known or reasonably anticipated by the contracting business entity for each category below *(attach additional pages if necessary)*:

1. **Subcontractors or other entities performing work or service under the Contract**

   □ Check here if none, otherwise list entity/individual names below.

2. **Any person or entity who owns 25% or more of contracting entity (not applicable to publicly traded entities)**

   □ Check here if none, otherwise list entity/individual names below.

3. **Any person or entity that facilitated, or negotiated the terms of, the applicable contract (excluding legal services related to the negotiation or drafting of the applicable contract)**

   □ Check here if none, otherwise list entity/individual names below.

Signature: ____________ Date Signed: May 10, 2018

Notary Verification

State of Maryland, County of Howard:

I, John C. Huffard Jr, the authorized agent of the contracting business entity listed above, being duly sworn, acknowledge that the Disclosure herein is being made under oath and under the penalty of perjury.

Taken, sworn to and subscribed before me this 10th day of May, 2018

Kelly K

Notary Public's Signature

KELLY KALINOWSKI
Notary Public
Anne Arundel County
Maryland
My Commission Expires May 31, 2021

To be completed by State Agency:

Date Received by State Agency: ____________

Date submitted to Ethics Commission: ____________

Governmental agency submitting Disclosure: ____________

State of West Virginia

Supplemental Information for CRFQ 0210 ISC1800000013

In response to 3.1.1 Specific Validation:
Services / Application Capabilities and Features Documentation

May 10, 2018

Submitted By:

Stan Sharrow | Territory Sales Manager
Tenable, Inc.
ssharrow@tenable.com
C: 412 527-2193
www.tenable.com

Confidential and Proprietary
Please note, this offer, which incorporates Tenable's Subscription Agreement, including software usage terms and conditions, supersedes all other prior or contemporaneous communications between the parties (whether written or oral) relating to Tenable's response to this proposal/tender. In the event a customer chooses to make an award based upon Tenable's response herein, only the terms of the Subscription Agreement, as negotiated by the Parties at the time of award, shall govern the license of software from Tenable to the customer. The terms contained in this RFP shall not apply to Tenable's offer, nor to any subsequent award or license. Copies of Tenable's software license agreements can be viewed at: http://static.tenable.com/prod_docs/tenable_slas.html

Table of Contents

Introduction

Organizations have more security products than ever, yet the frequency and severity of cyberattacks keeps growing. Multiple security approaches solve specific challenges, but can lead to gaps in defensive coverage. These gaps expose organizations to data breaches and fail to detect hidden threats and vulnerabilities, while giving those inside the organization a false sense that they are fully protected.

Cybersecurity is one of the existential threats of our time. New types of connected devices and compute platforms, from Cloud to IoT, have exploded the cyber attack surface. And more tools collecting more data doesn't equate to actionable insight for the CISO, C-suite and Board of Directors. The old way of simply scanning on-premises IT devices for vulnerabilities is no longer enough. It's time for a new approach.

Today, 24,000 organizations around the world rely on Tenable to help them understand and reduce cybersecurity risk. Our goal is to arm every organization, no matter how large or small, with the visibility and insight to answer three critical questions at all times: ***Where are we exposed? To what extent are we exposed? Where should we focus to reduce our exposure?***

As the creator of Nessus®, we've spent years deeply understanding assets, networks and vulnerabilities. We continually build this expertise and knowledge into our technology, so when we get smarter, you get smarter.

For this response, we feel our SecurityCenter product will meet your network vulnerability management needs. SecurityCenter® is the next-generation vulnerability analytics solution that includes multiple Nessus scanners, the world's most widely deployed vulnerability scanner. It provides the most comprehensive visibility into the security posture of their distributed and complex IT infrastructure.

SecurityCenter consolidates and evaluates vulnerability data across the enterprise, prioritizing security risks and providing a clear view of your security posture. With SecurityCenter, get the visibility and context you need to effectively prioritize and remediate vulnerabilities, ensure compliance with IT security frameworks, standards and regulations, and take decisive action to ensure the effectiveness of your IT security program and reduce business risk. SecurityCenter includes functionality from Nessus as well as the following additional capabilities:

- Measure security assurance and the effectiveness of your security investments using Tenable exclusive Assurance Report Cards® (ARCs)
- Use customizable dashboards, reports and workflows to quickly identify and rapidly respond to security incidents
- Communicate consolidated metrics to business executives and other IT security stakeholders
- View vulnerability management and security assurance trends across systems, services and geographies
- Group and control team member permissions by role
- Use advanced analytics with actionable information and trending to prioritize events and alerts

Tenable Strengths/Differentiators

Nessus Experience and Customer Base. Since 1998, Nessus has been the de facto vulnerability assessment standard. Tenable also has the largest install base with more than one million users and more than 20,000 customers worldwide. Organizations trust Tenable for proven security innovation.

Widest Coverage for Vulnerabilities, Compliance Regulations. Tenable consistently delivers more plug-ins/CVE coverage, SCADA and coverage of Unix and Linux variations, and it ensures compliance with more regulations than any other vendor.

Eliminate Blind Spots. Passively monitor network traffic to take an inventory of all assets communicating, and identify activity associated with breaches.

Correlation of Vulnerabilities to Exploits. Tenable automatically shows exploitability information from more than five sources.

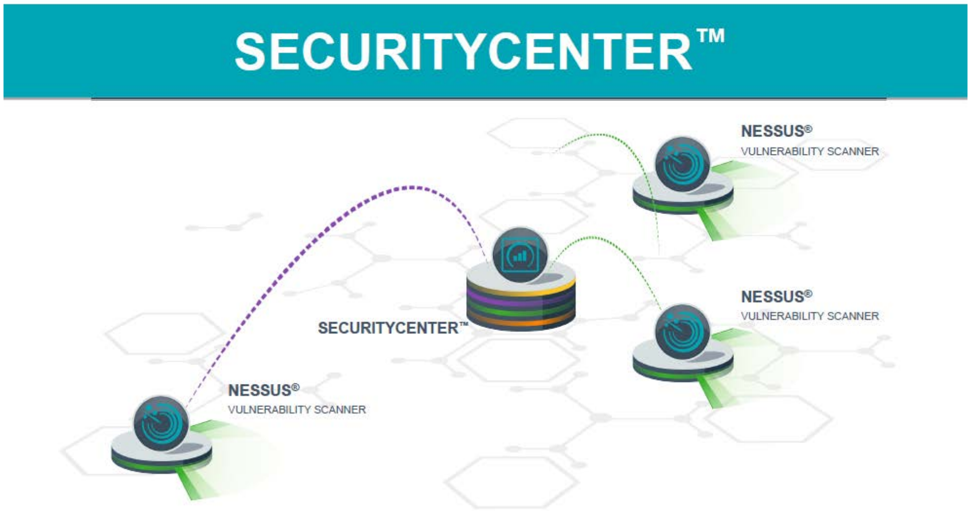
Continuous Monitoring Across Environments. Tenable monitors across the most environments, providing a unified view across virtualized systems, cloud environments, and mobile devices, including integration with Mobile Device Management (MDM) solutions.

Dynamic Threat Intelligence. Tenable incorporates multiple high-quality commercial sources of threat intelligence which continually assess threats across monitored environments,

Policy-Based Assurance. Gain a comprehensive view across hosts, users, and network traffic. Assurance Report Cards combine this in a customizable dashboard tailored to an organization's policy.

Proposed Solution: SecurityCenter ™

SecurityCenter® consolidates and evaluates vulnerability data across your organization, prioritizing security risks and providing a clear view of your security posture. With SecurityCenter's pre-built, highly customizable dashboards and reports, and the industry's only Assurance Report Cards® (ARCs), you can visualize, measure and analyze the effectiveness of your security program.


SECURITYCENTER™
NESSUS® VULNERABILITY SCANNER
NESSUS® VULNERABILITY SCANNER
SECURITYCENTER™
NESSUS® VULNERABILITY SCANNER

SecurityCenter Product Features

Advanced Analytics

Consolidate and analyze all vulnerability data gathered from multiple Nessus® scanners distributed across your enterprise. Use Assurance Report Cards (ARCs) to measure, analyze and visualize your security program and evaluate program effectiveness.

Reporting and Dashboards

Leverage pre-built, highly customizable HTML5-based dashboards and reports. Quickly give CISOs, security managers, analysts and practitioners the visibility and context they need to take decisive action to reduce exposure and risk.

Alerts and Notifications

Utilize customizable alerts, notifications and actions to enable rapid response. Quickly alert administrators to high-priority security events, speed up incident response and vulnerability remediation, and reduce overall risk.

Asset Grouping and Assessment

Dynamically group assets based on policies to obtain a near real-time view into overall risk when new vulnerabilities are discovered. Speed mitigation by identifying how many assets are affected by new vulnerabilities in minutes instead

Compliance

Use pre-defined checks against industry standards and regulatory mandates, such as CIS benchmarks, DISA STIG, FISMA, PCI DSS, HIPAA/HITECH, SCAP and more. Get the visibility and context you need to

Integrations

Utilize intelligent connectors to integrate with leading solutions in patch management, mobile device management, threat intelligence, cloud and more. Integrations leverage existing security investments to provide of days, and easily see remediation progress.

easily demonstrate adherence to multiple compliance initiatives.

additional data and improve visibility, context and analysis.

Distribution Model

Tenable does not sell direct, our distribution model is based on an indirect (2 tier) model, partnering with resellers.

Tenable has an extensive global network of certified resellers and distributors that combine local presence with deep cybersecurity experience to serve customers effectively.

At Tenable, we're committed to collaborating with leading security technology resellers and distributors worldwide. The Tenable Assure Partner Program rewards the investment our resellers make in expertise and customers, while helping our partners build a predictable annuity stream of renewals. Together, we are committed to protecting organizations of all sizes with industry-leading solutions designed to understand and reduce their cyber risk. Tenable's list of authorized partners can be found here: http://www.tenable.com/partners/find-a-reseller

General Requirements

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

3.1.1 Specification Validation: Vendor must provide service/application capabilities and features documentation. This documentation is preferred with the bid but must be submitted upon request.

Confirmed.

See link below:

https://docs.tenable.com/SecurityCenter.htm

3.1.2 The Enterprise Vulnerability Management System (EVMS) must provide full-feature vulnerability management capabilities to include, but not limited to, the specifications outlined below.

Confirmed to all, except those regarding appliance outlined in Section 3.1.5, Central Management Appliance. CDW will be supply the hardware

3.1.3 The State will operationally utilize the EVMS application. The EVMS will not be provided as a managed service. The State will hold responsibility for leveraging the application to carry out vulnerability management activities.

Confirmed.

3.1.4 Enterprise Vulnerability Management System

3.1.4.1 Enterprise Vulnerability Management System (EVMS) must adhere to the following architecture, performance, scalability and licensing functionality requirements:

3.1.4.1.1 The license must provide full functionality of the service for up to 25,000 individual hosts. The 25,000 does not apply to inactive IP addresses.

Confirmed. SecurityCenter is extremely scalable with no technical limit to the number of scanners per console. Our pricing model is; the more product you purchase the less per unit the cost is.

Each management console can manage hundreds of scanners which can each scan "tens of thousands" of hosts depending on system resources and other limits such as network performance and time requirements. A single instance of SecurityCenter can scale to hundreds of thousands of IPs. There is no additional cost of additional nessus scanners, you can deploy as many as needed with zero additional costs.

SecurityCenter counts every scanned IP against the license. If an IP is no longer used it will eventually age out and free up a license. When the license limit is reaching capacity or has been exceeded, SecurityCenter generates a warning in the web interface.

Note: Offline repositories are not counted against the IP license count.

3.1.4.1.2 The license must provide capability to select which hosts are covered by the service, irrespective of network or subnet.

Confirmed. SecurityCenter allows policies to be created/tuned then the scan jobs that use those policies can specify which credentials are to be used with which targets.

3.1.4.1.3 The license must include discovery scanning (device enumeration) for an unlimited number of internal network IP addresses.

Confirmed. Tenable's Host Discovery scans can be run on an unlimited number of IP addresses and there will be no license count incurred. The Host Discovery scans only use plugins that are not counted towards the license. These plugins are documented in these knowledge articles.

Relevant Articles:

- https://community.tenable.com/s/article/Which-Plugin-IDs-are-ignored-by-SecurityCenter-when-considering-the-total-IP-count-for-licensing?
- https://www.tenable.com/blog/unlimited-discovery-scanning-with-securitycenter-and-nessus

3.1.4.1.4 The license must include internal and external scanner device license(s) at no additional cost.

SecurityCenter provides flexible licensing of scanner deployment with the ability to deploy additional scanners at no additional cost.

External Scanning can be done in one of three ways:

1. SecurityCenter has a web-based template, which can be modified to do specific web scanning.
2. Run Tenable.io as a stand-alone solution for external and internal scanning, data is stored on the cloud.
3. Combine the power of Tenable.io with the flexibility of SecurityCenter, where nearly all data can be configured to be stored on premise.

For the purposes of this proposal, we are presenting Option 3. Tenable's SecurityCenter and Tenable.io products can run in tandem with one another to provide a comprehensive view of your internal and external assets, managed all within a single console. This cohesive relationship can minimize your CyberExposure gap in one streamlined approach.

3.1.4.1.5 Minimum supported platforms for scanner hosts must include: Windows operating system, Linux operating system, virtual environments such as VMWare, Azure, Hyper-V, etc.

SecurityCenter (on premise) is available for 64-bit versions of Red Hat Enterprise Linux 5, 6, 7. 64-bit versions of CentOS 5, 6, and 7 are also officially supported. SecurityCenter can also be run on a Tenable Virtual Appliance (VMware, Hyper-V).

Nessus scanners (on premise or in private cloud: Azure, AWS, etc.) support Mac, Linux, and Windows operating systems

More detail can be found within the Hardware / Software list found at: https://docs.tenable.com/generalrequirements/Content/PDF/TenableGeneralRequirements.pdf

3.1.4.1.6 Must include internal network scanning $_{111}$ a distributed environment across multiple subnets.

Yes. Tenable's solutions support internal and external scanning. Scans can be scheduled to run automatically or performed on demand and then can report their findings back to the system's management console, which offers customers a single global view of your internal and external network scan results. Using these features enables users to scan a wide range of environment be it internal, external, cloud and wireless. Tenable's Nessus scanners can be distributed across the network and remotely to collect data to be reported back to the management console.

3.1.4.1.7 Must include multiple deployment options to include: agent- based, agentless, internal network scans and external network scan capabilities.

Confirmed.

3.1.4.2 EVMS must adhere to the following risk and remediation management requirements:

3.1.4.2.1 Must include an advanced risk scoring algorithm.

Yes. SecurityCenter supports CVSS 1, CVSS 2, and Nessus supports CVSS 3. Temporal, Vector and Base score. The scores of the all vulnerabilities on a host are combined to calculate the risk of each host.

3.1.4.2.2 Risk scoring must be based on CVSS scoring, asset exploitability and susceptibility to known malware kits.

Yes.

The severity of a vulnerability is defined using the Common Vulnerability Scoring System (CVSS) base score. The CVSS is a method to define and characterize the severity of a vulnerability. Vulnerabilities are scored on a scale of 1 to 10, with a CVSS base score of 10 considered to be the most severe. Vulnerabilities with a CVSS base score of 10 are defined as ”critical.” In addition to specifying the severity of a vulnerability, industry sources are checked to determine if a publically-known exploit for the vulnerability exists. These critical and exploitable vulnerabilities create gaps in the network's integrity, which attackers can take advantage of to gain access to the network. Once inside the network, an attacker can perform malicious attacks, steal sensitive data, and cause significant damage to critical systems. By identifying the most severe vulnerabilities, analysts and security teams can better focus patch management efforts and better protect the network.

3.1.4.2.3 Risk scoring must integrate organization determined variables, such as asset criticality (critical business assets).

Critical assets can be defined using asset groups and then dashboards, reports and assurance report cards can be focus on those critical assets to help with prioritization.

3.1.4.2.4 Capable of both quantitative and qualitative metrics.

Vulnerability checks are assigned a Qualitative rating of Critical, High, Medium, Low and Informational. Extensive reporting and dash-boarding component types allow for Quantitative metrics such as counts or percentages. Assurance Report cards allow for the definition of "SMART" style goals, aligned to business statements with pass/fail, percentage or count reporting.

3.1.4.2.5 Able to provide remediation information to include: engineer level instructions and cross linking to external database for patches, downloads, and references.

SecurityCenter provides remediation views that are automatically prioritized and streamlined for the IT audience.

enable's remediation report offers detailed information on the top discovered vulnerabilities, and lists the affected hosts tracked within SecurityCenter. This report also contains steps to mitigate the risk of the vulnerabilities, including resources from CVE, BID, and vendor knowledge base articles. Additionally, this report indicates if the vulnerability is exploitable and by which exploit platform. The report includes executive summary, active vulnerability remediation plan, passive vulnerability remediation plan, and a compliance check remediation plan.

It is up to your operations team to implement the remediation plan based on the recommendations provided within, this software does not do the actual patching. Once done, SecurityCenter can track and trend remediation efforts.

3.1.4.2.6 *Support identification and management of vulnerability exceptions, to include an approval workflow.*

Yes. SecurityCenter provides a workflow to accept or recast risk of vulnerabilities. The exception can be applied to all assets, a group of assets or a single host:

- Accept Risks - Allows user to accept risks for vulnerabilities, which removes them from the default view for analysis, dashboards, and reports.
- Recast Risks - Allows user to change the severity for vulnerabilities.

3.1.4.3 *EVMS must adhere to the following management requirements:*

3.1.4.3.1 *Include the following asset management functions: asset grouping, asset import, asset categorization, asset definition, and dynamic & static tagging.*

Asset groupings can be easily imported, modified or deleted within the UI. Other methods of asset grouping and management includes Dynamic Grouping of Assets which automatically update according to defined filters, LDAP Query to automatically import computer groupings from a Directory Server and block lists or blackout windows for preventing assets from being scanned.

3.1.4.3.2 *Support data query based upon asset management functions.*

SecurityCenter consolidates and evaluates vulnerability data across the enterprise, prioritizing security risks and providing a clear view of your security posture. With SecurityCenter, get the visibility and context you need to effectively prioritize and remediate vulnerabilities, ensure compliance with IT security frameworks, standards, and regulations, and take decisive action to ensure the effectiveness of your IT security program and reduce business risk.

SecurityCenter enables you to continuously measure, analyze, and visualize the security and risk posture of your enterprise. SecurityCenter includes a HTML-based UI, which enables you to create highly customizable dashboards and reports to satisfy unique stakeholder needs, simplified workflows for faster trending and remediation, and new API's to make it easier to integrate with your existing IT processes and workflows.

SecurityCenter also includes the industry's first Assurance Report Cards (ARCs) that enable your Chief Information Security Officer (CISO) and security leaders to define the company's security program objectives in clear and concise terms, identify and close potential security gaps, and communicate effectiveness of your security investments to C-level executives and board members.

With SecurityCenter, all vulnerability information is presented in a single console. This provides an aggregated interface to view current, remediated, and trending vulnerability information through the use of dashboards, filters, searches, and reports - operated by authorized personnel via an efficient role based browser interface. Utilize customizable alerts, notifications and actions to enable rapid response. Quickly alert administrators to high-priority security events, speed up incident response and vulnerability remediation, and reduce overall risk.

3.1.4.3.3 Support role-based access control with both pre-defined and custom roles.

Security Center supports role-based access (RBAC) with both predefined and custom roles, with permissions being set by the CISO directly within the application. RBAC can be used to create different user roles to provide need-to-know separation of scan capability and the ability to view scan results for different groups, and also grant access on an Asset which can contain a single or multiple IP addresses and/or subnets. RBAC can also be used to restrict access to data contained within the system, which IP addresses can be scanned and what operations can be performed by a given user and/or group of users.

3.1.4.3.4 Support role-based access approval permissions to be assigned for vulnerability exclusions or exceptions.

SecurityCenter supports assigning tickets to individual users by providing an integrated ticketing system that can also send tickets to 3rd party systems. Alerts, tickets, requests and more are all configurable within the console through RBAC. SecurityCenter's internal ticketing system enables users to create tickets both manually or automatically by issuing an alert based on predefined set of conditions, which is fully customizable. In addition, The RBAC can be used to prevent some users from being able to accept or recast vulnerabilities.

3.1.4.3.5 Support credential management for authenticated scans.

SecurityCenter supports authenticated and non-authenticated scanning to be performed both for compliance/auditing and vulnerability management. Credentialed scans can utilize pre-defined ssh, windows, kerberos, Cyberark, snmp, database, and other IDs used to access IP devices remotely or locally for full access and accurate data based on the valid "admin or root" level credentials.

3.1.4.3.6 Support automatic and manual update options for both the EVMS and for vulnerability and configuration updates.

Our plugin and template feed is continuously updated, often on a daily basis, to ensure maximum protection for newly developed coverage. As information about new vulnerabilities are discovered and released into the public domain, Tenable's research staff designs detection programs. Typically, Tenable produces plugins for vulnerabilities within 24 hours of its public release. Manual updates can be initiated; application code updates require manual updating.

Plugin updates are automatically downloaded on a customizable schedule, typically once per day. There is also an offline update process the customer can initiate to download the plugins, and manually apply to the system which doesn't have internet access. Tenable uses an RSS feed to issue notifications, and SecurityCenter will also show the latest plugins. RSS feed available here: http://www.tenable.com/expert-resources/rss-feeds

3.1.4.3.7 Support workflow automation to include: scan scheduling, scan event and vulnerability alerts, and report generation and distribution.

SecurityCenter provides full automation of scanning, reporting, and alerting. SecurityCenter provides full automation of scheduled or ad-hoc scanning, reporting, and alerting. SecurityCenter allows a user to accept risk (make an exception) with configurable expiration dates of a detected vulnerability, or to recast risk (change severity levels) to a level other than what the vendor-defined for that vulnerability. SecurityCenter also has an alerting function within the workflow process which can email, distribute, or report on specific alerts or events.

3.1.4.4 EVMS must adhere to the following scanning requirements:

3.1.4.4.1 Capable of asset discovery/mapping scans, including operating system fingerprinting.

Yes, SecurityCenter supports asset discovery scans including operating system fingerprinting.

3.1.4.4.2 Capable of both unauthenticated and authenticated scans.

Yes, SecurityCenter supports authenticated and non-authenticated scanning.

3.1.4.4.3 Capable of configuration assessment scans in accordance with NIST Security Content Automation Protocol (SCAP).

SecurityCenter is NIST SCAP 1.2 Validated and supports the use of a dissolvable agent for SCAP auditing.

3.1.4.4.4 Capable of database configuration scans.

SecurityCenter provides auditing of databases for security and configuration settings. We can perform scans against the database management system software looking for vulnerabilities in the software as well as check for configuration compliance.

3.1.4.4.5 *Support DAST system scan data through native or import capabilities.*

Confirmed, DAST scanning is natively supported.

3.1.4.4.6 *Identify known exploits and malware kits associated with detected vulnerabilities.*

Yes. Detailed output is included with credentialed scans that identify specific versions of software and libraries with known vulnerabilities. The output lists the identified version and the version required to remediate the vulnerability.

For every exploitable vulnerability there is a section in the plugin output that identifies exploitability. That section describes the the known tools and/or malware that are able to exploit that vulnerability. The solution identifies whether or not the vulnerability has a publicly available exploit along a list of known tools and/or malware that are able to exploit that vulnerability.

3.1.4.4.7 *Include customizable, pre-configured scantemplates.*

Yes.
Tenable offers large number of templates are available out of the box at no additional charge, these templates can be customized in addition to providing a flexible template library for new and customized template versions. Our library of hundreds of templates , which is continually updated, include dashboards, reports, compliance audits and asset templates can be reviewed at https://www.tenable.com/sc-report-templates

3.1.4.4.8 *Include the ability to scan against a specificvulnerability.*

Yes. Out-of-the-box scan polices can be modified by customers. Scan policies are able to be customized using numerous variables. The Template section allows users to create scan policies based on industry standards. After selecting a policy template the user is presented with a configuration screen to configure settings unique to the network being scanned. This includes options such as web directories to scan, compliance audit files to use, credentials to use, and other scan options depending on the template selected.

Additionally, The Advanced Scan Add Policy option provides the ability to build a finely tuned scan policy utilizing all the available settings. The link below contains detailed descriptions of options available on each of the tabs displayed under the Advanced Scan Add Policy screen:
https://docs.tenable.com/sccv/5_5/Content/AddAScanPolicy.htm

3.1.4.4.9 *Include capability for scheduled scans, unsafe scan checks and scan blackout capabilities on a per-scan basis.*

Scan schedules are fully customizable by the customer, providing full automation of scheduled or ad-hoc scanning, reporting, and alerting. SecurityCenter also includes the ability to schedule scan blackout windows to prevent scanning during prohibited hours.

3.1.4.4.10 *Support a policy editor for custom configuration policy scans.*

SecurityCenter and its vulnerability policies are tailorable via the advanced custom option. All parameters are modified via a web interface. The compliance/auditing policies are standard html or text files, and can be modified with text editors such as wordpad, vi, nano, note++ etc.

3.1.4.4.11 *Provide a log or feedback mechanism m the event scan failure.*

The Scan Results page allows you to manage individual sets of scan results from active and agent scans (running, completed, or failed) run by SecurityCenter. By clicking on a scan you then can see the error details and status of the scan.

3.1.4.5 *EVMS must adhere to the following reporting requirements:*

3.1.4.5.1 *Capable of aggregated reporting, leveraging the data from multiple scan engines.*

With SecurityCenter, customers are able to deploy an unlimited number of scanners. Tenable supports a variety of scan engine platforms to include Windows, Linux, Mac OS, as well as virtual and hardware-based appliances. Tenable's Nessus scanners can be distributed across the network and remotely to collect data to be reported back to the management console. Tenable aggregates the results of individual scans into cumulative vulnerability views with filtering and analysis to allow drill-down and pivot capabilities.

Individual scans can be distributed across multiple scanners for load balancing. These distributed scan results are brought back into the management console and consolidated to provide a scan result of all the target systems.

Scanners can also be used to scan different sets of systems. These scan results are brought back into the management console where the individual scan results can be viewed. At the same time, the scan results are consolidated into the results database for the entire customer environment. In this way customers are able to see scan results for their entire environment and across all device types, as well as being able to dive into individual scan results and detailed data for particular hosts.

3.1.4.5.2 *Include pre-configured, customizable report templates to include compliance, risk prioritization and executive-level reports.*

Tenable offers over 400 templates and the list keeps growing, all of which are available out of the box at no additional charge. Templates can be customized in addition to providing a flexible template library for new and customized template versions. Our extensive library for each category noted in this question is too lengthy to list in this response, so please refer to: http://www.tenable.com/sc-report-templates

Some examples include:

- Executive reports in Tenable include the "Monthly Executive Report" which provides executive-level directors and managers with a detailed understanding of the vulnerability risk management program via a series of trend graphs, charts, tables, and other reporting components.
- Trending reports in Tenable include reports that show trends in the vulnerabilities and remediation efforts of the customer environment, as well as trend reports focused on vulnerabilities that are currently trending in popularity amongst attackers, like Shellshock, POODLE, and Heartbleed.
- Baseline reports in Tenable include our compliance and configuration reports, such as "Oracle Audit Results", "Microsoft SQL Server Audit Results", and the "Configuration Change Management Report" whose purpose is to establish configuration baselines, implement configuration management, and monitor for configuration changes. Configuration management and monitoring ensure systems start from known-good configuration states and that all changes are evaluated and approved.
- Vulnerability reports are common in Tenable, and include reporting vulnerabilities by hosts, by vulnerabilities, by particular manufacturer vulnerabilities, and by remediation instructions.

Reports by assets can be done in two ways. First, all reports can be generated to use only data for a specific group of assets. Second, reports can be generated to categorize the data within the reports by asset groups, allowing for comparisons between various asset groups. SecurityCenter provides customizable trending of scan results in reports using filtered results to define multiple trend lines in a single graph.

3.1.4.5.3 Capable of scheduled reports and report distribution within the system and via email.

Yes - All reports can be run in several different ways. These are scheduled, on demand, attached to an alert, and as part of the scanning process. These reports can be distributed to end users via email, reporting sites such as SharePoint, and exported via the API.

3.1.4.5.4 Support vulnerability asset management variable report filtering.

SecurityCenter allows the exclusion of vulnerabilities and assets from scans and reports by using different tools within the product suite. Filtering, asset groupings, tags, specific vulnerability plugins can be disabled to exclude from any customized scan policy and reporting data.

3.1.4.5.5 Supply reference IDs from vulnerability databases including NVD and CVE.

SecurityCenter reports on known weaknesses in a given target identified by security advisory organizations (e.g., Common Vulnerabilities and Exposures database (CVE) or the The Open Source Vulnerability Database (OSVDB) or the SecurityFocus Bugtraq (BID) or any combination of them).

3.1.4.5.6 Support the following report formats: HTML, PDF, CSV, or XML.

SecurityCenter standard report formats are RTF, PDF, and CSV. The report templates are in XML format - for copying, modifying or creating a custom report.

3.1.4.6 EVMS must adhere to the following integrationrequirements:

3.1.4.6.1 Support integration with the patch management solutions, System Center Configuration Manager (SCCM) and Windows Server Update Services (WSUS).

Confirmed. Patch management systems supported include Dell KACE; IBM Tivoli Endpoint Manager; Microsoft SCCM and WSUS, RedHat Satellite Server 5 and 6; Symantec Altiris.

3.1.4.6.2 Support bi-directional APL API usage shall not require additional fees.

Yes. SecurityCenter utilizes a RESTful API, and as such, the integration with other tools is extremely flexible at no additional charge. SecurityCenter's RESTful APIs are for developers who want to integrate SecurityCenter with other standalone or web applications, and administrators who want to script interactions with the SecurityCenter server. The API is designed to allow automation to solve the same business problems that are solved via UI interaction. There are no technical limitations in the software on rate and quantity of API usage.

3.1.4.6.3 Support integration with virtual environments, to include tracking virtual assets that may have a shared IP address and/or MAC address.

SecurityCenter tracks virtual assets and integrates with VMWare, Hyper-V, and other virtual environments.

3.1.4.7 The Vendor must provide EVMS support and maintenance for troubleshooting and errors as part of the licensed service.

The links below. The pricing provided is based on a Subscription Model. All standard level support, upgrades, templates, plugins, and patches are included as part of our software contract.

- Master License Agreement: http://static.tenable.com/prod_docs/Tenable_Master_Agreement_Template_v.1_(4.2018)_CLICK.pdf
- Technical Support Agreement: http://static.tenable.com/prod_docs/Technical_Support_Plans_v1.4-03092018_FINAL.pdf

3.1.4.7.1 Support and maintenance must be provided to include escalation, and multilevel support services. Support response time of four (4) hours or less is required.

Support is offered 24x7x365. Tenable's Response Time Objectives (RTO), as part of our standard technical support plan, are as follows:

P1-Critical: < 2 hr

P2-High: < 4 hr

P3-Normal: < 12 hr

P4-Low: < 24 hr

Please review the link below:

http://static.tenable.com/prod_docs/Tenable_Technical_Support_Plans.pdf

3.1.4.7.2 *Support and maintenance must be available Monday- Friday, from 8AM - 5PM EST.*

Tenable's Technical Support team is available 24 hours a day, 7 days a week, 365 days a year (24x7x365).

Phone support is available to named support contacts with Standard Support plans between 9am and 5pm, Monday through Friday, in the region where the product was purchased.

- Americas: 9:00am to 5:00pm EST
- EMEA: 9:00am to 5:00pm GMT
- APAC: 9:00am to 5:00pm SGT

3.1.4.8 *For any components of this system that use SaaS or cloud services, the vendor must adhere to the followingrequirements:*

3.1.4.8.1 *Meet or exceed all applicable controls of NIST Special Publication 800-53, Rev 4, for a moderate/moderate/moderate categorized information system.*

Tenable provides a role-based access control system designed to limit unauthorized access, modification, and deletion of audit data. These RBAC settings comply with NIST SP 800-53 requirements, where applicable to our product.

Control Enhancements:

(1) PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE MEDIA

The information system writes audit trails to hardware-enforced, write-once media. Supplemental Guidance: This control enhancement applies to the initial generation of audit trails (i.e., the collection of audit records that represents the audit information to be used for detection, analysis, and reporting purposes) and to the backup of those audit trails. The enhancement does not apply to the initial generation of audit records prior to being written to an audit trail. Write-once, read-many (WORM) media includes, for example, Compact DiskRecordable (CD-R) and Digital Video Disk-Recordable (DVD-R). In contrast, the use of switchable write-protection media such as on tape cartridges or Universal Serial Bus (USB) drives results in write-protected, but not write-once, media.

(2) PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS

The information system backs up audit records [Assignment: organization-defined frequency] onto a physically different system or system component than the system or component being audited. Supplemental Guidance: This control enhancement helps to ensure that a compromise of the information system being audited does not also result in a compromise of the audit records.

(3) PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION

The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools. Supplemental Guidance: Cryptographic mechanisms used for protecting the integrity of audit information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

(4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged users]. Supplemental Guidance: Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

(5) PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION The organization enforces dual authorization for [Selection (one or more): movement; deletion] of [Assignment: organization-defined audit information]. Supplemental Guidance: Organizations may choose different selection options for different types of audit information. Dual authorization mechanisms require the approval of two authorized individuals in order to execute. Dual authorization may also be known as twoperson control.

(6) PROTECTION OF AUDIT INFORMATION | READ ONLY ACCESS The organization authorizes read-only access to audit information to [Assignment: organizationdefined subset of privileged users]. Supplemental Guidance: Restricting privileged user authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users (e.g., deleting audit records to cover up malicious activity).

3.1.4.8.2 Provide strict data protection to all data transmitted, processed, and stored in the service, to include, at a minimum, data-in-transit and data-at-rest encryption.

Data generated by SecurityCenter is stored on-premise within the customer's architecture. Credentials are stored using AES-256 encryption; however other data that is stored locally in repositories is not encrypted at rest. Data in transit is encrypted using TLS v1.2 with a 4096-bit key.

3.1.4.8.3 The cloud environment (primary and redundant sites) must reside in the continental United States.

Not applicable to an on-premise solution.

3.1.4.8.4 Agree to provide a cloud exit plan detailing the functionality, capability, and support to extract all stored data from the service in a non-proprietary format. The cloud lock-in protection cannot include additional fees or charges for data extraction.

Agreed

3.1.4.8.5 Agree to include the method(s) of data destruction and how validation of data destruction will be provided to the State in the cloud exit plan.

Not applicable to an on-premise solution.

3.1.4.8.6 Be willing to participate in a vendor assurance program, which can include, but not limited to, providing FedRAMP or Cloud Security Alliance documentation, for security and privacy protection validation.

Tenable recently completed a Cloud Security Alliance (CSA) Star Self-Assessment, certification is pending. The assurance questionnaire can be downloaded directly from: https://cloudsecurityalliance.org/star-registrant/tenable-inc

3.1.4.9 The vendor must recognize the State as the data owner for all data transmitted, processed, and stored in the service. As such, the data cannot be shared or utilized in any manner by the vendor without prior written approval.

Yes, all data will reside on-premise within the State's infrastructure. Tenable cannot access or utlilize customer data in any way.

3.1.5 Central Management Appliance

3.1.5.1 The vendor will provide the central management appliance hardware to be physically installed by the State, but configured by the Vendor - in accordance with all State security procedures - with the following requirements:

3.1.5.1.1 The specifications of the appliance must be aligned with the size of an

environment of 25,000+ assets.

Confirmed

3.1.5.1.2 The appliance must include all standard data connection and power cables.

Confirmed

3.1.5.1.3 The appliance must include, at minimum, a 3-year warranty.

Confirmed

3.1.5.1.4 The vendor must provide a knowledge transfer concerning implementation, configuration, recommended maintenance actions, and troubleshooting guidance concerning the appliance.

Confirmed

3.1.6 System Deployment

3.1.6.1 Required Installation and Configuration support services will consist of a support engagement for conducting initial configuration and implementation support functions. The support engagement can be conducted in-person or remotely, leveraging voice, email and teleconference communication methods.

For this implementation plan, we propose our Quick-Start implementation program, which can be conducted remotely without any of the Tenable Staff needing to be onsite at your location.

Our QuickStart service is available to customers with under 25,000 IPs. This program speeds up your implementation to get you identifying vulnerabilities, actively managing risks and providing valuable insights quickly. Immediately improve your security posture and ensure you have a stable foundation for achieving and even expanding upon your vulnerability management objectives.

3.1.6.2 A Statement of Work (SOW) between the State and the Vendor will be drafted and agreed upon after the Contract is awarded. At a minimum, the SOW will address how the system will be initiated and configured for full operation, and support requirements that:

3.1.6.2.1 Provide the deliverable of a deployment project plan designed to ensure a sound architecture of the system.

Our professional services team will work with you to develop and deliver the following documentation and task-based deliverables.

Documentation Provided:

- Project plan
- Architecture diagram, including a high-level network topology with Tenable products, scan zones and repositories
- Configuration design specific to your deployment
- Vulnerability management operational plan

Tasks Completed:

- Install and configure one instance of SecurityCenter and up to four (4) Nessus scanners
- Produce up to three (3) standard scanning policies
- Produce up to four (4) of each of the following: static and dynamic asset lists, queries, dashboard views, reports and alerts

3.1.6.2.2 Provide technical support during the deployment and initial configuration of the system.

In a QuickStart for SecurityCenter, you'll work with a Tenable Certified Security Consultant from Tenable Professional Services. Typically we will work with one or more of your team members in the roles of system administrator, security analyst or infrastructure administrator.

We typically perform the approximately two-day engagement remotely, but it can be performed on-site, depending on what's most convenient for you. Our professional services team will advise you in advance of your engagement on how to prepare for your QuickStart service so that it goes smoothly and you get the most benefit from it.   When the service concludes, you'll receive key documentation to help you maintain your deployment and evolve your vulnerability management practice as new threats emerge.

3.1.6.2.3 Provide the deliverables of all documentation pertaining to the service to include installation, operation, maintenance, troubleshooting and support manuals.

The Tenable team will provide hands-on training, knowledge transfer and best-practices sharing as we work with you to complete the following key tasks:

- Create, initiate, validate and review scan results of up to three (3) standard scan policies, including a:
  - Discovery scan (non-credentialed)
  - Microsoft and/or Linux Unix Credentialed Security Checks scan
  - Audit or compliance scan selected from the CIS group of audit files
- Review scan results and create up to four (4) static and dynamic asset lists
- Create up to four (4) queries and understand how to fully use SecurityCenter query capabilities in creation of dashboards or reports
- Create up to four (4) dashboard views using dashboard templates or create a custom dashboard for which you create and add up to 4 dashboard components
- Create tables, components, pie charts, bar graphs and other tools to make the dashboard interface more useful for your stakeholders

- Create up to four (4) reports and layouts demonstrating the types of reports you can create based on queries, selected scan data or data from specific criteria
- Create customized reporting templates to show data in a way that is consumable by stakeholders
- Create up to four (4) alerts and demonstrate how to optimally use the various types of alert functions available in SecurityCenter

In addition to the deliverables mentioned in the response above, we provide user and administrator manuals online: https://docs.tenable.com/

3.1.6.3 Training Services.

3.1.6.3.1 Provide two (2) training seats for application administration, configuration, & operations training. The training can be a single course or multiple courses, but must encompass both basic and advanced functionality of the application. The training must be a live training environment, but can be web-delivered and each training seat can be scheduled independently.

Tenable's strategy around product training is to develop and deliver on-demand web-based training. Tenable provides an update to the training with every major release of the software. Leveraging Tenable's OnDemand product training (offered for free) will provide sufficient product knowledge. Tenable also offers virtual and customized onsite training at additional cost. These classes educate users on doing everything from installation and configuration to best practices in alerting and reporting.

Tenable offers training in one of three ways:

1. OnDemand - Self-guided online Courses that are free with subscription, available 24/7 (free, included as part of subscription)
2. Virtual - 2 day virtual classroom settings (additional cost)
3. Onsite - For up to 15 participants at a time (additional cost)

For the purposes of this response, we feel that Option #2 stated above, Virtual Training, is the best choice to meet your needs. This pricing will be included in our product quote.

3.1.7 Notice to Proceed will be issued via Change Order upon System Acceptance, thereby activating the license service period and appliance warranty. System Acceptance will be provided after a successful test of the service for no less than 30 days. Once Change Order has been issued, the State will pay the Vendor for the first year's value of this contract.

Tenable does not sell direct, our distribution model is based on an indirect (2 tier) model, partnering with resellers.

Tenable has an extensive global network of certified resellers and distributors that combine local presence with deep cybersecurity experience to serve customers effectively.

At Tenable, we’re committed to collaborating with leading security technology resellers and distributors worldwide. The Tenable Assure Partner Program rewards the investment our resellers make in expertise and customers, while helping our partners build a predictable annuity stream of renewals. Together, we are committed to protecting organizations of all sizes with industry-leading solutions designed to understand and reduce their cyber risk. Tenable's list of authorized partners can be found here: http://www.tenable.com/partners/find-a-reseller

3.1.8 Vendor should include, as part of its bid, pricing for optional renewal years 2, 3, and 4 for maintenance and support of system. The contract will be awarded on the initial year's cost only.

Our product licensing is a subscription-based model. Maintenance and Support are included as part of the subscription cost and will be offered as long as the subscription remains active. If WV chooses to purchase only 1 year, they will receive 1 year maintenance and support, with an option to renew at the end of the term.

Appendix

Tenable Master Services License Agreement (MSLA)

IMPORTANT

THIS AGREEMENT IS INTENDED TO BE LEGALLY BINDING. BY CLICKING THE "AGREE" OR "ACCEPT" BUTTON BELOW AND/OR CONTINUING TO DOWNLOAD, INSTALL OR USE TENABLE SOFTWARE AND OR SERVICES (OR AUTHORIZING/ALLOWING A THIRD PARTY TO DO SO ON YOUR BEHALF), YOU INDICATE:

(1) YOUR ACCEPTANCE OF THIS AGREEMENT;

(2) YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO BE LEGALLY BOUND BY THEM; AND

(3) YOU ARE AUTHORIZED TO BIND CUSTOMER TO THE TERMS OF THIS AGREEMENT.

****IF YOU DO NOT WISH TO ACCEPT THE TERMS OF THIS AGREEMENT OR ARE NOT AUTHORIZED TO DO SO PLEASE CLICK THE "REJECT" OR "DECLINE" OR OTHER SIMILAR BUTTON AND DO NOT PROCEED TO DOWNLOAD, INSTALL OR USE THIS PRODUCT.*

TENABLE MASTER AGREEMENT

This Master Agreement (this "Agreement") is between Tenable (as defined below), and you, the party licensing Software and/or receiving Services ("You" or "Customer") with an effective date as of the date You click to accept these terms (the "Effective Date"). Hereinafter each of Tenable and Customer may be referred to collectively as the "Parties" or individually as a "Party".

1. Definitions.

(a) "Affiliate" means any entity that controls, is controlled by, or is under common control with a Party. "Control" shall mean: (1) ownership (either directly or indirectly) of greater than fifty percent (50%) of the voting equity or other controlling equity of another entity; or (2) power of one entity to direct the management or policies of another entity, by contract or otherwise.

(b) "Documentation" means the then-current official user manuals and/or documentation for the Products available at docs.tenable.com.

(c) "Hosted Services" are a type of service offered through the Tenable.io (SaaS) platform and include Scans and access to and use of the hosted environment (the "Hosted Environment").

(d) "Product(s)" means any of the products that Tenable offers, including Software, Hosted Services, Support Services and Professional Services.

(e) "Professional Services" means services purchased, including consulting services which are relevant to the implementation and configurations of Tenable Products as well as on-site or virtual training courses. Generally, Professional Services are defined either in a separate SOW or a Services Brief. Professional Services do not include the Hosted Services or Support Services.

(f) "Scan(s)" are a function performed by the Software and/or the Hosted Services on Scan Targets, which are conducted in order to provide data to Customer regarding its network security. "PCI Scans" are a specific type of Scan designed to assess compliance with the Payment Card Industry Data Security Standard. "Scan Data" is the resulting information created by the Scan. "Scan Target(s)" are the targets or subjects of a Scan.

(g) "Services Brief" means the document which outlines Tenable's basic, pre-packaged, non-customized, installation, or training Professional Services offered under a Tenable SKU and which do not require a separate SOW. For the avoidance of doubt, Customer may purchase commercial off the shelf SKU-based Professional Services without executing a separate Statement of Work. A "SOW" or "Statement of Work" shall further describe Professional Services, the terms of which may be customized and which shall require execution by the Parties.

(h) "Software" means each software product made available by Tenable under this Agreement for download. Software includes patches, updates, improvements, additions, enhancements and other modifications or revised versions of the same that may be provided to Customer by Tenable from time to time.

(i) "Tenable" means: (i) Tenable, Inc., if Customer is a commercial entity or individual located in North or South America (Tenable, Inc. is a Delaware corporation having offices at 7021 Columbia Gateway Drive, Suite 500, Columbia, MD 21046); (ii) Tenable Public Sector LLC, if Customer is an agency or instrumentality of the United States Government, a commercial entity operating predominately as a federal systems integrator for eventual sale or resale or for the benefit of the United States Government, or an agency or instrumentality of a State or local government within the United States (Tenable Public Sector LLC is a Delaware limited liability company having offices at 7021 Columbia Gateway Drive, Suite 500, Columbia, MD 21046); or (iii) Tenable Network Security Ireland Limited, if Customer is located outside of North or South America (Tenable Network Security Ireland Limited is a private limited company having offices at 81b Campshires, Sir John Rogerson's Quay, Dublin 2, Ireland).

2. Orders and Transactions.

(a) Reseller Transactions. If Customer purchases Tenable Products through an authorized Tenable reseller (a "Reseller"), all terms related to pricing, billing, invoicing and payment ("Payment Terms") set forth in this Agreement (if any) shall not apply. For the avoidance of doubt, all such Payment Terms shall be as agreed to between Customer and Reseller. To place an order, Customer shall provide the Reseller with a purchase order (or other similar document acceptable to Reseller) in response to a valid quote from such Reseller. Following Reseller's receipt of such purchase order, Tenable shall issue a sales order confirmation or other similar order acceptance document (the "Ordering Document"). No order shall be deemed accepted by Tenable until Tenable issues the Ordering Document. The Ordering Document shall set forth all Products (and corresponding licensing metrics) purchased by Customer.

(b) Direct Transactions. If the Parties have agreed to transact directly, the following Payment Terms shall apply. Customer agrees to pay all amounts due as specified in a Tenable invoice. Fees for Hosted Services are charged for access to the Host Environment (as defined herein), not actual usage. Customer further agrees to pay for actual travel and living expenses for Professional Services where Tenable is conducting on-site work. Payment is due within thirty (30) days from the date of Tenable's invoice to Customer. Customer will pay directly or reimburse Tenable for any taxes (including, sales or excise taxes, value added taxes, gross receipt taxes, landing fees, import duties and the like), however designated and whether foreign or domestic, imposed on or arising out of this Agreement. Notwithstanding the foregoing, Tenable will be solely responsible for its income tax obligations and all employer reporting and payment obligations with respect to its personnel. Customer agrees to pay Tenable without deducting any present or future taxes, withholdings or other charges except those deductions it is legally required to make. If Customer is legally required to make any deductions or withholding, Customer agrees to provide evidence of such withholding upon request. If a certificate of exemption or similar document or proceeding is necessary in order to exempt any transaction from a tax, Customer shall provide such certificate or document to Tenable.

(c) Delivery and Installation. Delivery of Tenable Products ("Delivery") shall be deemed to occur on the date of availability for electronic download or electronic access. Tenable has no duty to provide installation services for Tenable Products unless installation services are purchased separately.

3. Term and Termination.

(a) Agreement Term. This Agreement shall commence upon the Effective Date and continue until terminated in accordance with the terms set forth herein.

(b) License Term and Renewals. The "License Term" is the term of the license or subscription for Products as set forth in the Ordering Document. If this Agreement has been signed by both Parties, then unless otherwise agreed to in writing, any renewal License Term shall be governed by the terms set forth herein. If this Agreement has been accepted via shrinkwrap or click-through, upon any renewal of the License Term, the terms then in effect, available at http://static.tenable.com/prod_docs/tenable_slas.html (or a successor location), will come into effect and govern the term of such renewal. Customer agrees that use of the Products at the time of such renewal will be deemed full and adequate acceptance of the updated terms.

(c) Termination for Cause. Either Party may terminate this Agreement for cause if the other Party materially breaches this Agreement provided that such breaching Party has received written notice of such breach and failed to cure such breach within thirty (30) days. If this Agreement is terminated for cause by either Party, Customer shall cease to use any Software or Hosted Services purchased hereunder and shall certify to Tenable that it has returned or destroyed all copies of the Software. If this Agreement is terminated for cause by Tenable, Customer shall remain responsible for any outstanding payment obligations throughout the rest of the License Term.

(d) Termination for Convenience. Customer may terminate this Agreement for any lawful reason upon ninety (90) days prior written notice to Tenable. If Customer terminates for convenience, Customer shall not receive a refund and shall remain obligated to pay for Products for which it has previously entered into a transaction as well as any additional payment obligations agreed upon prior to the termination date.

4. Products.

(a) Product-Specific Terms. Pursuant to this Agreement, Customer may receive the right to use various Products. Terms related to Customer's use of Software are described in **Schedule A** (*Software*). Terms related to Customer's use of Hosted Services are described in **Schedule B** (*Hosted Services*). Terms related to the provision of Professional Services are described in **Schedule C** (*Professional Services*). For each Product, Customer will have the right to use the corresponding Documentation.

(b) Licensing Model. Product licenses shall be in accordance with the terms of the applicable licensing model as set forth in the Documentation and the Ordering Document, which may include limitations on Scan Targets, License Term, the number of users, seats, licenses and/or types of modules licensed. Product licenses shall commence upon Delivery and shall be either perpetual or subscription in nature. If Customer exceeds the license restrictions, Customer must purchase an upgraded license to allow for all actual or additional usage.

(c) Restrictions on Use. Customer shall not directly or indirectly: (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive, obtain or modify the source code of the Products; (ii) reproduce, modify, translate or create derivative works of all or any part of the Products; (iii) remove, alter or obscure any proprietary notice, labels, or marks on the Products; (iv) without Tenable's prior written consent use the Products in a service bureau, application service provider or similar capacity; or (v) use the Products to gather information from Nessus Home scanners. Customer may not use the Products to manage or gather information from Scan Targets not owned or hosted by Customer.

(d) Intellectual Property in Products. This Agreement does not transfer to Customer any title to or any ownership right or interest in the Products. Any rights in the Products not expressly granted in this Agreement are reserved by Tenable. If Customer provides Tenable with any comments, suggestions, or other feedback regarding the Product, Customer hereby assigns to Tenable all right, title and interest in and to such feedback.

(e) Customer System Requirements. In order to use the Products, Customer must meet or exceed the specifications found in the Tenable General Requirements document, available at docs.tenable.com (or a successor location).

(f) Product Features. Tenable reserves the right to withdraw features from future versions of the Products provided that: (i) the core functionality of the affected Product remains the same; or (ii) Customer is offered access to a product or service providing materially similar functionality as the functionality removed from the affected Product. The preceding remedies under this Section 4(f) are the sole remedies available if Tenable withdraws features from the Products.

(g) Telemetry. Customer agrees to provide certain necessary Scan information, which may include the number of Scan Targets managed with the Product for billing purposes, behavioral attributes such as whether or not certain features in the Product are utilized, or other relevant information ("Technical Data"). Tenable may use Technical Data for reasonable business purposes, including product support, license validation and research and development. Tenable agrees to only disclose Technical Data which has been properly anonymized.

(h) Additional Details on Use Restrictions for Tenable Security Network Ireland Limited. The following shall only apply for transactions with Tenable Security Network Ireland Limited. Notwithstanding anything in Section 4(c), decompiling the Product is permitted to the extent the laws of Customer's jurisdiction give Customer the right to do so to obtain information necessary to render the Products interoperable with other software; provided, however, that Customer must first request such information from Tenable and Tenable may, in its discretion, either provide such information to Customer or impose reasonable conditions, including a reasonable fee, on such use of the Products to ensure that its proprietary rights in the Product are protected.

5. Support.

(a) Support Services. Tenable shall provide Customer with support services (the "Support Services") in accordance with Tenable's then-current Technical Support Plan and consistent with Tenable's Product Lifecycle Policy, each of which is available at http://static.tenable.com/prod_docs/tenable_slas.html (or a successor location). The Support Services include bug fixes, updates (including new vulnerability plug-ins), or enhancements that Tenable makes generally available to users of the Products. The Support Services also include the provision of new minor (Example: 1.1.x to 1.2.x, etc.) and major version releases of the Products (Example: 1.x to 2.x, etc.).

(b) Support Fees. Standard Support Services for Products licensed for a finite License Term will be provided at no additional charge beyond the license fee for the duration of the License Term. Support Services for Products licensed on a perpetual basis must be purchased separately in advance. In all cases, premium support may be purchased at an additional charge. If during the course of a perpetual license Customer terminates or fails to renew the Support Services, Customer may, at any time during the term of this Agreement, request that Tenable reinstate the Support Services provided that Customer pays for the lapsed Support Services in an amount equal to the total fees Customer would have paid for the Support Services between the time Customer's Support Services lapsed and the then-current date.

6. Confidentiality.

(a) Definition. "Confidential Information" means information learned or disclosed by a Party under this Agreement that should reasonably be assumed to be confidential or proprietary, including the Products and the terms of this Agreement. Confidential Information will remain the property of the disclosing Party, and the receiving Party will not be deemed by virtue of this Agreement or any access to the Confidential Information to have acquired any right, title or interest in or to the Confidential Information.

(b) Obligations. Each Party agrees to only use the Confidential Information in connection with this Agreement or a purchase hereunder. The receiving Party agrees to hold the disclosing Party's Confidential Information confidential and to use at least the same level of protection against unauthorized disclosure or use as the receiving Party normally uses to protect its own information of a similar character, but in no event, less than a reasonable degree of care. Each Party may share Confidential Information with its Affiliates or authorized contractors in the performance of its duties under this Agreement; provided, however, each Party shall be responsible to ensure that such Affiliate or authorized contractors are bound by obligations of confidentiality at least as stringent as those set forth in this Agreement.

(c) Exclusions. Confidential Information shall not include information that: (i) is already known to the receiving Party free of any confidentiality obligation; (ii) is or becomes publicly known through no wrongful act of the receiving Party; (iii) is rightfully received by the receiving Party from a third party without any restriction or confidentiality; or (iv) is independently developed by the receiving Party without reference to the Confidential Information. Furthermore, if Customer intentionally or unintentionally requests or performs scans on third party Scan Targets, Customer agrees that Tenable may provide all relevant information to the owner of the Scan Targets of such unlawful or impermissible scanning as well as to relevant legal authorities, and such disclosure shall not be considered a breach of confidentiality.

(d) Information Not to be Disclosed. The Parties agree not to disclose to each other any sensitive, non-public, personally identifiable information (such as social security numbers, personal credit card information or health care data, etc.) which may be the subject of any data privacy regulations as well as any Personal Data of an EU Data Subject as such terms are defined under the European Union General Data Protection Regulation (together, hereinafter, "PII"). Tenable does not require the transmission or processing of any such PII in order to perform its duties under this Agreement or sell any Products hereunder. If Customer inadvertently or unintentionally discloses any PII to Tenable, Customer shall identify to Tenable that it has disclosed PII and Tenable shall promptly return and/or destroy such PII.

(e) Legal Disclosures; Remedies. The receiving Party may disclose Confidential Information if required to do so by law provided the receiving Party shall promptly notify the disclosing Party so that the disclosing Party may seek any appropriate protective order and/or take any other action to prevent or limit such disclosure. If required hereunder, the receiving Party shall furnish only that portion of the Confidential Information disclosure of which is legally required. The receiving Party acknowledges and agrees that the breach of any term, covenant or provision of this Agreement may cause irreparable harm to the disclosing Party and, accordingly, upon the threatened or actual breach by the receiving Party of any term, covenant or provision of this Agreement, the disclosing Party shall be entitled to seek injunctive relief, together with any other remedy available at law or in equity. The receiving Party will notify the disclosing Party promptly of any unauthorized use or disclosure of the disclosing Party's Confidential Information.

7. Representations and Warranties; Disclaimer.

(a) Warranty of Authority. The Parties hereby represent and warrant that they have the full power and authority to enter into this Agreement.

(b) Products. Product warranties and associated warranty periods are set forth in the relevant Schedules.

(c) Antivirus Warranty. Tenable represents it has taken commercially reasonable efforts to ensure that the Products, at the time of Delivery, are free from any known and undisclosed virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design that would erase data or programming or otherwise cause the Products to become inoperable or incapable of being used in the manner for which it was designed or in accordance with the Documentation.

(d) Warranty Disclaimer. EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT AND TO THE GREATEST EXTENT PERMITTED BY LAW, TENABLE OFFERS ITS PRODUCTS "AS-IS" AND MAKES NO OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SECURITY, INTEGRATION, PERFORMANCE AND ACCURACY, AND ANY IMPLIED WARRANTIES ARISING FROM STATUTE, COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE. THE WARRANTIES SET FORTH IN THIS AGREEMENT

ARE MADE TO CUSTOMER FOR CUSTOMER'S BENEFIT ONLY. CUSTOMER'S USE OF THE PRODUCTS IS AT CUSTOMER'S OWN RISK. CUSTOMER UNDERSTANDS THAT ASSESSING NETWORK SECURITY IS A COMPLEX PROCEDURE, AND TENABLE DOES NOT GUARANTEE THAT THE RESULTS OF THE PRODUCTS WILL BE ERROR-FREE OR PROVIDE A COMPLETE AND ACCURATE PICTURE OF CUSTOMER'S SECURITY FLAWS, AND CUSTOMER AGREES NOT TO RELY SOLELY ON SUCH PRODUCTS IN DEVELOPING ITS SECURITY STRATEGY. CUSTOMER ACKNOWLEDGES THAT THE PRODUCTS MAY RESULT IN LOSS OF SERVICE OR HAVE OTHER IMPACTS TO NETWORKS, ASSETS OR COMPUTERS (INCLUDING MODIFICATION OF SCAN TARGETS), AND CUSTOMER IS SOLELY RESPONSIBLE FOR ANY DAMAGES RELATING TO SUCH LOSS OR IMPACT.

8. Limitation of Liability.

(a) Direct Damages. The cumulative liability of one Party to the other for all claims arising from or relating to the Products or this Agreement (including without limitation, any cause of action sounding in contract, tort or strict liability) shall be limited to proven direct damages in an amount not to exceed, in the aggregate, the fees paid by Customer to Tenable for the Products over the twelve (12) months immediately prior to the event giving rise to the claim.

(b) Indirect Damages. Neither Party shall be liable to the other for any indirect, incidental, special, punitive, consequential or exemplary damages regardless of the nature of the claim. This prohibition on indirect damages shall include, but not be limited to, claims based on lost profits, cost of delay, any failure of delivery, business interruption, cost of lost or damaged data, or liabilities to any third parties even if such Party is advised of the possibility thereof.

(c) Carve Outs. The liability caps set forth in Sections 8(a) and 8(b) shall not apply to damages resulting from:

(i) damage to real or personal property;
(ii) personal injury or death;
(iii) fraud or willful misconduct;
(iv) indemnification obligations set forth in Section 9 (*Indemnification*); or
(v) Customer's breach of Section 4(c) (*Restrictions on Use*).

(d) Limitations; Time Period. Each of the limitations set forth in this Section 8 shall be enforced to the fullest extent of the law. Any laws preventing such limitations shall only apply to the extent required by law and the remaining unaffected terms shall apply in full. Unless expressly prohibited by law, each Party shall have a period of no greater than twelve (12) months from the date the cause of action accrues to bring a claim against the other Party for such cause of action.

9. Indemnification.

(a) Indemnification Obligations.

(i) By Tenable. Tenable shall (at its sole cost and expense): (i) defend and/or settle on behalf of Customer (including Customer's officers, directors, employees, representatives and agents); and (ii) indemnify Customer for, any third party claims brought against Customer based upon a claim that Customer's use of the Products in accordance with this Agreement infringes or misappropriates such third party's intellectual property rights in a jurisdiction which is signatory to the Berne Convention.

(ii) By Customer. Customer shall (at its sole cost and expense): (i) defend and/or settle on behalf of Tenable (including Tenable's officers, directors, employees, representatives and agents) and (ii) indemnify Tenable for, any third party claims brought against Tenable arising out of or relating to Customer's use of the Products to perform Scans on third party Scan Targets, except to the extent that any such claim or action is caused by a failure of the Products to materially comply with the Documentation.

(b) In Case of Infringement. If Customer's use of the Products is, or in Tenable's opinion is likely to be, the subject of an infringement claim, Tenable may, in its sole discretion and expense: (i) modify or replace the infringing Products as necessary to avoid infringement, provided that the replacement Products are substantially similar in functionality; (ii) procure the right for Customer to continue using the infringing Products; or (iii) terminate this Agreement and, upon Customer's return or certified destruction of the infringing Product, provide Customer a pro-rata refund calculated as follows: (x) for infringing Products licensed on a subscription basis, the refund shall consist of any prepaid but unused fees for the remainder of the applicable License Term; or (y) for infringing Software licensed on a perpetual basis, the refund shall consist of a straight line depreciation of the license fee based on a three (3) year useful life. This Section 9 sets forth Tenable's sole and exclusive liability and Customer's sole and exclusive remedy with respect to any claim of intellectual property infringement.

(c) Exclusions. Tenable shall have no liability with respect to a third party intellectual property infringement claim arising out of: (i) modifications of the Product made to conform with Customer's specifications; (ii) modifications of the Product made by anyone other than Tenable or a Tenable authorized third party; (iii) Customer's use of the Product in combination with other products or services not provided by Tenable; (iv) Customer's failure to use any updated versions of the Product made available by Tenable; or (v) Customer's use of the Product in a manner not permitted by this Agreement or otherwise not in accordance with the Documentation.

(d) Requirements. The indemnitor shall only be responsible for the indemnification obligations set forth in this Section 9 if the indemnitee: (i) provides the indemnitor prompt written notice of such action or claim; (ii) gives the indemnitor the right to control and direct the investigation, defense, and/or settlement of such action or claim; (iii) reasonably cooperates with the indemnitor in the defense of such a claim (at the indemnitor's expense); and (iv) is not in breach of this Agreement. Nothing herein shall prevent the indemnitee from engaging in defense of any such claim with its own legal representation, provided that this does not materially prejudice the indemnitor's defense. The indemnitor may not settle any claim on behalf of the indemnitee without obtaining the indemnitee's prior written consent; provided, however, the indemnitor shall not be required to obtain consent to settle a claim which settlement consists solely of: (x) discontinued use of infringing Products and/or (y) the payment of money for which the indemnitor has a duty to indemnify.

10. Legal Compliance.

(a) Generally. The Products are intended solely for lawful purposes and use. Each party agrees to perform their respective obligations in a manner that complies with all applicable national, federal, state and local laws, statutes, ordinances, regulations and codes ("Applicable Laws") including, without limitation, the Computer Fraud and Abuse Act (CFAA), 18 USC Sec. 1030.

(b) Exporter of Record. Applicable Laws include U.S. export laws (including the International Traffic in Arms Regulation (ITAR), 22 CFR 120-130, and the Export Administration Regulation (EAR), 15 CFR Parts 730 *et seq*.). Customer agrees that it will be the exporter of record any time it causes the Products to be accessed outside the United States or by a national of any country other than the United States. The parties further agree to comply with sanctions administered by the Department of Treasury's Office of Foreign Assets Control and shall not engage in prohibited trade to persons or entities on the Specially Designated Nationals list.

11. Governing Law; Venue.

(a) For transactions with Tenable, Inc. and Tenable Public Sector LLC, this Agreement shall be governed in all respects by the laws of the State of Delaware, USA, without regard to choice-of-law rules or principles. The Parties agree that: (i) no aspect or provision of the Uniform Computer Information Transactions Act shall apply to this Agreement; and (ii) this Agreement shall not be governed by the U.N. Convention on Contracts for the International Sale of Goods. The Parties hereby submit to the exclusive jurisdiction of the courts of Howard County, Maryland, and the United States District Court for Maryland, Baltimore Division, for any question or dispute arising out of or relating to this Agreement. Due to the high costs and time involved in commercial litigation before a jury, the Parties waive all right to a jury trial with respect to any issues in any action or proceeding arising out of or related to this Agreement.

(b) For transactions with Tenable Network Security Ireland Limited, this Agreement and any issues, disputes or claims arising out of or in connection with it (whether contractual or non-contractual in nature such as claims in tort, from breach of statute or regulation or otherwise) ("Disputes") shall be governed by, and construed in accordance with, the laws of Ireland. You expressly agree with Tenable that this Agreement shall not be governed by the U.N. Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. All Disputes arising out of or relating to this Agreement shall be subject to arbitration within the meaning of the Arbitration Act 2010 or any legislation amending or repealing that act and shall be an arbitration conducted in Dublin, Ireland in the English language and shall be governed by the Arbitration Act 2010. Notwithstanding the foregoing, nothing in this Agreement shall limit the right of either party to seek any injunctive, equitable or other interlocutory relief as it may be entitled to in the Courts of Ireland.

12. Other Legal Clauses.

(a) Third Parties. Customer may permit a third party ("Customer's Agent") to use the Products to perform security services for and on behalf of Customer but solely for Customer's benefit and solely for Customer's internal business purposes. Customer shall be fully responsible for Customer's Agent's use of the Products including liability for any breaches of the Agreement or use beyond the licensed quantities set forth in the Ordering Document. If Customer elects to utilize a Customer's Agent to perform Scans on its behalf, then only Customer's Agent (and not Customer) will be permitted to contact Tenable Support Services. Tenable shall have the right to withdraw its consent to the use of any Customer's Agent in its reasonable discretion.

(b) Notices. Any legal notices or other communication pursuant to this Agreement must be in writing, in English, and will be deemed to have been duly given when delivered if delivered personally or sent by recognized overnight express courier. All notices to Tenable must be sent to the address described in this Agreement to the attention of the Legal Department (unless otherwise specified by Tenable). All notices Tenable sends to Customer shall be at the physical address referenced in this Agreement (or otherwise provided to Tenable). Tenable may provide notices with regard to Products via the email address Customer provided during Product registration and Customer hereby consents to receive such communications from Tenable in an electronic form.

(c) Assignment. Neither Party may assign or otherwise transfer this Agreement without the other Party's prior written consent, which will not be unreasonably withheld; provided, however, either Party may transfer this Agreement to an Affiliate or in connection with a merger or sale of all (or substantially all) of the stock or other ownership units of such Party.

(d) Force Majeure. With the exception of payment, neither Party shall be liable for any loss or delay (including failure to meet the service level commitment) resulting from any force majeure event, including, but not limited to, acts of God, fire, natural disaster, terrorism, labor stoppage, Internet service provider failures or delays, civil unrest, war or military hostilities, or criminal acts of third parties, and any delivery date shall be extended to the extent of any resulting delay.

(f) Language. The language of this Agreement is English and all invoices and other documents given under this Agreement must be in English to be effective. No translation, if any, of this Agreement or any notice will be of any effect in the interpretation of this Agreement or in determining the intent of the parties. The Parties have expressly agreed that all invoices and related documents be drafted in English. The following shall apply solely for Agreements which are under French Canadian jurisdiction: *C'est la volonté expresse des parties que la presente convention ainsi que les documents qui s'y rattacent soient rediges en anglais.*

13. Evaluations and NFR Licenses.

(a) Evaluations. If Customer wants to conduct an evaluation, proof of value or other similar trial of Tenable Products ("Evaluation Products"), Tenable may (in its sole discretion) provide evaluation licenses for such Evaluation Products in accordance with the following: (i) Customer shall have no obligation to make payment for such Evaluation Product for such evaluation usage; (ii) the license term will expire at the end of the agreed-upon evaluation period, at which time Customer must either return or destroy the Software and cease access to the Hosted Services; and (iii) Tenable shall have no obligation to provide Support Services. Customers may not use the Evaluation Products to scan third party Scan Targets or provide a service to Customer's clients.

(b) Technology Partners. Tenable in its sole discretion may allow Customers who are technology partners (a "Technology Partner") to obtain an Evaluation license and use such evaluation license to create a interoperability ("Interoperability") between Tenable Products and their own products. At the conclusion of the Evaluation Term, Customer may apply for an NFR license at which time Tenable may convert the Evaluation license to an NFR license. Tenable's conversion to an NFR license shall be Tenable's sole discretion and may require Interoperability validation by Tenable. Customer may not use Tenable's name or logo without prior written consent and in accordance with Tenables guidelines available at www.tenable.com/brand or a successor location.

(c) NFR. If Customer is a sales partner or Technology Partner to whom a "Not For Resale" or "NFR" license has been granted, Customer's license to the Product will commence upon delivery and continue for a period of one year (unless the Ordering Document sets forth a different term) and shall automatically renew for consecutive one (1) year terms unless either Party provides the other Party with written notice of its non-renewal of the NFR license at least thirty (30) days before the expiration of the then-current term. Notwithstanding the foregoing, Tenable may terminate Customer's NFR license for its convenience upon thirty (30) days' notice, or immediately should Customer breach any obligations under this Agreement.

(d) NFR Customer Prohibitions. Customer shall not purport to take on any obligation or responsibility, or make any representations, warranties, guarantees or endorsements to anyone on behalf of Tenable, including without limitation, relating to Tenable products, software, or services. Except as specifically permitted in this Agreement, Customer shall not state or imply that any of Customer's products have been endorsed, reviewed, certified or otherwise approved by Tenable.

(e) NFR Customer Representations. Customer hereby represent and warrant to Tenable that: (i) Customer will not intentionally harm the reputation or goodwill of Tenable through any act or omission, and (ii) Customer have used commercially reasonable efforts to ensure that any software, code, algorithm, API, etc., transferred to Tenable is free from any time bomb, virus, drop dead device, worm, Trojan horse, or trap door that is designed to delete, disable, deactivate, interfere with, or otherwise harm hardware, data, or other programs or that is intended to provide access or produce modifications not authorized by Tenable.

(f) NFR Customer Responsibilities. Customer shall, at its sole cost and expense, defend (or at its option, settle) and indemnify Tenable and Tenable's subsidiaries and affiliates, and their officers, directors, employees, representatives and agents, from and against any and all third party claims brought against Tenable based upon a claim that use of Customer's software or Customer's product in accordance with this Agreement infringes such third party's patent, copyright or trademark or misappropriates any trade secret, and shall pay all settlements entered into and damages awarded to the extent based on such claim or action.

14. General.

This Agreement constitutes the entire agreement between the Parties, and supersedes all other prior or contemporaneous communications between the Parties (whether written or oral) relating to the subject matter of this Agreement. No Customer document or purchase order shall modify, supersede, or become part of this Agreement, or otherwise contractually bind Tenable unless signed by Tenable. The provisions of this Agreement will be deemed severable, and the unenforceability of any one or more provisions will not affect the enforceability of any other provisions. If any provision of this Agreement, for any reason, is declared to be unenforceable, the Parties will substitute an enforceable provision that, to the maximum extent possible under applicable law, preserves the original intentions and economic positions of the Parties. Section headings are for convenience only and shall not be considered in the interpretation of this Agreement. Customer agrees that Tenable may use Customer's name or logo in a customer list. Customer may not use Tenable's name or logo without prior written consent and in accordance with Tenable's guidelines. No failure or delay by a Party in exercising any right, power or remedy will operate as a waiver of that right, power or remedy, and no waiver will be effective unless it is in writing and signed by the waiving Party. If a Party waives any right, power or remedy, the waiver will not waive any successive or other right, power or remedy the Party may have under this Agreement. The Parties are independent contractors and this Agreement will not establish any relationship of partnership, joint venture, employment, franchise or agency between the Parties. This Agreement is not intended nor will it be interpreted to confer any benefit, right or privilege in any person or entity not a party to this Agreement. Any party who is not a party to this Agreement has no right under any law to enforce any term of this Agreement. Any provision of this Agreement that imposes or contemplates continuing obligations on a party and any section which by its nature is intended to survive will survive the expiration or termination of this Agreement, including Sections 3, 4, 8, 9 and 11.

15. Government Entities. *This Section 15 shall only apply to Government Customers, as defined below.*

If Customer is an agency or instrumentality of a sovereign government (a "Government Customer"), all Government Customer end users acquire the rights to use and/or access the Products and or Services with only those rights set forth herein (consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4). The terms and conditions of this Agreement govern Government Customer's use and disclosure of the Products and supersede any conflicting terms and conditions that may be applicable through the Government Customer's procurement regulations. If this Agreement fails to meet the Government Customer's needs or is inconsistent in any way with federal law, the government must return the Product, unused, to Tenable. If Customer is prohibited by law, regulation, or relevant attorney general opinion from agreeing to any clause of this Agreement (collectively, "Restrictions"), the Agreement shall be modified to the extent required under such Restrictions. Each of the components that constitute the Product is a "commercial item" as that term is defined at 48 C.F.R. 2.101, consisting of "commercial computer software" and/or "commercial computer software documentation" as such terms are used in 48 C.F.R. 12.212.

SCHEDULE A: SOFTWARE

This Schedule for Tenable Software (this "Schedule") is subject to and made part of the Agreement.

1. General. This Schedule governs Customer's license of Software.

2. License; Right to Use. Subject to the terms of the Agreement and payment of the applicable license fees, Tenable grants Customer for the duration of the License Term a non-exclusive, non-transferable, non-sublicensable license to use the Software (in object code form only) solely for Customer's own internal business purposes. Customer's right to install such Software is limited to use with the computers or machines for which the Software is registered for use. Customer is permitted to make one copy of the Software for backup or archival purposes.

3. Warranty. Tenable warrants that the Software shall materially conform to the Documentation for a period of thirty (30) days after Delivery. Customer's sole and exclusive remedy for breach of this warranty shall be for Tenable to, at its sole option: (i) use commercially reasonable efforts to modify or correct the Software such that in all material respects it conforms to the functionality described in the Documentation; or (ii) if Tenable is unable to restore such functionality within a reasonable period of time, Customer shall be entitled to a refund for the non-confirming Software.

4. Open Source and Third Party Software. Any code or other intellectual property included as part of the Software that was licensed to Tenable by third parties that is not marked as copyrighted by Tenable is subject to other license terms that are specified in the Documentation available on Tenable's website at https://docs.tenable.com/licensedeclarations/ (or a successor location). Customer agrees to be bound by such other license terms.

5. Audit Rights. Tenable may, by itself or through a third party independent auditor, audit Customer's usage of the Software to confirm compliance with this Agreement or the applicable Ordering Document. Tenable shall: (i) provide Customer with reasonable advance notice of the audit; (ii) not request such audit more than once per year; and (iii) not unreasonably interfere with Customer's business activities when conducting the audit.

SCHEDULE B: HOSTED SERVICES

This Schedule for Tenable Hosted Services (this "Schedule") is subject to and made part of the Agreement.

1. General. This Schedule governs Customer's purchase and use of the Hosted Services.

2. License; Right to Use. Subject to the terms of the Agreement and payment of the applicable license fees, Tenable grants Customer for the duration of the License Term a non-exclusive, non-transferable, non-sublicensable right to access the Hosted Environment and use those modules of the Hosted Services set forth on a valid Ordering Document solely for Customer's own internal business purposes.

3. Warranty. Tenable warrants that the Hosted Services will materially comply with the functionality described in the Documentation. Customer's sole and exclusive remedy for breach of this warranty shall be for Tenable to use commercially reasonable efforts to modify the Hosted Services to provide in all material respects the functionality described in the Documentation. If Tenable is unable to restore such functionality within sixty (60) days, Customer shall be entitled to terminate the Agreement and receive a pro-rata refund of any prepaid but unused fees for the nonconforming Hosted Services. Tenable shall have no obligation with respect to a warranty claim hereunder unless Customer notifies Tenable of such claim within thirty (30) days of the date the underlying condition first arose. This warranty shall only apply if the applicable Hosted Service has been utilized in accordance with the Agreement and the Documentation.

4. Acknowledgements. Customer authorizes Tenable to perform the Scans, including accessing the Scan Targets in the context of the Scans. Customer understands and acknowledges that the Scans may originate or appear to originate from a Tenable URL which could cause Customer (or the owner of the Scan Targets) to believe they are under attack. Customer agrees not to pursue any claims against Tenable as a result of any access to Scan Targets when such access was made in connection with an authorized Scan unless such a claim is based on the gross negligence or willful misconduct of Tenable.

5. Usage Requirements. Customer must provide current and accurate information in all submissions made in connection with the Hosted Services, including registration information and the location of the Scan Targets to be Scanned. Tenable may, in its reasonable discretion, prohibit or suspend access of certain users of the Hosted Services. Customer agrees to safeguard and maintain the confidentiality of all user names and passwords. Customer further agrees to use best efforts to ensure that no unauthorized parties have access to the Hosted Services through Customer's account and/or log-in credentials. Customer will promptly notify Tenable of any unauthorized access of which Customer is aware or reasonably suspects. Customer is responsible for compliance with this Agreement and all use of the Hosted Services through Customer's account.

6. PCI Scans. Tenable makes no guarantee that a successful completion of a PCI Scan will make Customer compliant with the Payment Card Industry Data Security Standard.

7. Data Retention Policy. Tenable will maintain Customer Scan data stored in the Hosted Environment for a period of not less than one year from the Scan date. Customer acknowledges that Tenable is in no way responsible for any of Customer's data retention compliance requirements. Tenable's data retention policy with respect to PCI Scans will match then-current requirements set forth by the PCI Security Standards Council.

8. Service Level Agreement. Tenable commits to make access to the Hosted Environment available in accordance with Tenable's then-current service level agreement, available at http://static.tenable.com/prod_docs/Service_Level_Commitment.pdf (or a successor location).

SCHEDULE C: PROFESSIONAL SERVICES

This Schedule for Tenable Professional Services is subject to and made part of the Agreement.

1. General. The Parties may agree, from time to time, on the purchase and sale of Tenable Professional Services. Professional Services shall be as further described in a separate SOW or Services Brief. No SOW shall be binding upon the Parties until it has been executed by both Parties. Except as otherwise agreed to by the Parties in writing, all Services Briefs or signed SOWs will be governed by this Agreement. In the event of inconsistency between the Agreement and a signed SOW, the signed SOW shall govern.

2. Type of Services. Tenable offers a range of Professional Services; provided, however, unless otherwise agreed upon in writing, Tenable does not offer creation of custom intellectual property. Tenable is not obligated to provide any Professional Services except as mutually agreed in a Services Brief or SOW.

3. Deliverables. "Deliverable(s)" means the reports, analysis, codes, scripts slides, documents, examples and other written materials or work results provided as part of the Professional Services.

4. Intellectual Property Rights.

(a) Grant of License in Deliverables. Tenable grants Customer a non-exclusive, non-transferable, irrevocable (except in case of breach of the Agreement or SOW) perpetual right to use, copy and create derivative works from the Deliverables (without the right to sublicense) for Customer's internal business operations, as contemplated by the applicable SOW or Services Brief.

(b) Reservation of Rights. Except for the rights expressly granted herein to Customer, Tenable expressly reserve all other rights in and to the Professional Services and Deliverables. Notwithstanding anything to the contrary in this Schedule, nothing shall prevent Tenable from providing similar Professional Services to other customers and nothing in this Schedule shall be construed to provide any intellectual property rights whatsoever in the Products (or any modifications or enhancements thereto) that Tenable develops or makes generally available for sale to its customers.

(c) Pre-Existing Materials. Any pre-existing materials, proprietary item or intellectual property rights of either Party which is disclosed or used in performing the Professional Services shall remain fully vested in such Party. Nothing in this Schedule shall transfer any rights whatsoever in Tenable's Products. Customer hereby grants to Tenable the intellectual property rights (if any) required for Tenable to perform the Professional Services.

5. Warranty. Tenable warrants that all Professional Services shall be performed in a professional manner and in accordance with industry standards. Tenable further warrants for a period of ten (10) days from the service completion date that the Professional Services shall materially conform to with the applicable SOW or Services Brief. If Customer provides written notice of a non-conformity during this warranty period, Tenable shall promptly confirm the non-conformity and upon confirmation, Tenable's entire liability and Customer's exclusive remedy shall be for Tenable to use commercially reasonable efforts to re-perform the Professional Services within a reasonable amount of time. If Tenable is unable to re-perform the Professional Services, then Tenable may elect to refund amounts paid by Customer for the non-conforming Professional Services.

6. Scheduling; Cancellation. Professional Services must be scheduled within three (3) months of the date of the Ordering Document under which such Professional Services were purchased and completed within six (6) months of the of the Ordering Document. If Customer does not schedule the Professional Services within this time frame, Tenable shall have no obligation to perform the Professional Services or provide a refund. Tenable shall have no obligation to perform the Professional Services or provide a refund if Customer or Customer's designated attendees do not attend a scheduled training session or cancel a Professional Services engagement without providing proper notice. Customer must provide Tenable at least ten (10) business days' notice to reschedule any Professional Services.

7. Customer Responsibilities. For Professional Services occurring on Customer's site, Tenable agrees to comply with applicable and reasonable security procedures provided Customer provides Tenable with such written procedures in advance. Some of the Professional Services may require Customer to have specialized knowledge or meet particular software or hardware requirements (for example, appropriate computers or appliances, stable Internet connection or up-to-date web browsers or operating system, etc.). If technical issues arise during the Professional Services, Tenable will use commercially reasonable efforts to resolve such issues, but will have no liability based on Customer's failure to meet technical requirements. Tenable will not provide any refund based on Customer's failure to meet these prerequisites.

8. Changes. Either party may request that a change be made to the Professional Services. Tenable reserves the right to charge a fee for any material changes to the Professional Services. No changes shall be binding unless executed by both Parties.

9. Non-Solicitation. During the term that Professional Services are being provided and for a period of one (1) year after their completion, Customers will not, either directly or indirectly, solicit for employment any person employed by Tenable or any of its Affiliates that have provided Customer Professional Services under this Agreement. For the avoidance of doubt, this restriction shall not prevent Customer from hiring based on a response to Customer's advertising in good faith to the general public a position or vacancy to which an employee or worker of Tenable responds, provided that no such advertisement shall be intended to specifically target Tenable personnel.