



A Proposal to

State of West Virginia

for

RFP for Cyber Security Program (OT 19152)

ISC2000000001

Original Technical Proposal

August 29, 2019

Presented by:
Sandra Hawkins
Sr. Client Executive

Verizon
4700 Maccorkle Avenue SE
Charleston, WV 25304
304-356-3395/304-356-3590
sandra.k.hawkins@verizon.com

RECEIVED
2019 AUG 29 AM 10:45
WV PURCHASING
DIVISION



Verizon Business Group
4700 MacCorkle Av SE
Charleston, WV 25304
304-356-3395

August 29, 2019

Department of Administration
Purchasing Division
2019 Washington St., E
Charleston, WV 25304

Dear Ms. Chambers:

Verizon is pleased to submit its proposal for Cyber Security Program in response to RFP ISC2000000001.

Verizon is one of the largest communication technology companies in the world. With over 150 locations, Verizon is a global leader delivering innovative communications and technology solutions that improve the way our customers live, work, learn and play. Every day, we connect millions of people, companies and communities with our powerful technology.

Verizon provides communication solutions for 95%+ Fortune 500 Companies in Financial, Retail, Manufacturing, Utilities, Information and Transportation companies. In the U. S most of the largest enterprises trust Verizon for their technology solutions. Verizon Ranks 16th in Fortune 500 US Rankings, 37th in Fortune Global 1000 Ranking, a Dow 30 Company and rank 18th in Forbes Global 2000 Ranking.

Verizon's security team has over 180 consultants in 30 countries. We have conducted more than 16,000 assessments since 2009. Verizon has provided Security Consulting Services since 1999 and we deliver PCI compliance services since 2003.

We appreciate the time invested in review of this response and look forward to a long, successful partnership with the State of West Virginia. Should any questions arise as a result of our submission, please feel free to contact me at either (304) 356-3395 or sandra.k.hawkins@verizon.com.

Sincerely,

Sandra K. Hawkins

Sandra K. Hawkins
Senior Client Partner

Contents

Section 1. General Information and Instructions

Section 2. Instructions to Vendors Submitting Bids

Section 3. General Terms and Conditions

Section 3A. Definitions

Section 4. Project Specifications

Section 5. Vendor Proposal

Section 6. Evaluation and Award

Certification and Signature Page

Addendum 1

Addendum 2

Exhibit 1. Verizon CRP Model of Example Offerings for Agency Charge Back

Exhibit 2. Verizon Project Management Approach & Methods

Exhibit 3. Verizon Cyber Risk Management Program Service Description

Exhibit 4. Sample Resume for Professional Services Principal Lead

Exhibit 5. Verizon CRP Risk Assessment Reporting Samples

Exhibit 6. Verizon Project Manager Resume

Exhibit 7. United States Service Agreement

Exhibit 8. WV96/Purchasing Affidavit/Disclosure of Interested Parties forms, signed

Exhibit 9. Insurance & Indemnification Clarifications



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

State of West Virginia
 Request for Proposal
 10 – Consulting

Proc Folder: 609025

Doc Description: Cyber Security Program RFP (OT19152)

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-07-26	2019-08-29 13:30:00	CRFP / 0210 ISC2000000001	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:

Verizon Business Network Svcs Inc. on behalf of MCI Communications Services Inc d/b/a Verizon Business Services
 4700 MacCorkle Av SE, Charleston, WV 25304
 304-356-3395

FOR INFORMATION CONTACT THE BUYER

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

Signature X

FEIN #

47-0751768

DATE

08/27/2019

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

ADDITIONAL INFORMATION:

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code 5A-3-10b, for the West Virginia Office of Technology (hereinafter referred to as the "Agency") to establish a Cyber Security Risk Program per attached documents.

MANDATORY PRE-BID MEETING:

DATE: 08/08/2019

TIME: 10:00 am - 12:00 pm EDT

LOCATION: WV Office of Technology

1900 Kanawha Blvd. E.,

Building 6, Conference Room 122A

Charleston, WV 25305

NOTE: Online responses to this solicitation are prohibited. Please see the Instructions to Bidders in Section 2 for proposal submission.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV 25305 US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Cyber Security Risk Program	1.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description :

Cyber Security Risk Program

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV 25305 US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Post Implementation Consultant	1000.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description :

Post Implementation Consultant

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Mandatory Pre-Bid at 10:00 am	2019-08-08
2	Question Deadline by 4:00 pm	2019-08-19

ISC2000000001	Document Phase Final	Document Description Cyber Security Program RFP (OT19152)	Page 3 of 3
----------------------	--------------------------------	---	------------------------------

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

REQUEST FOR PROPOSAL

CRFP ISC200000001

WVOT - Cyber Security Program

TABLE OF CONTENTS

1. Table of Contents
2. Section 1: General Information and Instructions
3. Section 2: Instructions to Vendors Submitting Bids
4. Section 3: General Terms and Conditions
5. Section 4: Definitions

6. Section 5: Project Specifications
7. Section 6: Vendor Proposal
8. Section 7: Evaluation and Award
9. Certification and Signature Page

SECTION 1: GENERAL INFORMATION

1.1. Introduction:

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code §5A-3-10b, for the West Virginia Office of Technology (hereinafter referred to as the "Agency") to establish a Cyber Security Risk Program.

The RFP is a procurement method in which vendors submit proposals in response to the request for proposal published by the Purchasing Division. It requires an award to the highest scoring vendor, rather than the lowest cost vendor, based upon a technical evaluation of the vendor's technical proposal and a cost evaluation. This is referred to as a best value procurement. Through their proposals, vendors offer a solution to the objectives, problem, or need specified in the RFP, and define how they intend to meet (or exceed) the RFP requirements.

1.2. RFP Schedule of Events:

RFP Released to Public	See wvOASIS
Mandatory Pre-bid Conference	08/08/2019 at 10:00 am
Vendor's Written Questions Submission Deadline	08/19/2019
Addendum Issued	TBD
Technical Bid Opening Date	08/29/2019 at 1:30 pm
Technical Evaluation Begins	TBD
Oral Presentation (<i>Agency Option</i>)	TBD
Cost Bid Opening	TBD
Cost Evaluation Begins	TBD
Contract Award Made	TBD

REQUEST FOR PROPOSAL

CRFP ISC2000000001

WVOT - Cyber Security Program

SECTION 2: INSTRUCTIONS TO VENDORS SUBMITTING BIDS

Instructions begin on next page.

INSTRUCTIONS TO VENDORS SUBMITTING BIDS

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

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

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

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

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

August 8, 2019

10:00 am to 12:00 pm

WV State Capitol Complex
Building 6, Conference Room 122A
Charleston, WV

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:

Submit Questions to: August 19, 2019 by 4:00 pm
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:
SOLICITATION NO.:
BID OPENING DATE:
BID OPENING TIME:
FAX NUMBER:

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 four (4) 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: August 29, 2019 at 1:30 pm

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

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

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

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

Revised 06/05/2019

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

REQUEST FOR PROPOSAL
CRFP ISC2000000001
WVOT - Cyber Security Program

SECTION 3: GENERAL TERMS AND CONDITIONS

Terms and conditions begin on next page.

GENERAL TERMS AND CONDITIONS:

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

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

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

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

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

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

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

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

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

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

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

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

Term Contract

Initial Contract Term: This Contract becomes effective on Award _____ and extends for a period of Two (2) 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 Two (2) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

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

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

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

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

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

Other: See attached.

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

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

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

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

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

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

6. **EMERGENCY PURCHASES:** The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute a 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.

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

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

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

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

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

LICENSE(S) / CERTIFICATIONS / PERMITS: In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits prior to Contract award, in a form acceptable to the Purchasing Division.

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

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

Vendor must maintain:

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

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

Professional/Malpractice/Errors and Omission Insurance in at least an amount of: \$1,000,000 per occurrence.

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

Cyber Liability Insurance in an amount of: _____ per occurrence.

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

Pollution Insurance in an amount of: _____ per occurrence.

Aircraft Liability in an amount of: _____ per occurrence.

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

Verizon Response: See clarification

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

10. [Reserved]

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

_____ for _____

Liquidated Damages Contained in the Specifications

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

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

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

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

Verizon Response: Verizon's preferred payment options are 1) electronic Automated Clearing House (ACH) payment; 2) electronic bank account Wire Transfer; or 3) paper check payment. Both electronic payment options can be set up through the customer's account on Verizon's online billing portal, the VEC.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[Verizon Response: See clarification](#)

Revised 06/05/2019

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

Sandra Hawkins, Senior Client Partner

(Name, Title)
Sandra Hawkins, Senior Client Partner

(Printed Name and Title)
4700 MacCorkle Av SE Charleston WV 25304


(Address)
304-356-3395/ 304-356-3590

(Phone Number) / (Fax Number)
sandra.k.hawkins@verizon.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.

Verizon Business Network Svc Inc, on behalf of MCI Communications Svcs Inc
d/b/a Verizon Business Services

(Company)


(Authorized Signature) (Representative Name, Title)
OBI ROMAINE - SNR ANALYST

(Printed Name and Title of Authorized Representative)
08/27/2019

(Date)
304-356-3395/304-356-3590

(Phone Number) (Fax Number)

REQUEST FOR PROPOSAL

CRFP ISC200000001

WVOT - Cyber Security Program

SECTION 3A: DEFINITIONS: The terms listed below shall have the meanings assigned to them below.

3A.1 "Cybersecurity framework" means computer technology security guidance for organizations to assess and improve their ability to prevent, detect, and respond to cyber-attacks.

3A.2 "Cyber incident" means any event that threatens the security, confidentiality, integrity, or availability of information assets, information systems or the networks that deliver the information.

3A.3 "Cybersecurity risk assessment" means the process of identifying, analyzing and evaluating risk and applying the appropriate security controls relevant to the information custodians.

3A.4 "Cybersecurity risk management service" means technologies, practices and policies that address threats and vulnerabilities in networks, computers, programs and data, flowing from or enabled by connection to digital infrastructure, information systems or industrial control systems, including but not limited to, information security, supply chain assurance, information assistance and hardware or software assurance.

3A.5 "Enterprise" means the collective departments, agencies and boards within state government that provide services to citizens and other state entities.

3A.6 "Information custodian" means a department, agency or person who owns accountability for a set of data assets.

3A.7 "Privacy impact assessment" means a tool for identifying and assessing privacy risks throughout the development life cycle of a program or system.

3A.8 "Plan of action and milestones" means a remedial plan, or the process of accepting or resolving risk, which helps the information custodian to identify and assess information system security and privacy weaknesses, set priorities and monitor progress toward mitigating the weaknesses.

3A.9 "Security controls" means safeguards or countermeasures to avoid, detect, counteract or minimize security risks to physical property, information, computer systems or other assets.

REQUEST FOR PROPOSAL

CRFP ISC200000001

WVOT - Cyber Security Program

SECTION 4: PROJECT SPECIFICATIONS

4.1. Background and Current Operating Environment:

The purpose of this RFP is to contract with a Vendor to establish a Cyber Security Risk Program that will be utilized by the West Virginia Office of Technology supported state agencies as described in West Virginia Code §5A-6B. This program shall be completed in 24 calendar months. Strict time and deliverable requirements must be met to ensure compliance with State law.

The West Virginia Office of Technology (WVOT), under the Department of Administration, and its Chief Technology Officer, sets goals to develop an organized approach to information resource management for this state while providing technical assistance to state entities in the design and management of information systems.

The WVOT provides highly reliable, secure, and cost-effective technology services to 25,000 computers and 20,000 network users. Services are delivered by approximately 200 full-time and temporary employees and supplemented by specialized contract services and staff on an as-needed basis.

Services are provided to the following departments within the Executive Branch: Administration, Commerce, Environmental Protection, Health and Human Resources, Military Affairs and Public Safety, Transportation, Revenue, Veterans Affairs, and several independent boards and commissions. There are approximately 210 entities total, within these departments. Funding for the Office of Technology is derived from charges for services to state agencies.

4.2. Project Goals and Mandatory Requirements:

On March 25, 2019, West Virginia House Bill 2452 was codified into law as West Virginia Code 5A-6B-1, *et seq.*, requiring a statewide cyber risk assessment program to be established by the Cybersecurity Office of WVOT. The office will need to identify and adopt an established cybersecurity standard to serve as the statewide framework for conducting cybersecurity and privacy assessments, both for self-assessment and third-party assessment. The framework must align with the cyber risk posture assessment program, enabling an "apples-to apples" analysis for executive leadership.

This solicitation is intended to obtain a vendor that will plan for, create, implement and ultimately turnover to WVOT personnel the Cyber Risk Program. As part of the Cyber Risk Program, the Vendor will be expected to assist WVOT in developing two solicitations on behalf of WVOT as more fully described below. The Program will help drive strategic planning for cybersecurity initiatives and outside of the two solicitations mentioned in the Goals and Objectives section, will NOT directly involve technology procurements, vendor-led services, or out-sourced cybersecurity staff. The Vendor awarded this contract will not be permitted to bid on the two solicitations that Vendor developed for WVOT hereunder.

REQUEST FOR PROPOSAL

CRFP ISC200000001

WVOT - Cyber Security Program

Vendor should provide its approach and methodology to providing the service or solving the problem described by meeting the goals/objectives identified below. Vendor's response should include any information about how the proposed approach is superior or inferior to other possible approaches, outline project deliverables, and provide supporting documentation.

4.2.1. Goals and Objectives – Cyber Risk Program: The goal and objective of this solicitation is to contract with a Vendor to plan for, create, implement and ultimately turnover to WVOT personnel the Cyber Risk Program. That overarching goal/objective is described in more detail below.

4.2.1.1. Framework Development: Vendor should define an enterprise set of policies supported by a tactical framework aligned to a shared view of critical risk areas. Vendor should:

4.2.1.1.1. Identify most critical information assets and align to applications and agencies.

4.2.1.1.2. Evaluate agencies with the highest risk exposure based off their assets and any mandated compliance requirements.

4.2.1.1.3. Develop and consolidate evaluation framework. Framework should account for maturity of varying organizations with option of 'tiering' framework alignment. Framework detail should be aligned with overarching State policies and standards.

4.2.1.1.4. Establish a Risk Profiling Procedure and pilot the results of the risk profile.

Verizon Response: Verizon has read, understands, and will comply with all elements of 4.2.1.1

Verizon will assist WVOT with identifying high value assets, applications and business functions essential to the WVOT's business and services. Designing the Cyber Risk Program (CRP) involves Verizon:

- 1. Examining WVOT's organizational structure;*
- 2. Documenting objectives, priorities, and options; and*
- 3. Review of WVOT policies*

Verizon will develop a CRP with the essential elements of identifying, assessing, responding, monitoring and reporting the risks. The CRP is designed to identify and measure the effectiveness of risk controls and potential weaknesses within your systems.

Verizon has a proven history of understanding data loss as evidenced by The Verizon Data Breach Investigations Report (DBIR). The DBIR serves as the foundation of the Verizon CRP by using the threat scenarios and attack patterns reported by organizations to create potential risk scores, which WVOT would use to enhance their cyber security posture.

Underlying the DBIR is the Vocabulary for Event Recording and Incident Sharing (VERIS). VERIS is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. VERIS helps organizations understand what they need to know and how to measure it. The CRP help organizations better understand each landscape through a set of cyber risk metrics that improves an organization's ability to make informed cyber risk determinations and decisions.

Verizon will assist WVOT with the development of a framework to identify, analyze and present IT related security risks and opportunities in a business context reflective of WVOT's risk-based management approach. The framework to be developed will be designed will be aligned with NIST 800-30 and 800-37 as it pertains to performing risk assessments and implementing an overall IT risk management framework. Verizon will work with WVOT to establish ongoing processes for analyzing changing IT risks and updating WVOT's enterprise IT security risk profile. Verizon will also assist WVOT to develop ongoing processes to maintain and monitor WVOT's IT protection strategy and objectives.

Verizon will assist WVOT to develop a standard framework to bring IT security risks in line with defined risk tolerances for WVOT's organization. This framework design will address the four major risk reduction options (Avoid, Transfer, Mitigate, and Accept) and provide workflows to complete the response process.

Verizon will develop the CRP to risk frameworks such as NIST to meet the industry accepted standards. Verizon will work with WVOT to define, develop, build/integrate, and train WVOT to use a maintainable IT IS Policy framework consisting of applicable Information Security Policies (Capstone security policy and second-level security policies to cover ISO 27001 & NIST 800-53 integrated requirements), security standards and baselines to document technical security controls, and security procedures and guidelines to document operational security controls.

Verizon and WVOT will agree on common formats for security artifacts and define common control language structure and nomenclature, and Verizon will revise existing content and develop new content to represent all of the agreed controls that will make up WVOT's control base. Verizon will also collaborate with WVOT to implement a data and document stores to house policy documents, common content, and references. These data systems will support content and document management, Intranet publication of policy information to the WVOT workforce, and serve as a reference point for security training programs across WVOT companies.

Verizon will provide guidance and recommendations on tools/platforms selection, and may act as a re-seller of tools & platforms necessary to build out a program.

4.2.1.2.Cyber Risk Program Documentation/Creation: Vendor should create a fully documented Cyber Risk Program, deploy program in set of pilots, and incorporate lessons learned after pilot programs are executed. Vendor should:

4.2.1.2.1. Develop Policies and operations procedures, reporting templates, and program roadmap.

4.2.1.2.2. Define roles and responsibilities between central teams and agencies.

4.2.1.2.3. Document approach, tools, and templates for agencies to apply framework and manage audit and assessment activities.

4.2.1.2.4. Pilot the program with at least one small and one large agency.

4.2.1.2.5. Assess the results and document lessons learned from Pilot program. Remediation of issues should be accounted for in the milestones and deadlines.

Verizon Response: Verizon has read, understands, and will comply all elements of 4.2.1.2 Verizon's CRP consultancy will help the State of West Virginia to develop a program to identify, evaluate, and prioritize risk using measurements acquired from a series of risk assessment methods. The CRP program will identify risks threats to the State and its Agencies and provide expert assessment and diagnostic methods integrated into a single program.

Verizon will support an ongoing program performance for the specified time to review completed risk assessments, identify gaps and/or areas for improvement, and ensure quality and consistency in conducting risk assessments.

Verizon will also facilitate the performance of periodic risk management activities. Key components will include, but not be limited to, the development of dashboards and reports addressing risk assessments performed to date, planned risk assessments, performance against forecast/plan and a high level review of completed risk assessments.

Verizon will review risk management plan performance to highlight key success factors, track risk reduction efforts against submitted plans, and update previously reported risk ratings based on changes to perceived threat, vulnerability and impact.

The Verizon CRP consultancy will help the WVOT and its Agencies meet all the objectives described and develop playbooks for program operation, as well as, reporting such as an Executive level report and detail risk-assessment reports with recommendations. This is the approach that Verizon takes with our CRP which has served our customers for over 10 years and is fully developed with mature business processes and best practices.

See Exhibit 5 – CRP Risk Assessment Reporting Samples

REQUEST FOR PROPOSAL

CRFP ISC200000001

WVOT - Cyber Security Program

4.2.1.3. Compliance Audit Solicitation: Vendor should conduct market research to define the specifications and goals needed to create a solicitation that will allow agencies a procurement means to have a third party evaluate their adherence to security standards. Vendor should:

4.2.1.3.1. Assist WVOT in developing solicitation. (Vendor will not be permitted to bid on this solicitation it helps to develop and is also prohibited from serving as a subcontractor to the vendor that is awarded a contract thereunder.)

4.2.1.3.2. Vendor should provide expertise in identifying, analyzing and evaluating agency risk and applying the appropriate security controls relevant to

the information custodians

4.2.1.3.3. Review vendor responses and advise reviewers.

4.2.1.3.4. Provide guidance and assistance to WVOT to process and assist agencies in using the solicitation.

Verizon Response: Verizon has read, understands, and will comply with 4.2.1.3 Verizon's CRP consultancy will assist the State of West Virginia to define specifications and standards in order to make recommendations for selections of 3rd parties that will further evaluate and validate adherence to the WVOT CRP program and Compliance Audit.

Verizon is well versed and has a proven expertise with identifying, analyzing, and evaluating risks associated with security controls such as NIST 800-53 and ISO 27001/27002.

4.2.1.4. Governance, Risk, & Compliance (GRC) Tool Solicitation: Vendor should assist WVOT in developing a solicitation to obtain a GRC tool to support risk-based scoping, capture audit results, conduct qualitative & quantitative risk assessment, and track action items, and further assist in implementing that tool. Ultimately, the tool solicitation should be focused on the procurement and implementation of a tool designed to directly support the Cyber Risk Service. Vendor should:

4.2.1.4.1. Assist WVOT in developing a solicitation for a governance tool. (Vendor will not be permitted to bid on this solicitation it helps to develop and is also prohibited from serving as a subcontractor to the vendor that is awarded a contract thereunder.)

4.2.1.4.2. Implement the governance tool to support future assessment.

4.2.1.4.3. Establish baseline security and use procedures for the tool.

4.2.1.4.4. Customize the tool to align with state specific requirements established during programs development.

4.2.1.4.5. Train users to utilize the governance tool and develop policies and procedures for the governance tool.

Verizon Response: Verizon has read, understands, and will comply 4.2.1.4. Verizon's CRP consultancy will assist the State of West Virginia to define specifications and standards in order to make recommendations for selections of GRC tools that will further evaluate and validate adherence to the WVOT CRP program for measures of Governance, Risk, and Compliance.

Verizon is familiar with industry leading GRC (e.g., Archer, FAIR methodology, etc.) tools and will assist WVOT with developing a solicitation for procurement and implementation of a tool that best fits the WVOT cyber risk services.

REQUEST FOR PROPOSAL CRFP ISC2000000001

WVOT -Cyber Security Program

4.2.1.5.Full Implementation: Based on previously established roadmap and pilot results Vendor should create a roll-out plan to incrementally deploy framework and Cyber Risk Program to agencies. The roll out plan should:

- 4.2.1.5.1. Include a communications plan.
- 4.2.1.5.2. Include education and enablement of tools,
- 4.2.1.5.3. Incrementally expand pilot program,
- 4.2.1.5.4. Plan for framework deployment and audit execution across the enterprise,
- 4.2.1.5.5. Include the performance of audit of enterprise services,
- 4.2.1.5.6. Support agencies with utilizing the third-party vendor awarded a contract to perform assessments.

Verizon Response: Verizon has read, understands, and will comply.

4.2.1.6. Ongoing Support: Vendor should develop the financial rates model for cover the projected operational expenses of the Cyber Risk Program based on a charge-back model. The Cyber Risk Program should be supportable and sustainable business model, where the Office of Technology provides services to customer agencies and charges a fee for those services. Vendor should:

- 4.2.1.6.1. Ensure that its Cyber Risk Program services are trackable in accordance with WVOT charge back model,
- 4.2.1.6.2. Identifying appropriate points for fee assessment,
- 4.2.1.6.3. Assist WVOT in establishing pricing for various aspects of the Cyber Risk Program.
- 4.2.1.6.4. Recommendations would recommend Enterprise cybersecurity risk services based on services which directly addresses state-wide critical cyber risks.
- 4.2.1.6.5. Recommendations should take into consideration leveraging cost-sharing and economies of scale opportunities to drive cost-efficiencies; and, is
- 4.2.1.6.6. implemented and delivered as an enterprise/managed service, addressing cyber workforce challenges.

Verizon Response: Verizon has read, understands, and will comply with elements of 4.2.1.6. Verizon is prepared to develop an acceptable financial model so the State can provide charge back to its Agencies. We have deep experience in creating financial modeling for customers to include

our own CRP model. See Exhibit 1 - CRP Model of Example Offerings for Agency Charge Back

REQUEST FOR PROPOSAL

CRFP ISC200000001

WVOT - Cyber Security Program

4.2.1.7. Communication: Vendor should establish a clear communication plan

4.2.1.7.1. The State can apply custom branding to all documents and materials.

4.2.1.7.2. Vendor should establish regular communications to discuss project status at a minimum of every two (2) weeks.

4.2.1.7.3. Vendor should provide communications to different levels of stakeholders identified in the project proposal.

4.2.1.7.4. Vendor should provide on-site support for major milestones and project initiatives.

Verizon Response: Verizon has read, understands, and will comply. Verizon is prepared to engage with your team for on-site sessions for a week each month for the duration of the contract. In addition, we will also have an assigned Project Manager who will steward the Project Plan for CRP and ensure that regular work stream efforts and resources from Verizon are meeting the plan milestones. The Project Manager will also establish regular communication and project touchpoints to the different levels of stakeholders identified in the Project.

Verizon's communication plan will clearly lead users through the process of determining which messages to deliver throughout the project for the following personnel:

- *Project personnel*
- *Sponsors*
- *Vendors*
- *Other stakeholders*

The purpose of the Verizon Communications Plan is to provide an overall framework for managing and coordinating the wide variety of communication that will directly or indirectly take place as part of the project.

4.2.2. Mandatory Project Requirements -The following mandatory requirements relate to the goals and objectives and must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it will comply with the mandatory requirements and include any areas where its proposed solution exceeds the mandatory requirement. Failure to comply with mandatory requirements will lead to disqualification, but the approach/methodology that the vendor uses to comply, and areas where the mandatory requirements are exceeded, will be included in technical scores where appropriate. The mandatory project requirements are listed below.

4.2.2.1. The proposed project timeline must be provided with key goals and objectives within the first sixty (60) working days following award of a contract.

4.2.2.2. The proposed plan must comply with applicable West Virginia state and federal laws.

Verizon Response: Verizon has read, understands, and will comply.

The Verizon Project Plan that we will use for the CRP engagement will include;

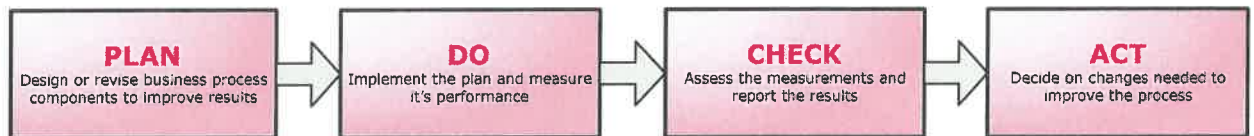
- *Project Schedule (Milestones/Interdependencies)*
- *Project Change Management (Schedules/Contractual Documents)*
- *Risk Management Plans*
- *Issues and Actions Management Tracking*
- *Executive and Operational Progress Reporting*
- *ITIL Process Integration*
- *Communications Plans and Responsibilities*

To complete the development of the Program Architecture that will support the WVOT program and Governance processes the following steps will be taken;

- *Develop a program schedule architecture and joint management and reporting framework that satisfy all stakeholders.*
- *Summarize at a program milestone based level for Governance*
- *Have highly visible and integrated risk management and tactical action planning process*
- *Agree upon reporting cadence at governance layers (Weekly/Monthly, etc.)*
- *Agree on change management process and approvals*
- *Agree on progress reporting formats that meet WVOT Governance requirements*

Process Management Progression

Contained within each of the Project Management Method is the Process Management Progression, the cycle of plan-do-check-act is the underlying concept for the interaction. This is the approach the Verizon recommends in our engagement with the State and its Agencies.



Process Management Prgression

Integrated into the Process Management Progression is Management by Objectives, the process of agreeing upon objectives within an organization so that management and employees buy into and understand the objectives so as to align the project objectives with the organizational objectives.

The Project Management Method and the Process Management Progression comes together with the ITIL Change, Release and Configuration process. The Project Management Methodology is supported via tools that produce and track project resources, documents and deliverables.

Our team has reviewed the requirements of the CRP program development project and are confident that we can meet and exceed the described Mandatory Project Requirements working with the State's team of Information Security professionals.

For additional information on Verizon's approach to the Project Management approach that we propose for the CRP Project with the State of West Virginia please see Exhibit 2 – Verizon Project Management Approach

4.2.2.3. Vendor must agree the Cyber Risk Program adhere to the following:

- 4.2.2.3.1.** The program must enable a 3-tiered organizational hierarchy allowing for cyber risk ownership to be assigned to a single government organization (agency), a collection of government agencies (department) and the collection of government departments (state)

Verizon Response: Verizon is prepared to assist in the development of the described 3-tiered organizational hierarchy for Cyber Risk Program. For further details of Verizon's approach and methodology to CRP please see Exhibit 3 – Verizon Cyber Risk Management Program Service Description

- 4.2.2.3.2.** The program must account for the standardization of the impact risk variable.

Verizon Response: The development of a CRP program will include the standardization of not only the risk variables but also include the development of standard criteria for classifying risk and ensuring that a standard process will yield consistent results. Please refer to Exhibit 3 Service Description for additional details.

- 4.2.2.3.3.** The program must include the capability to leverage both qualitative and quantitatively risk assessments and provide recommendations how to effectively and efficiently leverage both.

4.2.2.4. Vendor must agree that all documentation and materials associated with the development and implementation of the Cyber Risk Program are owned by the State of West Virginia.

4.2.2.5. Vendor must agree to base the project on an industry standard framework, such as the Cybersecurity Framework, selected by the State of West Virginia.

Verizon Response: Verizon has read, understood, and will comply. Verizon will work with the State of West Virginia to select the most appropriate industry standard framework to utilize for the CRP program. Verizon will utilize its CRP program and framework methodology as a baseline model to develop WVOT's CRP program.

REQUEST FOR PROPOSAL

CRFP ISC200000001

WVOT - Cyber Security Program

4.3. Qualifications and Experience: Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives were and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.

4.3.1. Qualification and Experience Information: Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below.

4.3.1.1. Vendor should specify previous experience in deploying and developing Cyber Security Risk Programs, preferably with government organizations. Vendor should include the scope of programs implemented. Vendor should also include any contacts at the specified entity who can be contacted for verification.

Verizon Response: Verizon has clients in the financial, healthcare, manufacturing, hospitality, as well as, public sector. Our Cyber Risk Programs are effective in any/all markets and regardless of size & complexity.

We can either use our platforms/tools to deliver or particularly with many of our large & "mature" that have already invested in other vendor platforms/tools, we can make use of those and in many cases, enhance the value to clients of those tools/platforms.

We currently also deliver Cyber Risk Programs to several States and their specific agencies within the State Governments. In Q4 2019, we will be available on the Federal Government schedules and are already in discussions with US government agencies on using our Cyber Risk Programs. (Verizon Q4 2019 = FedGov Q1 2020).

4.3.1.2. Vendor should list all references and/or examples for previous experiences in deploying and creating Cyber Security Risk Programs. Vendor should include any applicable documentation pertaining to these Cyber Security Risk Programs.

4.3.1.3. Vendor should provide resumes for staff that will be responsible for overseeing and completing the work on this contract.

4.3.1.4. Vendors should provide staff with the appropriate background, education, and experience to address all components and phases of the project. Please see attachment C –Sample Resumes for additional details on background, educations, and experience.

Verizon Response: Attached please find copy of the PS Principal's resume for whom we are proposing to lead the CRM engagement, see Exhibit 4. Verizon HR policy prevents us from sharing PII during RFI/RFP responses. We will provide the name and full background of both the Principal Consultant and Project Manager (both of whom have performed similar work for State agencies and clients adopting Cyber Risk Programs to follow upon award. Most of the consultants have been providing services to State Agencies since 2015.

Please see Exhibit 6 – Jeff Cornelius Resume

4.3.2. Mandatory Qualification/Experience Requirements -The following mandatory qualification/experience requirements must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it meets the mandatory requirements and include any areas where it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications/experience requirements are listed below.

4.3.2.1. Vendor must have fully implemented a Cyber Risk management program within an organization of similar size and complexity or larger.

Verizon Response: Verizon has implemented the Verizon Cyber Risk Program (CRP) to both commercial and SLED organizations over the past decade. Among the organizations we have implemented are clients of varying size and complexity, including international/multi-national company's locations in over 30 countries, and organizations with their own platforms and organizations where we provide the tools & platforms. Most clients have corporate policies that prevent them being used as a reference client for their own security.

See anonymized CRP customer references above.

REQUEST FOR PROPOSAL

CRFP I SC2000000001

WVOT - Cyber Security Program

4.4. Oral Presentations (Agency Option): The Agency has the option of requiring oral presentations of all Vendors participating in the RFP process. If this option is exercised, it would be listed in the Schedule of Events (Section 1.3) of this RFP. During oral presentations, Vendors may not alter or add to their submitted proposal, but only clarify information. A description of the materials and information to be presented is provided below:

Materials and Information Requested at Oral Presentation:

4.4.1.1. The vendor will discuss their approach for developing a comprehensive implementation plan or "roadmap" that sets out goals, identifies priorities, and provides a process for managing and measuring progress.

4.4.1.2. The vendor will discuss each phase or major milestone listed in the following paragraphs and subparagraphs: 1.2.1.1-1.2.1.7

4.4.1.3. The State will ask clarifying questions regarding the Vendor's submitted technical response.

4.4.1.4. Oral Presentations will be conducted at the Agency's facility provided by the Agency. Vendors should plan to provide their own media and demonstration hardware and, if preparing handouts, should prepare a number equal to the number of convenience copies of their Proposals supplied on the Bid Opening Date, unless specifically advised by the Agency otherwise.

Verizon Response: Verizon has read and understood.

SECTION 5: VENDOR PROPOSAL

5.1. Economy of Preparation: Proposals should be prepared simply and economically providing a concise description of the items requested in Section 4. Emphasis should be placed on completeness and clarity of the content.

5.2. Incurring Cost: Neither the State nor any of its employees or officers shall be held liable for any expenses incurred by any Vendor responding to this RFP, including but not limited to preparation, delivery, or travel.

5.3. Proposal Format: Vendors should provide responses in the format listed below:

5.3.1. Two-Part Submission: Vendors must submit proposals in two distinct parts: technical and cost. Technical proposals must not contain any cost information relating to the project. Cost proposal must contain all cost information and must be sealed in a separate envelope from the technical proposal to facilitate a secondary cost proposal opening.

5.3.2. Title Page: State the RFP subject, number, Vendor's name, business address, telephone number, fax number, name of contact person, e-mail address, and Vendor signature and date.

REQUEST FOR PROPOSAL

CRFP ISC200000001

WVOT - Cyber Security Program

5.3.3. Table of Contents: Clearly identify the material by section and page number.

5.3.4. Response Reference: Vendor's response should clearly reference how the information provided applies to the RFP request. For example, listing the RFP number and restating the RFP request as a header in the proposal would be considered a clear reference.

5.3.5. Proposal Submission: All proposals must be submitted to the Purchasing Division prior to the date and time stipulated in the RFP as the opening date. All submissions must be in accordance with the provisions listed in Section 2: Instructions to Bidders Submitting Bids.

Verizon Response: Verizon has read and understood.

REQUEST FOR PROPOSAL

CRFP ISC200000001

WVOT - Cyber Security Program

SECTION 6: EVALUATION AND AWARD

6.1 Evaluation Process: Proposals will be evaluated in two parts by a committee of three (3) or more individuals. The first evaluation will be of the technical proposal and the second is an evaluation of the cost proposal. The Vendor who demonstrates that it meets all of the mandatory specifications required, attains the minimum acceptable score and attains the highest overall point score of all Vendors shall be awarded the contract.

6.2. Evaluation Criteria: Proposals will be evaluated based on criteria set forth in the solicitation and information contained in the proposals submitted in response to the solicitation. The technical evaluation will be based upon the point allocations designated below for a total of 70 of the 100 points. Cost represents 30 of the 100 total points.

Evaluation Point Allocation:

Project Goals and Proposed Approach (§ 4.2)	
Approach & Methodology to Goals/Objectives (§ 4.2.1)	(40) Points Possible
Approach & Methodology to Compliance with Mandatory Project Requirements (§ 4.2.2)	(5) Points Possible
Qualifications and experience (§ 4.3)	
Qualifications and Experience Generally (§ 4.3.1)	(10) Points Possible
Exceeding Mandatory Qualification/Experience Requirements (§ 4.3.2)	(5) Points Possible
<u>Oral interview (§ 4.4)</u>	(10) Points Possible
<u>Total Technical Score:</u>	<u>70 Points Possible</u>
<u>Total Cost Score:</u>	<u>30 Points Possible</u>
Total Proposal Score:	100 Points Possible

REQUEST FOR PROPOSAL

CRFP ISC2000000001

WVOT - Cyber Security Program

6.3. Technical Bid Opening: At the technical bid opening, the Purchasing Division will open and announce the technical proposals received prior to the bid opening deadline. Once opened, the technical proposals will be provided to the Agency evaluation committee for technical evaluation.

6.4. Technical Evaluation: The Agency evaluation committee will review the technical proposals, assign points where appropriate, and make a final written recommendation to the Purchasing Division.

6.5. Proposal Disqualification:

6.5.1. Minimum Acceptable Score ("MAS"): Vendors must score a minimum of 70% (49 points) of the total technical points possible in order to move past the technical evaluation and have their cost proposal evaluated. All vendor proposals not attaining the MAS will be disqualified.

6.5.2. Failure to Meet Mandatory Requirement: Vendors must meet or exceed all mandatory requirements in order to move past the technical evaluation and have their cost proposals evaluated. Proposals failing to meet one or more mandatory requirements of the RFP will be disqualified.

6.6. Cost Bid Opening: The Purchasing Division will schedule a date and time to publicly open and announce cost proposals after technical evaluation has been completed and the Purchasing Division has approved the technical recommendation of the evaluation committee. All cost bids received will be opened. Cost bids for disqualified proposals will be opened for record keeping purposes only and will not be evaluated or considered. Once opened, the cost proposals will be provided to the Agency evaluation committee for cost evaluation.

The Purchasing Division reserves the right to disqualify a proposal based upon deficiencies in the technical proposal even after the cost evaluation.

REQUEST FOR PROPOSAL

CRFP ISC200000001

WVOT - Cyber Security Program

6.7. Cost Evaluation: The Agency evaluation committee will review the cost proposals, assign points in accordance with the cost evaluation formula contained herein and make a final recommendation to the Purchasing Division.

Cost Evaluation Formula: Each cost proposal will have points assigned using the following formula for all Vendors not disqualified during the technical evaluation. The lowest cost of all proposals is divided by the cost of the proposal being evaluated to generate a cost score percentage. That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.

Step 1: $\text{Lowest Cost of All Proposals} / \text{Cost of Proposal Being Evaluated} = \text{Cost Score Percentage}$

Step 2: $\text{Cost Score Percentage} \times \text{Points Allocated to Cost Proposal} = \text{Total Cost Score}$

Example:

Proposal 1 Cost is \$1,000,000
Proposal 2 Cost is \$1,100,000
Points Allocated to Cost Proposal is 30

Proposal 1: Step 1 – $\$1,000,000 / \$1,000,000 = \text{Cost Score Percentage of } 1 (100\%)$
Step 2 – $1 \times 30 = \text{Total Cost Score of } 30$

Proposal 2: Step 1 – $\$1,000,000 / \$1,100,000 = \text{Cost Score Percentage of } 0.909091 (90.9091\%)$
Step 2 – $0.909091 \times 30 = \text{Total Cost Score of } 27.27273$

6.8. Availability of Information: Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

Verizon Response: Verizon has read and understood.

REQUEST FOR PROPOSAL
CRFP ISC2000000001
WVOT – Cyber Security Program

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Verizon Business Network Svc Inc on behalf of MCI Communications Svc Inc

d/a/a Verizon Business Servies

(Company)

OBI ROMAINE - SNR ANALYST

(Representative Name, Title)

304-356-3395/304-356-3590

(Contact Phone/Fax Number)

08/27/2019

(Date)

REQUEST FOR PROPOSAL

CRFP ISC2000000001

WVOT - Cyber Security Program

Attachment A: Cost Sheet

A.1 Payment Terms

A.1.1. An amount representing ten percent (10%) of the contract resulting from this RFP for the Cyber Security Risk Program line item one (1) shall be withheld by the State. Upon formal acceptance by the State of the Cyber Security Risk Program, the State will release the retainage. Upon termination of the contract for reasons other than awarded vendor's uncured material breach of Contract, retained fees for accepted work will be released.

A.2 Payment Milestones

A.2.2. The payment milestones are based upon specific Deliverables and will be invoiced as completed. The payment milestones are listed below (A.2.2.1 through A.2.2.8); each milestone will have ten percent (10%) retainage held. Item Deliverable(s) and retainage where applicable will be detailed on each invoice. The awarded vendor will be authorized to invoice the State based upon acceptance of the deliverables as shown below; once the State has accepted the Deliverable(s) related to a payment milestone.

A.2.2.1 Developed information security framework

A.2.2.2 Reporting templates

A.2.2.3 Program roadmap

A.2.2.4 Third-party procurement solicitations quantity two (2)

A.2.2.5 Implementation of governance tool

A.2.2.6 Agency roll-out plan

A.2.2.7 Policies and operations procedures

A.2.2.8 Assessment results

REQUEST FOR PROPOSAL

CRFP ISC2000000001

WVOT – Cyber Security Program

A.3 Post Implementation Hourly Consultant Rate

A.3.3. The Post Implementation Hourly Consultant Rate (item two (2) of the Attachment A: Cost Sheet) must be a single hourly rate that will be billed for all staff time and is to be used to consult with vendor staff on unforeseen issues related to the Cyber Risk Program that may arise after the Cyber Risk Program has been successfully implemented. Requests to use the Implementation Consultant Hours must be outlined in a SOW (Statement of Work) and include both the problem and required number of hours to address the problem, and must be executed by an authorized representatives of both Parties. The Post Implementation Consultant Hours will not be allowed to exceed one-thousand (1,000) hours.

Verizon Response: Verizon has read and understood.



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

State of West Virginia
 Request for Proposal
 10 – Consulting

Proc Folder: 609025

Doc Description: Addendum 1-Cyber Security Program RFP (OT19152)

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-07-30	2019-08-29 13:30:00	CRFP 0210 ISC2000000001	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:
 Verizon Business Network Svc Inc., on behalf MCI Communications Services Inc. d/b/a
 Verizon Business Services
 4700 MacCorkle Av SE, Charleston WV 25304
 304-356-3395

FOR INFORMATION CONTACT THE BUYER

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

Signature X *Obi Oromane* FEIN # 47-0751768 DATE *08/27/2019*

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

ADDITIONAL INFORMATION:

Addendum

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

 The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code 5A-3-10b, for the West Virginia Office of Technology (hereinafter referred to as the "Agency") to establish a Cyber Security Risk Program per attached documents.

NOTE: Online responses to this solicitation are prohibited. Please see the Instructions to Bidders in Section 2 for proposal submission.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Cyber Security Risk Program	1.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description :
 Cyber Security Risk Program

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Post Implementation Consultant	1000.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description :
 Post Implementation Consultant

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Mandatory Pre-Bid is being removed per Addendum 01.	2019-08-01
2	Question Deadline by 4:00 pm	2019-08-19

SOLICITATION NUMBER: CRFPISC2000000002

Addendum Number: No.01

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

Applicable Addendum Category:

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

Description of Modification to Solicitation:

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

1. The purpose of this addendum is to remove the Mandatory Prebid requirement from the solicitation.

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

INSTRUCTIONS TO VENDORS SUBMITTING BIDS

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

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

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

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

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

All Vendors submitting a bid must attend the mandatory pre-bid meeting. Failure to attend the mandatory pre-bid meeting shall result in disqualification of the Vendor's bid. No one person attending the pre-bid meeting may represent more than one Vendor.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. The State will not accept any other form of proof or documentation to verify attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing.

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

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

Questions submitted at least five business days prior to a scheduled pre-bid will be discussed at the pre-bid meeting if possible. Any discussions or answers to questions at the pre-bid meeting are preliminary in nature and are non-binding. Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: _____

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

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

Addendum Numbers Received:

(Check the box next to each addendum received)

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

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

Verizon Business Network Svc Inc, on behalf MCI
Communication Svc Inc d/b/a Verizon Business Services

Company

Obi W. Lorraine

Authorized Signature

08/27/2019

Date

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

Revised 6/8/2012



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

State of West Virginia
 Request for Proposal
 10 — Consulting

Proc Folder: 609025

Doc Description: Addendum 2-Cyber Security Program RFP (OT19152)

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-08-21	2019-08-29 13:30:00	CRFP 0210 ISC2000000001	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:

Verizon Business Network Svc Inc on behalf of MCI Communications Svc Inc d/b/a
 Verizon Business Services
 4700 MacCorkle Av SE Charleston WV 25304
 304-356-3395

FOR INFORMATION CONTACT THE BUYER

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

Signature X

FEIN #

47-0751768

DATE

08/27/2019

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 Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code 5A-3-10b, for the West Virginia Office of Technology (hereinafter referred to as the "Agency") to establish a Cyber Security Risk Program per attached documents.

NOTE: Online responses to this solicitation are prohibited. Please see the Instructions to Bidders in Section 2 for proposal submission.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Cyber Security Risk Program	1.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description :
Cyber Security Risk Program

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Post Implementation Consultant	1000.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description :
Post Implementation Consultant

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Mandatory Pre-Bid is being removed per Addendum 02	2019-08-01
2	Question Deadline by 4:00 pm	2019-08-19

SOLICITATION NUMBER: CRFP ISC2000000001

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 all technical questions received.

No additional changes.

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

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.
2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

CRFP ISC20000001
Cyber Security Program
Vendor submitted Questions and Agency Responses
08/19/2019

Q 1. Proposal Reference: Section 4.2.1.4 Governance, Risk, & Compliance (GRC) Tool Solicitation
Section 4.2.1.4.1, Section 4.2.1.4.2

Relevant Proposal Content: In 4.2.1.4, WV states, "Vendor should assist WVOT in developing a solicitation to obtain a GRC tool..." "Ultimately, the tool solicitation should be focused on the procurement and implementation of a tool designed to directly support the Cyber Risk Service."

In 4.2.1.4.1, WV states, "(Vendor will not be permitted to bid on this solicitation it helps to develop and is also prohibited from serving as a subcontractor to the vendor that is awarded a contract thereunder.)"

In 4.2.1.4.2, WV states, "Implement the governance tool to support future assessment."

Question: The Section 4.2.1.4.1 guidance cited, advising the vendor assisting with developing a GRC Tool solicitation is not permitted to bid on that solicitation or serve as a subcontractor to the vendor awarded the subsequent contract, contradicts the Section 4.2.1.4 and Section 4.2.1.4.2 guidance cited, advising the vendor should assist in developing a GRC Tool solicitation and implement it.

A 1. The State is looking for the winning vendor to assist in implementing the policies and procedures for the GRC tool and how it works into the Cyber Risk Program. Not implement the tool from a technical perspective. The specifications will not be modified.

Q 2. Proposal Reference: Section 4.3

Relevant Proposal Content: In section 4.3, WV states "Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives where and how they were met.)"

A 2. The Project Manager responsible for managing the similar project that the vendor implemented.

Q 3. Proposal Reference: Section 4.1.3.2

Relevant Proposal Content: In section 4.1.3.2, WV states "Vendor should list all references and/or examples for previous experiences in deploying and creating Cyber Security Risk Programs. Vendor should include any applicable documentation pertaining to these Cyber Security Risk Programs."

Question: How many client references need to be included in the response?

A 3. There is no set number. A number which shows that the Vendor is competent in building Cyber Risk Programs.

CRFP ISC20000001
Cyber Security Program
Vendor submitted Questions and Agency Responses
08/19/2019

<p>Q 4. Section 4.3.2.1 mentions “Vendor must have <u>fully implemented</u> a Cyber Risk management program within an organization of similar size and <u>complexity</u> or larger.” Can you better describe what is meant by "fully implemented" as well as organization "complexity"? It appears that if the vendor has not performed services the meet this criteria, then we will be disqualified from this RFP, is that correct?</p>
<p>A 4. The term “Fully Implement” means the Vendor managed the project from planning to implementation and then successfully left the project in a position where the client could move forward by themselves.</p>
<p>Q 5. Would the West Virginia Department of Administration extend the due date out to September 12, 2019?</p>
<p>A 5. No</p>
<p>Q 6. What is the makeup of stakeholders/decision makers? How are the agencies represented? What is the intention of key stakeholder feedback and input into the program? How does WVOT envision soliciting feedback from supported agencies?</p>
<p>A 6. Stakeholders would be identified by the Vendor plan. Examples: Agency Directors or designees, technical staff, and business-level staff.</p>
<p>Q 7. Is the winning vendor expected to interact directly with each of the 210 entities?</p>
<p>A 7. No.</p>
<p>Q 8. Is there an estimate of the number of critical assets in each agency?</p>
<p>A 8. No</p>
<p>Q 9. Are most agencies and locations in the Charleston area?</p>
<p>A 9. Yes, headquarter locations are in Charleston. However, some agencies have regional offices/locations.</p>
<p>Q 10. Can you estimate the number of business processes for each agency?</p>
<p>A 10. No</p>
<p>Q 11. Of the 200 “services” employees, how many are responsible for security?</p>
<p>A 11. Twelve (12)</p>
<p>Q 12. In Section 4.2.1.1.3, what is meant by “tiering”? Does this mean consideration for small, medium, and large entities?</p>
<p>A 12. Tiering should be based off size (small, medium, large agencies) as well as the amount of critical systems an agency might have. Some agencies have no critical systems or data, while others have a large volume.</p>
<p>Q 13. Please provide an approximate number of West Virginia state’s departments and agencies that this Cyber Risk Program will apply to?</p>

CRFP ISC20000001
Cyber Security Program
Vendor submitted Questions and Agency Responses
08/19/2019

A 13. All Departments and agencies within the Executive branch. That's approximately 8 departments and 208 subsequent agencies within the departments.
Q 14. If possible, based the list of departments and agencies, how many are large versus small (approx. number / percentage split)? (for e.g., in terms of number of enterprise applications, number of IT assets, number of employees, number of end-users, etc.)
A 14. Unable to determine that information. General statistics on agency staffing can be found on their individual websites. A directory and organizational chart can be found at https://www.wv.gov/Pages/StateGovernmentDirectory.aspx
Q 15. Does WVOT already have an existing / documented IT risk or cyber security risk management methodology of some sort?
A 15. No
Q 16. Does WVOT's cyber risk program need to align with or conform to specific industry standards such as NIST SP-800 series, ISO 27000 family, etc.? Please provide details, if relevant.
A 16. The State is looking at the vendor to recommend which framework should be followed. See 4.2.1.1.
Q 17. Would the Cyber Risk Program also expect Vendor to perform any technical assessments / testing as well to identify vulnerabilities and determine technical risks? (Examples include: vulnerability assessments, penetration testing, physical site reviews, etc.)
A 17. No
Q 18. Does WVOT currently have and maintain an IT risk register of some sort? Is it centralized or siloed? Please provide relevant details.
A 18. No
Q 19. Does WVOT have a dedicated team (or personnel) to run (execute) the Cyber Risk Program? If yes, approx. how many full-time employees is the team made up of? - please provide relevant details.
A 19. Currently there are 4 full-time staff devoted to the project, but WVOT does anticipate more based on recommendations by the Vendor
Q 20. Does WVOT expect Vendor to also support and execute on the Cyber Risk Program post Go-Live? (e.g. staff augmentation)
A. 20. The ultimate goal is for WVOT staff to maintain the program at the close of the project.
Q 21. In addition to ongoing risk reporting and dashboards, what other levels of periodic reporting and ongoing monitoring is expected:

CRFP ISC200000001
Cyber Security Program
Vendor submitted Questions and Agency Responses
08/19/2019

<p>Within WOT? Outside WVOT, i.e. non-IT stakeholders? Please provide details.</p>
<p>A 21. Would be dependent on the recommendation of the Vendor and the Project Plan.</p>
<p>Q 22. Does WVOT already have an existing controls framework? If yes, is the framework and controls library based on an industry standard such as NIST SP 800-53? Please provide details.</p>
<p>A 22. WVOT uses NIST SP 800-53 but the process is not formalized.</p>
<p>Q 23. Does WVOT already have existing Information Security (or Cyber Risk) policies and associated standards, guidelines, etc. documented? i.e., Will Vendor be expected to revise and/or refine existing policy documentation, or develop new policy documentation from scratch?</p>
<p>A 23. All policies can be found at https://technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx</p>
<p>Q 24. For Policy Management, is there already an existing workflow(s) for periodic policy review and approvals (e.g., for creating, updating, deleting, accepting/rejecting, and publishing policies content), or do workflows need to be developed?</p>
<p>A 24. See PO1000 on https://technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx</p>
<p>Q 25. Approx. how many stakeholders (including teams, titles, and roles) will need to be engaged during the policy review, finalization, and publishing phase?</p>
<p>A 25. This question depends on the Vendor's recommended communication plan.</p>
<p>Q 26. Is third party risk management, including assessments of WV's third-party suppliers considered in scope for this RFP?</p>
<p>A 26. No</p>
<p>Q 27. Does WVOT already have an existing third-party risk management (also called, supplier risk management) framework with defined components, including vendor tiers, triage mechanism, assessment schedule, etc.?</p>
<p>A 27. No</p>
<p>Q 28. Does WVOT already have third party assessment questionnaires (such as risk assessment questionnaires) documented; else, will such questionnaires need to be developed as part of the implementation scope?</p>
<p>A 28. WVOT currently has none. These templates would need developed.</p>
<p>Q 29. Does WVOT currently have an authoritative IT Asset Inventory in place?</p>

CRFP ISC20000001
Cyber Security Program
Vendor submitted Questions and Agency Responses
08/19/2019

A 29. No
Q 30. Is the WVOT IT Asset Inventory centralized or siloed at this time?
A 30. Each agency has their own inventory system.
Q 31. What solution/tool/platform does WVOT currently use for its IT Asset Inventory or CMDB (config. mgmt. database)?
A 31. Microsoft CRM, Oasis
Q 32. Have the assets already been classified into levels / values of some sort, based on criticality or risk?
A 32. No
Q 33. What technology platform / tool does WVOT currently have and use for system patch management and configuration management?
A 33. Microsoft SCCM
Q 34. Does WVOT or any of its larger agencies already own/use a GRC solution / tool / platform?
A 34. No
Q 35. To confirm, "Vendor will not be permitted to bid on the GRC Tool solicitation", i.e. GRC tool product software, licenses, resell, etc. Is this correct? [Ref: 4.2.1.4.1]
A 35. Yes
Q 36. If yes to the above question, Vendor will need to make assumptions for estimating the level of effort required to implement / configure / customize a typical GRC tool, fully knowing that actual implementation efforts may change depending on the selection and procurement of a specific tool.
A 36. The State is looking for the winning vendor to assist in implementing the policies and procedures for the GRC tool and how it works into the Cyber Risk Program. Not implement the tool from a technical perspective.
Q 37. To confirm, WVOT is still requesting Vendor to be able to "Implement the governance tool", i.e., consulting, system integration, configuration, professional services, and training / knowledge transfer, etc. Is this correct? [Ref: 4.2.1.4.2, .3, .4, and .5]
A 37. The State is looking for the winning vendor to assist in implementing the policies and procedures for the GRC tool and how it works into the Cyber Risk Program. Not implement the tool from a technical perspective.

CRFP ISC200000001
Cyber Security Program
Vendor submitted Questions and Agency Responses
08/19/2019

Q 38. Is WVOT also expecting Vendor to provide steady state maintenance and support for the GRC tool post Go-Live, i.e. “managed GRC”?
A 38. No.
Q 39. In CFRP RFP Section 4.2 Project Goals and Mandatory Requirements, paragraph 1 it states, “The framework must align with the cyber risk posture assessment program, enabling an “apples to apples” analysis for executive leadership. <ul style="list-style-type: none"> o What are the details on your current “cyber risk posture assessment program”?
A 39. We currently do not have a program. The framework established must fit with the whole risk program being created by the vendor.
Q 40. Do you have a definition of a Critical Information Asset or is the vendor expected to provide?
A 40. Vendor should refine it based on input from WVOT, but yes, the Vendor will qualify the term.
Q 41. What regulatory requirements do you have to be compliant with?
A 41. Multiple agencies have different requirements: IRS 1075, CJIS, PCI, SSA
Q 42. Do you have a current security framework that you are leveraging?
A 42. The State is looking at the vendor to recommend which framework should be followed. See 4.2.1.1. (A16) WVOT uses NIST SP 800-53 but the process is not formalized. (A22)
Q 43. Is there a current risk management program in place? Are there defined and documented policies and procedures (either enterprise or local) in place supporting the program in place?
A 43. All policies can be found at https://technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx
Q 44. Are current cyber policy and procedures developed and managed at an enterprise level, agency specific or a combination of the two. Is there a single authorizing agency for all policies and procedures?
A 44. WVOT and the Cybersecurity Office has authority to issue technology and cyber risk policies and procedures
A 45. Is a listing of security products currently within the environment available? Are there products to work with the GRC product solicitation defined in 4.2.1.4 or is product to be acquired to be ‘stand-alone’?
A 45. The winning Vendor will help the State make that determination.
Q 46. How many locations will be in scope?

CRFP ISC20000001
Cyber Security Program
Vendor submitted Questions and Agency Responses
08/19/2019

A 46. Physical locations? Unknown. Primarily, most agency headquarters are located in Charleston, WV.
Q 47. How many external Assessment: How many live Active External IP Addresses? (Please don't enter a "class C" or a Range - we need # of active IP's)
A 47. Not known/Not Applicable
Q 48. How many External Web Applications?
A 48. Not known/Not Applicable
Q 49. Number of Internal Assessment: How many live/Active Internal IP Addresses?
A 49. Not known/Not Applicable
Q 50. How many Email Domains in scope?
A 50. Not known/Not Applicable
Q 51. How many Perimeter Firewalls in scope?
A 51. Not known/Not Applicable
Q 52. How many Physical Assessment locations?
A 52. Not known/Not Applicable
Q 53. How many Wireless Assessment locations?
A 53. Not known/Not Applicable
Q 54. End Point Assessment: How many End Users/Devices for Policy Compliance?
A 54. See Section 4.1 of the RFP
Q 55. How many individual Policy, Process & Procedure Assessments are required?
A 55. Vendor will make recommendations
Q 56. Is WVOT seeking to host all their own tools/platforms or would a full managed solution such as the Verizon Risk Report or the Verizon Cyber Risk Program which can be customized to fit a clients needs including use of client owned tools and platforms be considered?
Q 56. This RFP is to find a vendor that will plan for, create, implement and ultimately turnover to WVOT personnel the Cyber Risk Program, as stated in Section 4.2.

**CRFP ISC20000001
Cyber Security Program
Vendor submitted Questions and Agency Responses
08/19/2019**

Q 57. Is the objective of the WVOT CRP to be both a Risk and Compliance program? These are normally treated as separate assessment program types and just want to clarify.
A 57. Risk is the primary objective.
Q 58. Section 4.2.2.5 describes “an industry standard framework, such as the Cybersecurity Framework, selected by the State of West Virginia.” Is there a Standard Framework that WVOT has selected or adheres to?
A 58. The State is looking at the vendor to recommend which framework should be followed. See 4.2.1.1. (A16) WVOT uses NIST SP 800-53 but the process is not formalized. (A22)
Q 59. Section 4.2.2.3.1 and 4.2.2.3.2 appear to be a “parent-child” hierarchy. For reporting and risk scoring is there a requirement for individual agencies and department level scores and recommendations, OR are you all seeking a single score?
A 59. Agency and department level scores, as well as a collective score/recommendation for the Enterprise.
Q 60. Also, should each agency have access to only their information and only the “parent” have access to all data/info, so there are specific agency/dept reports as well as an overall WVOT reporting? And are the requirements across all agencies the same, OR are there different compliance and risk requirements based on agency functions?
A 60. Each agency is different, has their own set of regulations, and information collected should remain confidential to other agencies being assessed.
Q 61. Are the Assessment time frames/cycles/inspection cadence the same for all WVOT agencies?
A 61. Determined by the proposal.
Q 62. Does WVOT have any specific qualifications, experiences, etc. that you are seeking from your vendor selection?
A 62. Yes, listed in the “Qualifications and Experience” section.
Q 63. When will answers to question be released? Will an extension be granted to allow vendors time to scope based on those answers?
A 63. No extensions

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: _____

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

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

Addendum Numbers Received:

(Check the box next to each addendum received)

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

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

Verizon Business Network Svc Inc on behalf MCI

Communications Inc d/b/a Verizon Business Services

Company

Obi W. Lomaine

Authorized Signature

08/27/2019

Date

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

Exhibit 1 – CRP Model of Example Offerings for Agency Charge Back

Cyber Risk Programs Sample Program Offerings Exhibit (TBD)

Cyber Risk Program - Risk Rating

**Reduced scope, designed for M&A, Partner/Vendor Assessments, base is focused on "outside-in" view.*

- **Risk Rating "Base"**
- External Vulnerability & Risk Assessment
- Web Application Vulnerability & Risk Assessment
- IP/Brand Reputational Assessment
- Netflow Assessment

- **Risk Rating "PLUS" – add any/all of:**
- Internal Vulnerability & Risk Assessment (LAN + DMZ)
- Endpoint System Assessment
- Firewall Assessment
- Email Filter Check
- Phishing Assessment
- Physical Inspection
- Wireless Risk Assessment (W/Bluetooth & IoT)
- Policy, Process and Procedure Assessment

Cyber Risk Program – Risk Assessment

**Full Risk Management program, designed to establish or enhance existing cyber security and risk initiatives*

- External Vulnerability & Risk Assessment
- Internal Vulnerability & Risk Assessment (LAN & DMZ)
- Web Application Vulnerability & Risk Assessment
- Endpoint System Assessment
- IP/Brand Reputational Assessment
- Netflow Assessment
- Firewall Assessment
- Phishing Assessment
- Email Filter Check
- Physical Inspection
- Wireless Risk Assessment (W/Bluetooth & IoT)
- Policy, Process and Procedure Assessment
- Executive Summary Risk Report

Add-On Assessment or Activities

**Optional program enhancements to meet your requirements*

- War Dial
- Compliance Reports (Adaptive Modeling)
- Site/Region/Location & Business unit Specific Reports
- Application Security Certification Program
- CRP Certification Available for Risk Assessment level
- *Cloud Security Assessment – Coming 2H 2019*

Exhibit 2 – Verizon Project Management Approach & Methods

Project Management

Verizon's Project Managers facilitate the implementation of our products and solutions by directing cross-functional teams representing multiple departments in the execution of implementation activities. This facilitation requires a multi-faceted approach to managing both internal and external resources in a coordinated manner, enabling efficient execution of activities by all parties. The Project Manager is responsible for the overall implementation of a project and serves as the single point of contact for you throughout the course of the project.

The Project Manager oversees and coordinates all aspects of a project. Projects are assigned to Project Managers based on their skills, experience, and availability. Project Managers may be assigned a variety of projects involving multiple types and combinations of products, services, technologies, and geographies and requiring the support and participation of various departments.

Our Project Management Methodology defines end to end responsibility for the delivery of your network. Aligned with the Credo, it promotes collaborative working with you to align and support the delivery of the network with your internal program and business objectives. The essence of the methodology is the successful set-up and execution of the project in collaboration with you.

Methodology Overview

Our Project Management function builds on the expertise and experience within the organization so that we can focus on effective solutions and professional implementation of your project. Project Managers are PMI and/or PRINCE2 qualified and have significant experience in leading and delivering large, complex global projects. The Project Management process starts at the point where a decision is made to bid on a project. The assigned Project Manager works in support of the Account Team to pre-plan the project and pull together all implementation and post implementation related inputs to the proposal. The Project Manager leads all of our activities in support of the project and is responsible for the final result. On completion of the project, the Project Manager hands off to the Account Manager and/or the Service Program Manager (as appropriate).

Project Management Responsibilities

The Project Manager facilitates the major phases of the project life cycle and key activities performed. These phases* include:

- **Initiating** – The Initiating phase consists of the activities performed to define a new project by obtaining authorization to start the project and to assign the Project Manager.
- **Planning** – The Planning phase consists of the critical up-front activities for the Project Manager to understand the total scope of the effort and to define the baseline set of plans, requirements, and timelines for executing the project.
- **Executing** – The Executing phase consists of activities performed by the project team to complete the work defined in the Project Plan to satisfy the project objectives.
- **Closing** – The Closing phase consists of the post-implementation activities performed to finalize deliverables across all project management process groups and formally close the project.

* Monitoring and Controlling activities are included throughout the above major phases. Monitoring and controlling is recognized as critical, iterative work efforts that require tracking, review, and regulation of the progress and performance of the project. Areas will be identified in which changes to the plan are required, and initiated the corresponding changes.

Project Management responsibilities during project delivery are shown below:

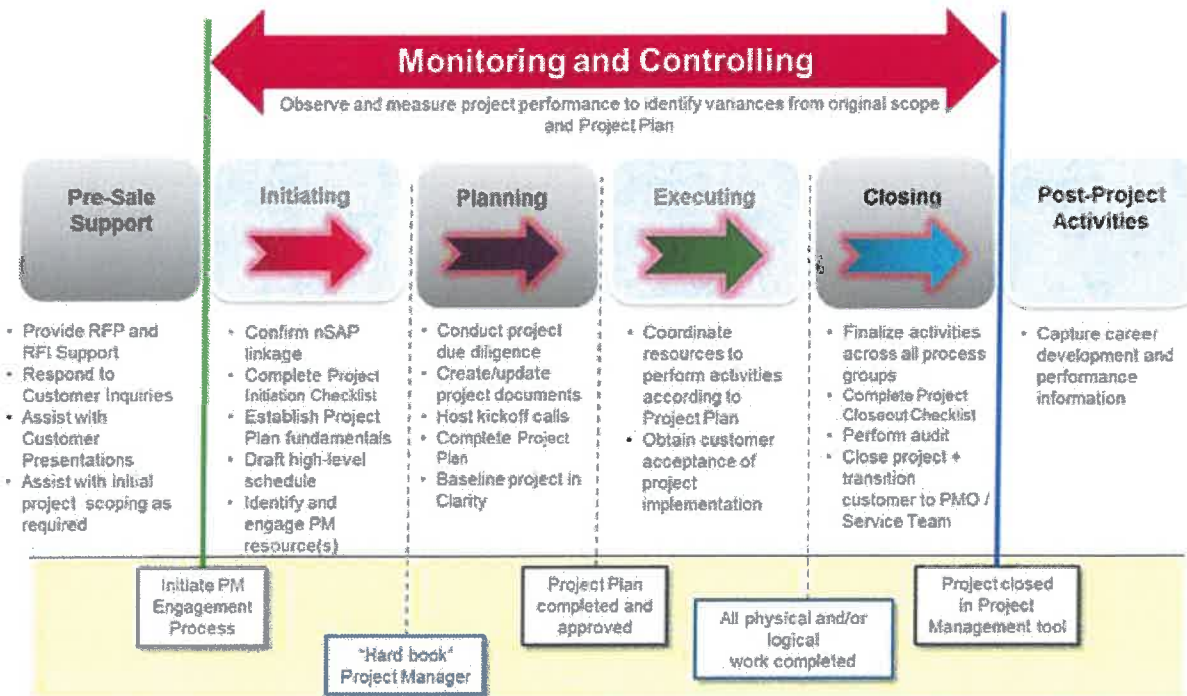


Figure 1 – Key PM Activities by Project Phase

Project Stages

The project life cycle is formally divided into stages that describe common activities as the project matures. Although all projects are unique, they do share common components or processes that are normally grouped together and these have been defined below:

Following is a high level overview of the project stages.

Initiation

There are a number of activities that occur within Project Management prior to the formal assignment of a Project Manager. These initial activities enable Project Management to prepare for pending projects ahead of time and to ensure that the right resources are available to implement the project. This preparation enables Project Managers to ramp up quickly when new projects are assigned to them. The activities include:

- Engage Project Management organization
- Apply project acceptance criteria
- Identify expedite projects
- Create/update project in Clarity
- Populate high-level Project Schedule
- Establish Project Plan Fundamentals
- Run Project Management Estimating Model
- Identify and engage Project Manager(s)
- Perform Gate Review – Initiating Phase

Planning

During the planning phase, the Project Manager performs a structured set of activities to plan and organize a project prior to implementation. These planning activities help lay the groundwork for successful project execution. The activities include:

- Conduct project due diligence
- Engage internal project resources
- Plan and conduct internal and external kickoff meetings

- Create/update Project Plan
- Obtain approval of Project Plan
- Baseline project in Clarity
- Perform Gate Review – Planning Phase

Executing

The Executing Phase in the project life cycle is focused primarily on managing the core project management activities. This phase commences after the Project Plan has been approved. Project Managers are responsible for ensuring that all project commitments are met on time and within the specified requirements established in your contract and Project Plan and that the project is implemented within the scope and requirements outlined in the Planning Phase.

The Project Manager develops and executes the activities in the agreed Project Schedule to deliver the contracted products using allocated resources.

The activities covered include:

- Execute Project Plan
- Obtain your acceptance of project implementation
- Perform Gate Review – Executing Phase

Monitoring and Control

While the activities and tasks are being planned and executed, a series of management processes is performed to monitor and to control the deliverables being produced by the project. Monitoring and Controlling activities are conducted throughout the project life cycle to track, to review, to measure, and to regulate project performance and progress, to identify and to document variances from the original scope, and to meet the performance objectives defined in the Project Plan. These activities include the identification of changes, risks, and issues, the review of deliverable quality, and the measurement of each deliverable being produced against the acceptance criteria.

The Project Manager is responsible for monitoring project progress and using the information gained to control the project delivery process and facilitate timely reporting. The iterative process of Monitoring and Controlling consists of:

- Reviewing the project schedule on a regular basis to determine how the project is progressing in terms of time/cost/quality
- Evaluating the impact of project change requests
- Updating the Project Schedule to show activity status and completion
- Determining whether there are activities that should be completed but have not been
- After each review and update of the schedule, determining whether the project will be completed within the original effort, cost, and duration; If not, determining the critical path and looking for ways to accelerate these activities to get back on track
- Monitoring the budget, if applicable; looking at the amount of money the projects have actually consumed and determining whether actual spending is more than originally estimated based on the work that has been completed
- Reviewing and updating risks and issues in Clarity on a regular basis (weekly, at minimum)

The activities covered include:

- Facilitate project calls
- Maintain project status and documentation
- Manage escalations
- Perform project Change Management and Governance

Close

When all physical and/or logical work on the project is complete and the Project Manager changes the project status to "Pending Bill Review", the project moves into the Closing Phase. Project Closure involves the release of final deliverables to you, the transition of project documentation and ongoing customer support to the Service Team/Program Management Office/Account Team, the possible termination of supplier contracts required during implementation, the release of project resources, and the communication of project closure to all stakeholders.

After all the activities in the "Pending Bill Review" status are completed, the project will be audited to ensure compliance to PM standards.

Post-Project Activities

Once the project is complete and transitioned to the Service Team, the Project Manager is responsible for supporting the overall Project Management organization by completing a series of knowledge management and professional development activities. While the execution of the core project management activities requires the majority of a Project Manager's time, the post-project knowledge management and professional development activities are equally important.

: :

Exhibit 3 – Verizon Cyber Risk Management Program Service Description

Verizon Cyber Risk Program Service Description

1. **Description of Service.** The Verizon Cyber Risk Programs are specifically designed to provide an objective review of an organization's ability to prepare for, recognize, and respond to today's threats. The programs consist of recurring activities that are designed to measure the effectiveness of cyber risk controls and identify potential weaknesses.

The Verizon Data Breach Investigations Report (DBIR) serves as the foundation of the Verizon Cyber Risk Programs. The Cyber Risk Programs use the threat scenarios and attack patterns identified in the DBIR to help create risk scores, which customers can then use to enhance their cyber security posture.

Underlying the DBIR is the Vocabulary for Event Recording and Incident Sharing (VERIS), a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. VERIS helps organizations understand what they need to know and what they need to measure to know it. The Cyber Risk Programs help organizations better understand each landscape through a set of cyber risk metrics that create knowledge and improve an organization's ability to make informed cyber risk decisions.

When providing consulting to organizations, such as the State of West Virginia, Office of Technology, to assist them in the build out their own Cyber Risk Management Program vs. purchase of the Verizon Cyber Risk Programs, Verizon will adapt another risk framework that meets the clients requirements, such as NIST or FAIR.

For custom & consulting programs, typically, the client is responsible for the purchase of the necessary tools, platforms & licensing to perform the assessment activities. Verizon can provide guidance and recommendations on tools/platforms selection, and may act as a re-seller of tools & platforms necessary to build out a program.

The program that we would consult developing with the State of West Virginia Office of the CTO would include the following Assessments and Reports.

- 1.1 **Cyber Risk Programs - Risk Assessment.** The Cyber Risk Programs - Risk Assessment is a periodic (Quarterly or Monthly) program that is reliable and pragmatic. Through a set of 12 recurring activities, the Risk Assessment provides an objective review of an organization's external and internal security postures as related to the most common Threat patterns. The Risk Assessment risk scores provide benchmark comparisons, references to the Verizon Data Breach Investigations Report (DBIR) database, known weaknesses (or vulnerabilities), and risk-reducing guidance.
- 1.2 **Cyber Risk Management Consulting and Custom Programs -** For consulting or custom programs, the risk scores and references will be made in relation to & in compliance with the framework(s) being required by the client for consulting and custom engagement.
 - 1.2.1 **Components.** The Cyber Risk Programs – Risk Assessment consists of critical analysis, insight, applicable cyber risk framework structure, and 12 cyber risk measurement activities:
 - External Vulnerability Assessment
 - IP Reputational Assessment
 - NetFlow Assessment
 - Web Application Assessment
 - Internal Vulnerability Assessment

- Email Filter Check
- Firewall Assessment
- End-Point System Assessment
- Phishing Assessment
- Wireless Assessment
- Physical Inspection
- Policy, Process, and Procedure Assessment

1.2.1.1 **External Vulnerability Assessment.** Conduct quarterly/monthly external Vulnerability assessments on prearranged dates and times. Scan specific Customer IP (CIP) addresses or a range of CIP addresses to discover active devices, identify operating systems, find open network ports and determine which services are running within those ports, and uncover vulnerabilities. The results of the assessment will be categorized in the following way:

- Active CIP – to understand the amount of active devices that are internet facing.
- Exploited vulnerabilities – to understand the amount of vulnerabilities in which intruders can easily gain control of the host.
- High severity vulnerabilities – to understand the amount of vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 7.0 or greater.
- Unexpected Services – to understand the amount of possible vectors that an intruder could use to gain access to the network.
- Moderate severity vulnerabilities – to understand the amount of vulnerabilities with a CVSS score of 4.0 to 6.9.

The results from the external risk assessment will be used to calculate a portion of the Risk Rating score and will be detailed in the quarterly/monthly Risk Rating report.

1.2.1.2 **IP Reputational Assessment.** Conduct quarterly/monthly IP reputational assessments within a predefined assessment window (such as a 15- or 30- day collection window). Analyze specific CIP addresses, CIP ranges, and/or Customer domain names within an internet based cyber analytic platform. The analysis will be based on a set of evolving use cases derived from emerging Threat conditions, such as registered fraud domains, disclosed incidents, watchlist hits, spam, and phishing activities. The results of the assessment will be categorized in the following way:

- Active CIP, CIP range, and/or Customer domain – to illustrate the Customer identifiers that were used within the assessment period.
- Exploit kit – to understand the volume of emerging exploit kits associated with the Customer identifiers.
- Exploitable vulnerabilities– to understand the volume of exploitable vulnerabilities associated with the Customer identifiers.
- Phishing and Malware – to understand the volume of phishing and malware spam associated with the Customer identifiers
- Negative Domain Mentions – to understand the volume of negative domain mentions associated with the Customer identifiers.

The results of the IP reputational assessment will be used to calculate a portion of the Risk Rating score and will be detailed in the quarterly Risk Rating report.

1.2.1.3 **NetFlow Assessment.** Conduct quarterly/monthly NetFlow assessments. Conduct a search to correlate CIP with NetFlow data (using public data available on the Internet) for a period of at least 15 days. The NetFlow assessment will identify the volume of:

- Command and control activity
- Spam and phishing activity
- Malicious site activity

The sole purpose of capturing routing and source/destination CIP information is to protect the Customer from potential abuses of services or unauthorized access to its information, systems and applications. The results of the NetFlow assessment will be used to calculate a portion of the Risk Rating score and will be detailed in the quarterly/monthly Risk Rating report.

1.2.1.4 **Web Application Assessment.** Conduct quarterly/monthly web application assessments on prearranged dates and times. Scan specific CIP addresses, a range of CIP addresses, and/or specific URLs to discover web application vulnerabilities and associated weaknesses. The results of the assessment will be categorized in the following way:

- Active Web Applications – to understand the amount of active web applications that are internet facing.
- Severity 5 Vulnerabilities – to understand the volume of vulnerabilities in which intruders can easily gain control of the application, including read and write access to files and remote execution of commands.
- Severity 4 Vulnerabilities – to understand the volume of vulnerabilities in which intruders can possibly gain control of the application or where there may be potential leakage of highly sensitive information.
- Severity 3 Vulnerabilities – to understand the volume of vulnerabilities in which intruders may be able to gain access to specific information stored within the application.

The results of the web application assessment will be used to calculate a portion of the Risk Rating score and will be detailed in the quarterly Risk Rating report.

1.2.1.5 **Internal Vulnerability Assessment.** Conduct quarterly/monthly authenticated internal Vulnerability assessments on prearranged dates and times. Scan specific Customer IP addresses or a range of Customer IP addresses to discover active devices, identify operating systems, and uncover vulnerabilities. The results of the assessment will be categorized in the following way:

- Active IP Addresses – to understand the amount of active devices within the internal network or networks.
- Exploited vulnerabilities – to understand the amount of vulnerabilities in which intruders can easily gain control of the host.
- High severity vulnerabilities – to understand the amount of vulnerabilities with a CVSS score of 7.0 or greater.
- End of Life Software – to understand the amount of systems that contain end-of-life software. End-of-life software is software that is no longer supported by the vendor, which means the vendor is no longer providing patches and service pack updates for Vulnerability remediation.
- Moderate severity vulnerabilities – to understand the amount of vulnerabilities with a CVSS score of 4.0 to 6.9.

The results from the internal Vulnerability assessment will be detailed in the quarterly Internal Vulnerability Assessment Report and used to calculate a portion of the Risk Assessment score.

Internal scanning includes provision of an Appliance which is hosted on Customer's internal network. The Appliance executes internal Network Scans and does not store any results but transmits results via an HTTPS connection to the proper destination. A Virtual Appliance for such internal scanning. A Virtual Appliance is a packaged set of data files which is deployed onto a Customer-provided virtualization platform (e.g., VMware) to bring security and compliance assessment capabilities to the Customer network without the need to deploy dedicated hardware.

1.2.1.6 Email Filter Check. Conduct quarterly email filter checks on a prearranged date to evaluate the effectiveness of Customer's email gateway content filtering and endpoint filtering controls. For this test, send a series of emails with attachments to an email address within the Customer's domain. The Customer's network should detect and block these messages and/or attachments. The emails sent during this check are not invasive or dangerous to the Customer. The Customer is responsible for ensuring that the analyst has an email account on the network and that the analyst will record the actions taken by the Customer's network to defend against the simulated threat scenarios. If the Customer does not allow the analyst to have an email account on the Customer's network, then the Customer will be responsible for recording the actions taken by the Customer's network to defend against the simulated threat scenarios and providing this to the analyst. The results of the check will be categorized in the following way:

- Current Email Malware Rate – to understand the amount of email that contains malware. This rate is derived from a valid cyber intelligence source.
- Failed Frequent Checks – the number of failed checks associated with email Threats that are very likely or have a very high probability of exploiting weaknesses within an organization.
- Failed Common Checks – the number of failed checks associated with email Threats that are likely or have high probability of exploiting weaknesses within an organization.
- Failed Occasional Checks – the number of failed checks associated with email Threats that are somewhat likely or have a moderate probability of exploiting weaknesses within an organization.

The results from the email filter check will be detailed in the quarterly Email Filter Check Report and used to calculate a portion of the Risk Assessment score.

NOTE: Verizon uses an internal, proprietary tool for this assessment. For consulting or custom engagements, another COTS tool will be necessary to perform this assessment activity as the Verizon proprietary tool is not available for resale outside of the Verizon delivered Cyber Risk Programs.

1.2.1.7 Firewall Assessment. Conduct quarterly/Monthly firewall assessments on prearranged dates. The Customer will provide copies of select firewall configurations. The analyst will analyze those configurations remotely for the presence of strong firewall configurations and/or necessary boundary protections that can detect, prevent, and correct the flow of data transferring networks. The results of the assessment will be categorized in the following way:

- Customer Firewalls – to understand the number of firewalls being assessed.
- Firewall Policy/Rules – to understand the amount of rules per firewall being assessed. The amount of rules can vary from one firewall vendor to the next.

- Critical Severity Rules – to understand the amount of failed hits associated with controls that are critical in risk reduction. The lack of each critical control could have real and serious effects on an organization.
- High-Severity Rules – to understand the amount of failed hits associated with controls that are high in risk reduction. The lack of each high control could have real and serious, but limited in scope, effects on an organization.
- Moderate Severity Rules – to understand the amount of failed hits associated with controls that are moderate in risk reduction. The lack of each moderate control could have real, but limited in scope and damage, effects on an organization.

The results from the firewall assessment will be detailed in the quarterly Firewall Assessment Report and used to calculate a portion of the Risk Assessment score.

1.2.1.8 **End-Point System Assessment.** Conduct quarterly end-point system assessments on prearranged dates via endpoint scanning platform. Analyze those end-points remotely, assessing the security baseline for the presence of improper anti-virus, screen saver passwords, default configurations, industry best practice build standards, and secure configurations:

- Urgent Severity Checks – to understand the amount of failed checks associated with controls that are highly critical in terms of risk reduction. The lack of critical controls could have serious effects on an organization. They will be weighted based on how many computers in the sample are found.
- Critical Severity Checks – to understand the amount of failed checks associated with controls that are critical in terms of risk reduction. The lack of critical controls could have serious effects on an organization. They will be weighted based on how many computers in the sample are found.
- Serious Severity Checks – to understand the amount of failed checks associated with controls that are high in terms of risk reduction. The lack of critical controls could have serious effects on an organization. They will be weighted based on how many computers in the sample are found.

The results from the end-point assessment will be detailed in the quarterly End-Point Assessment Report and used to calculate a portion of the Risk Assessment score.

1.2.1.9 **Phishing Assessment.** Conduct quarterly phishing assessments on prearranged dates and times. The phishing assessment consists of email campaigns that evaluate employee knowledge and organizational areas of susceptibility. The phishing assessment will:

- Offer a scenario-based template that gauges employees' behavior and their understanding of cyber security.
- Provide metrics on security awareness and behavior patterns, as well as reinforce effectiveness of training programs.

The results from the phishing assessment will be detailed in the quarterly Phishing Assessment Report and used to calculate a portion of the Risk Assessment score.

1.2.1.10 **Wireless Assessment.** Evaluate the effectiveness and security of an organization's wireless network implementation. Via an onsite survey or agent installed, review corporate wireless policy, procedure, and network architecture. Additionally, a wireless analyzer is used to detect wireless devices around the targeted organization's premise. The detected wireless devices and their configurations are analyzed to provide key reporting information. This is used to mitigate the risk of unauthorized or rogue wireless devices, as well as indicate how well the wireless security defenses are deployed.

The wireless assessment will identify:

- Wireless attributable networks
- Ad-hoc wireless networks
- Wireless printers
- Guest wireless networks
- Wireless infrastructure vulnerabilities
- Bluetooth technologies including IoT devices utilizing Low Energy Bluetooth

The results from the wireless assessment will be detailed in the bi-annual Wireless Assessment Report and used to calculate a portion of the Risk Assessment score.

1.2.1.11 Physical Inspection. The Physical assessment validates physical controls that focus on the security posture of the physical environment surrounding the critical network infrastructure. The activity is conducted by the analyst via onsite inspections and demonstrations on a semi-annual basis in the contract year.

The analyst will conduct—but is not limited to—the following activities when inspecting the facilities:

- Review door security: biometric security, key card, access control, etc.
- Review policies for physical security
- Review convergence of physical security and information security
- Review security awareness training related to physical security
- Review Incident response policies for physical security events.
- Review business continuity and disaster recovery processes

The results from the physical assessment will be detailed in the bi-annual Physical Inspection Report and used to calculate a portion of the Risk Assessment score.

1.2.1.12 Policy, Process, and Procedure Assessment. Review & evaluate the organization's development and management of corporate information (cyber) security policies that align to risk-reducing controls. The assessment will include, but is not limited to, the following activities:

- Distributing list of policies that will need to be reviewed prior to or during the assessment (Note, this will increase the length of time onsite).
- The analyst securely collecting policies for review and inspection. Electronic copies of policies are preferred
- The policies will be inspected for content that aligns to particular concepts within the control set being validated.

The results from the assessment will be detailed in the bi-annual Policy, Process, and Procedure Assessment Report and used to calculate a portion of the Risk Assessment score.

1.2.2 Optional Add on Assessments & Activities. The Cyber Risk Programs – Risk Assessment also has provisions for the following “optional” add on assessments and activities in addition to standard 12 cyber risk measurement activities from above. Adding these items makes the Service “Custom”.

1.1.2.1 War Dial Assessments. Conduct war dial assessments by testing connections to a defined range of analog phone numbers in sequential order and then checking for responses which are identified and grouped into the following categories: discovered fax machines, discovered modems, responses from systems penetrated and identified monitoring systems.

1.1.2.2 **Optional Site/Location Specific Reports.** For those locations/Sites identified, Provide assessment activity reports requested, on a per site/location basis. The Standard reports package is a single report, per assessment activity, encompassing all sites/locations in scope, and quarterly Executive Summary Risk Report, which provides a summary of the individual assessment activities, findings and recommendations. These reports can be provided as “parent-child” type relationships where the child only gets their report and the parent gets all reports.

1.1.2.3 **Adaptive Modeling - Compliance Reports.** For customers who have need for specific compliance reports based on the CRP assessment activities, The Standard reports package is a single report, per assessment period, encompassing all sites/locations in scope, and delivered quarterly. Custom & consulting engagements may have a full compliance report provided, to measure the organizations risk programs compliance to a particular framework or frameworks.

1.2.3 **Scoring Methodology.** The Risk Assessment Scores can be utilized by Customer to help understand the Customer’s risk exposure.

The objective of the Risk Assessment scores is to spotlight the most critical elements associated with cyber security breaches, allowing Customer to improve its cyber risk posture. The Risk Assessment scores are not intended as, and do not constitute, a ranking of the overall quality or goodness of Customer’s cyber security posture in each activity. The Risk Assessment scores do serve as a mechanism of comparison to help better understand how their organization trends over time. The data from each activity is used to demonstrate how the Customer has addressed the Threats and most common attack patterns.

NOTE: For Custom & Consulting engagements that are not utilizing the Verizon DBIR data, a customer approved scoring methodology will be implemented that meets their requirements or requirements of a specific Risk Framework, such as FAIR.

- External Vulnerability Assessment Score
 - Weakness Count / Total Active External IP Addresses
The above ratio will be compared with all other Risk Assessment customers.
- IP Reputational Assessment Score
 - Disclosed Incident Count / Total Active External IP Addresses
 - The above ratio will be compared with all other Risk Assessment customers.
- NetFlow Assessment Score
 - Suspicious Internet Communication Count / Total Active External IP Addresses
 - The above ratio will be compared with all other Risk Assessment customers.
- Web Application Assessment Score
 - Weakness Count / Total Active Web Applications
 - The above ratio will be compared with all other Risk Assessment customers.
- Internal Vulnerability Assessment Score
 - Weakness Count / Total Active Internal IP Addresses
 - The above ratio will be compared with all other Risk Assessment customers.
- Email Filter Check Assessment Score
 - Allowed common malicious attachment types / current email malware rate
 - The above ratio will be compared with all other Risk Assessment customers.

- Firewall Assessment Score
 - Number of violations / (the number of firewalls * number of checks)
 - The above ratio will be compared with all other Risk Assessment customers.
- End-Point System Assessment Score
 - Weakness count / total control instances
 - The above ratio will be compared with all other Risk Assessment customers.
- Phishing Assessment Score
 - Clicked emails / number of accounts tested
 - The above ratio will be compared with all other Risk Assessment customers.
- Wireless Assessment Score
 - Wireless weaknesses / total number of expected access points
 - The above ratio will be compared with all other Risk Assessment customers.
- Physical Inspection Score
 - Site score = control deficiencies / total number of controls * site criticality (as defined by the data collected or stored at that physical site)
 - Corporate score = average of the score of all physical sites.
 - The above ratios will be compared with other Risk Assessment customers. For site-specific comparisons, only like sites will be compared.
- Policy, Process, and Procedure Assessment
 - Control deficiencies / total number of controls
 - The above ratio will be compared with all other Risk Assessment customers

1.2.4 **Reports.** Following completion of the quarterly assessment/diagnostic components of Risk Assessment (as described above), an Executive Risk Assessment Report will be produced. The report will provide risk scores for each of the 12 assessment activities, as well as an overall risk score from the combined assessments.

- External Vulnerability Assessment Results
 - External Vulnerability Assessment Score – to understand how many weaknesses are associated with the customer’s external IPs
 - External Vulnerability Assessment Trend – to determine if Unexpected Services and vulnerabilities are being remediated over time
 - External Vulnerability Assessment Recommendations – a prioritized set of recommendations to reduce vulnerabilities and unexpected services
- IP Reputational Assessment Results
 - IP Reputational Assessment Score – to understand the extent to which Customer’s CIP may be included in incident disclosures
 - IP Reputational Assessment Trend – to determine if associated incident disclosures are improving, worsening or remaining neutral
 - IP Reputational Assessment Recommendations – to understand how to decrease the likelihood of incident disclosures
- NetFlow Assessment Results
 - NetFlow Assessment Score – to understand the volume of suspicious Internet communications.
 - NetFlow Assessment Trend – to determine if the volume of suspicious Internet communications.
 - NetFlow Assessment Recommendations – to understand how to decrease the volume of suspicious Internet communications.

- Web Application Assessment Results
 - Web Application Risk Assessment Score – to understand how many weaknesses are associated with Customer’s critical Internet web applications
 - Web Application Risk Assessment Trend – to understand whether or not OWASP top 10 vulnerabilities are being remediated
 - Web Application Risk Assessment Recommendations – a prioritized set of recommendations to reduce OWASP top 10 vulnerabilities
- Internal Vulnerability Assessment Results
 - Internal Vulnerability Assessment Score – to understand how many weaknesses are associated with the customer’s internal IPs
 - Internal Vulnerability Assessment Trend – to determine if unexpected/excessive services and vulnerabilities are being remediated over time
 - Internal Vulnerability Assessment Recommendations – a prioritized set of recommendations to reduce vulnerabilities and unexpected services
- Email Filter Check Assessment Results
 - Email Filter Check Assessment Score – to understand how many weaknesses are associated with the organization’s email domains
 - Email Filter Check Assessment Trend – to determine if actions taken to address potential hostile attachments are effectively blocked prior to entering the organization’s domain and are thereby reducing risk.
 - Email Filter Check Assessment Recommendations – a prioritized set of recommendations to reduce hostile inbound attachments to which organizations are susceptible
- Firewall Assessment Results
 - Firewall Assessment Score – to understand how many critical violations are associated with the assessed firewalls
 - Firewall Assessment Trend – to determine if firewall rules and configurations are being remediated over time
 - Firewall Assessment Recommendations – a prioritized set of recommendations to reduce redundant rules, unexpected rules, and outdated rules
- End-Point System Assessment Results
 - End-Point System Assessment Score – to understand weaknesses associated with customer internal endpoints
 - End-Point System Assessment Trend – to understand whether a customer has improved endpoint security
 - End-Point System Assessment Recommendations – to ensure that endpoint configurations align with the customer baseline
- Phishing Assessment Results
 - Phishing Assessment Score – to evaluate employee knowledge and organizational areas of susceptibility
 - Phishing Assessment Trend – to provide metrics on security awareness, behavior patterns, and effectiveness of training programs
 - Phishing Assessment Recommendations – a prioritized set of recommendations to reduce employee susceptibility and increase training program effectiveness.
- Wireless Assessment Results
 - Wireless Assessment Score – to understand Unexpected Services and vulnerabilities associated with Open/WEP security and/or ad hoc networks
 - Wireless Assessment Trend – to determine if wireless and Bluetooth vulnerabilities are being remediated over time

- Wireless Assessment Recommendations – a prioritized set of recommendations to reduce wireless and Bluetooth vulnerabilities
- Physical Inspection Results
 - Physical Inspection Score – to understand the risk exposure posed by physical and environmental Threats
 - Physical Inspection Trend – to determine if physical risks have changed over time
 - Physical Inspection Recommendations – a prioritized list of recommendations to reduce the risk posed by physical and environmental Threats
- Policy, Process, and Procedure Assessment Results
 - Policy, Process, and Procedure Assessment Score – to understand how policies, processes, and procedures affect risk exposure
 - Policy, Process, and Procedure Assessment Trend – to determine if policy, process, and procedure management has changed over time
 - Policy, Process, and Procedure Assessment Recommendations – a prioritized list of recommendations to reduce risk through better policies, processes, and procedures
- Executive Risk Assessment Report
 - Executive Risk Assessment Score – to understand the individual scores across the 12 risk assessments
 - Executive Risk Assessment Trend – to trend an organization's risk, from the perspective of multiple reporting periods and as identified in the risk framework employed and identify an organization's ongoing risk posture
 - Executive Risk Assessment Recommendations – a prioritized set of recommendations to reduce risk based on items identified in the 12 risk assessments

Optional Add On Service Consideration – Verizon Risk Report

Another area of threat intelligence that the State of West Virginia could consider in the engagement with Verizon consulting for CRP is the integration of the Verizon Risk Report for both the State and its Agencies. The Verizon Risk Report is a customized risk assessment tool that measures and benchmarks your security posture in nRT reporting. VRR orchestrates threat data elements from the Verizon Threat and Intelligence Advisory Center (VTRAC), the Data Breach Investigations Report, Bitsight, and Recorded Future.

And in addition to the Risk Scoring attributes in VRR Level 1, the Deep Web/Dark Web searches further give a broader more concise understanding of what real threats to the State may exist. VRR can be rendered in 19 different Frameworks. And lastly, the Third Party Vendor Management feature could be added to have finger tip review of the State's Agencies Security Risk Scoring from an external view.

The Verizon Risk Report is one example of an additional capability and base of experience that Verizon brings to bear in working with the State of West Virginia in assisting in the development of the Cyber Risk Program.

;

Exhibit 4 – Sample Resume for Professional Services Principal Lead

Principle Consultant (name redacted)

CONTACT INFORMATION

Fairfax, Virginia

Mobile: 571-xxx-xxxx
xxxxxxxxxx@verizon.com

Experience:

- **Verizon Business Group**
Principal Consultant

Ashburn, VA (09/2006-Present)

Facilitate and prioritize activities and compliance requirements for clients to achieve Verizon Business Cybertrust certification for clients in a wide range of industries (Health Insurance, Financial Institutions, eGovernment, ISP Providers). Certification control requirements also serve as a baseline to multiple statutory, regulatory, and governance requirements that I would assist the organization in meeting. Schedule and conduct onsite client interfacing assessments that included interviews with key process/business units, vulnerability scanning, risk mitigation and security recommendations according to findings. Primary focus under my leadership was customer satisfaction while maintaining high standard of Verizon seal.

- Team Lead for 17 employees servicing clients over 50 locations
- Served as acting Delivery Manager for Northeast region.
- Deliver reports with 98% on time rate for each client site under my responsibility.
- Conduct and analyze risk assessments via network vulnerability scans.
- Analyze vulnerabilities according to risk, assist in analyzing data, and provide remediation requirements.
- Research security threats and trends to provide to clients as ongoing security advisor
- Validate Policies, Processes, and Procedures
- Provide governance and compliance assessments against multiple standards (ISO27001, PCI, HIPPA, NIST, Verizon Enterprise)
- Over 13 years, developed experience in problem solving client and team issues, identify team members' skill levels, and properly delegate to team members where their skills are utilized for greatest results.
- Assist and conduct pre-sales presentation
- Mentoring employees to ensure quality of delivery

- **IT Security Training and Solutions (ITS)2**
Senior Security Consultant

Riyadh, KSA (6/2003-08/2006)

Started as security engineer responsible for managing specific security products and services that were implemented at various companies including financial institutions, large manufacturing enterprises and government agencies in the Middle East region. Promoted to Senior position after one year with company by showing ability to learn, adapt, and implement to a wide range of issues. Responsible for providing professional services in configuring, implementing and training in multiple products that was part of company security solution. Assist in RFP creations and pre-sale technical meetings.

- Developed Proof of Concept demonstrations utilizing various products and solutions
- Configuration and implementation of security vendor solutions (Tripwire, Polivec, Pointsec, and Lancope, Cisco, Juniper, Microsoft)
- Setup Desktop Security including Anti-virus, Anti-spam, Trojan mitigation
- Perform attack and penetration testing for various clients
- Identify vulnerabilities and perform penetration attempts on those exploitations
- Customization of Network Vulnerability Scanning System & Vulnerability Alert Notification System
- Conduct an automated vulnerability assessment for different IT infrastructures
- Assist in a Business Risk Analysis on a specified business section and infrastructure
- Install, customize, test, and implement Intrusion Prevention System, Change Management Solution, Honeypot server with dummy website, SysLog Server, among other solutions
- Conduct on-site training for purchased security solutions
- Supported enterprise security requirements as well as LAN/WAN tasks including managing file servers, firewall configuration, Intrusion Detection Systems, Anti-virus, and Patch Management solution

- **Comprehensive Technologies Int'l
Network Administrator**

Fairfax, VA (11/01-5/03)

Responsible for IT resources such as hardware equipment and software maintenance and implementation. Implemented basic physical security controls to server area. Install new window servers to be used in production environment. Conduct testing of patches prior to implementation on production servers and configure new servers upon request.

- Setup Windows desktop for medium sized office
- Configure and harden Windows servers on weekly basis
- Configure Cisco routers and switches
- Harden Cisco IOS on routers and switches
- Apply new patches in testing area
- Install and test new applications in production environment
- Administer and maintain Windows server/desktop environment
- Provide help desk support to staff

IT Skills

- **HARDWARE**
Cisco (firewalls, VPN, routers, switches), Juniper (firewall and SSL VPN), Teros (Web Application firewall),
- **SOFTWARE**
Tripwire, Polivec, Symantec, Oracle, Cisco VMS & CSA
- **OPERATING SYSTEMS**
Microsoft, Linux, Solaris, Cisco IOS
- **PROTOCOL EXPERIENCE & KNOWLEDGE**
TCP/IP SMTP SNMP NetBEUI IPX/SPX RIP IGRP

Education

George Mason University
B.S. in Economics
Minor in Information Technology
Minor in Business.

Fairfax, VA
May 2003

CERTIFICATIONS

Pointsec Engineer, November, 2003
Security Plus Professional (Security +), December, 2003
Foundation Certificate in IT-Service Management (ITIL), September, 2004
Certified Information Systems Security Professional (CISSP), December, 2004
BS7799 Implementation, December, 2004
Cisco Certified Network Associate (CCNA), January 2005
Tripwire Solution, March 2005
Cisco Secure, May 2005
ISO 27001 Lead Auditor, August 2006
Holistic Information Security Practitioner (HISP), April 2008
Certified Information Systems Auditor (CISA), August 2009
Payment Card Industry Qualified Security Assessor (PCI QSA), September 2010
Certified in Risk and Information Systems Control (CRISC), November 2016

Communication Skills

English - Native
Arabic - Fluent

References available upon request.

Exhibit 5 – CRP Risk Assessment Reporting Samples

CRP Risk Assessment Reporting Samples Exhibit (TBD)

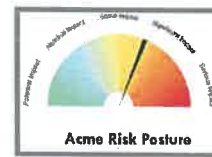
Detailed reporting on 12 risk assessments, plus an Executive Summary Risk Report.

Individual assessment reports include:

- Assessment score & trending – Maturity Model
- Risk-reducing recommendations
- 9 quarterly reports, 3 reports twice a year
- Technical details reports for remediation teams

Executive report includes:

- Executive risk assessment score
- Executive risk assessment recommendations
- Heat map scorecard
- Meeting & Review with Executive Management Options
 - Onsite
 - Via WebEx



Control Failure by Severity	Critical Risk	High Risk	Medium Risk	Low Risk
Control Failure Count	13	7	10	0



Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.

Risk Assessment Heat Map

Periodic, in-depth and reliable program for those concerned about risk

- The Heat Map provides a high level, graphical view of risks impacting your organization
- Twelve recurring risk-assessment activities
- Alignment to the DBIR Threat Vectors
- Objective review and risk scores
- Comparison of your score to others in your Vertical.
- Visibility of Security and Risk Posture for Executive Level and Board of Directors

Executive level scorecard

Data Breach Investigations Report Threat Vectors	Cyber Risk Program Deliverables												Customer Score	Email Hiker Check	Reputation	Network	Web Application Application	Endpoint	Policy, Process, and Procedures	Physical	Wireless	Risks/Rog	Firewall	Internal (DMZ) Vulnerability	Internal (LAN) Vulnerability	External Vulnerability	Member/Vertical Posture
	1 - Normal impact very unlikely	2 - Potential for impact	3 - Serious impact somewhat	4 - Serious impact likely	5 - Severe impact very likely	Technical issue	Non-credentialed	Forfeit Deliverable	Not Applicable																		
Point of Sale - Intrusion	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	1	1				
Web Application Attack	2	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	5	5			
Privileged Misuse	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2			
Theft/Loss	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	2	2			
Miscellaneous Error	2	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4			
CrimeWare	2	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	2	2	2			
Payment Card Skimmers	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	1	1			
Denial of Service	2	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	2	2	2			
Cyber Espionage	2	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	2	2	2			
Everything Else	2	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	2	2	2			

Risk Legend

- 1 - Normal impact very unlikely
- 2 - Potential for impact
- 3 - Serious impact somewhat
- 4 - Serious impact likely
- 5 - Severe impact very likely
- Technical issue
- Non-credentialed
- Forfeit Deliverable
- N/A - Not Applicable



Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.

Exhibit 6 – Resume for Jeff Cornelius, Project Manager



Jeff Cornelius

Senior Security Consultant Verizon Enterprise Solutions Global Consulting Services

Governance, Risk, & Compliance Practice

Professional Profile

Jeff Cornelius is a Senior Security Consultant in the Governance, Risk & Compliance Practice within Verizon Enterprise Solutions. This organization is responsible for providing consulting services, integration services, and e-business solutions covering all aspects of Information Security Management, IT Governance, Risk Management, and Regulatory Compliance pertaining to IT Security and Digital Privacy.

Jeff has over 40 years of experience as an IT professional covering diverse platforms and security issues. He possesses a wide range of skills and experiences that enable him to perform in multiple roles. His experience includes infrastructure and security management, project management, technology implementation, policy and procedure development, security awareness training, disaster recovery, risk assessments and compliance. He currently specializes in providing security solutions to meet with regulatory requirements and business drivers in multiple industries including healthcare, insurance, banking, manufacturing, retailing, services, communications, and education.

Experience and Accomplishments

Jeff as a Consultant has performed numerous Business Security Assessments (BSA) measuring organizational information security program compliance and readiness to industry standards including ISO 2700x, NIST 800, NIST CSF and CIS CSC. This has included a comprehensive analysis of organizational strengths, weakness and recommendations.

Jeff has also performed Security Risk Assessments (SRA) identifying, measuring and categorizing information security risk along with developing risk reducing recommendations for several organizations.

Additionally, Jeff has performed HIPAA Privacy and Security assessments addressing physical facilities, HIPAA compliance, HIPAA Meaningful Use, data risk and protection of PHI data for both small and large organizations some with many satellite offices.

Consultant Profile

Nationality, Location,

- American
- Indianapolis, IN, USA

Languages Spoken

- English

Qualifications and Memberships

Certifications

- Certified Information Systems Security Professional (CISSP)
- Certified Information Privacy Professional (CIPP)
- Payment Card Industry Qualified Security Assessor (PCI-QSA)
- Certified HIPAA Privacy and Security Expert (CHPSE)
- Holistic Information Security Practitioner (HISP)
- ITIL v3 Foundation

Education

- Associate of Applied Science in Computer Technology – Purdue (IUPUI) University



Jeff has developed information security and privacy policies and developed client customized cross mappings of policies to various industry regulatory requirements.

Jeff has developed assessment criteria for third party vendors and performed third party vendor assessments.

Jeff has developed PCI Compliance Run Book procedures for a major manufacturing company and PCI SDLC procedures for a major retailer of men's clothing.

Prior to working with Verizon, Jeff served as Director of Information Security for an insurance holding company and was responsible for overseeing multiple groups supporting information security in the mainframe, client-server and web environments. This involved monitoring compliance requirements for HIPAA, PCI and along with various state, federal and European data privacy laws. Additionally performed an ISO security risk assessment and developed a 3 year strategic security plan and roadmap.

Also, Jeff worked as a Security Manager for a major communications carrier was responsible for the information security program including access management administration, vulnerability management, threat monitoring and policy development.

Additionally as Data Center Director for a health insurance carrier, Jeff was responsible for overseeing and staff of 75 supporting all operational infrastructure functions of the data center. This included network, mainframe and client servers systems along with maintaining proper security and access for personal data in storage, at rest and being processed. This also required ensuring compliance with all regulatory requirements and laws.

As a Vice President of Data Processing for an insurance agency had responsibilities for all information systems, applications development, maintenance and support.

Expert Knowledge

- Security and Risk Management
- Information Security Policy and Process Development
- Security Compliance: ISO 27002/27001, HIPAA, PCI, NIST

Vertical Specific Experience

- Financial
- Health Care
- Manufacturing
- Retail
- Education

Exhibit 7 – United States Service Agreement

United States Service Agreement
between
Verizon Business Network Services Inc.
and
State of West Virginia, Office of Technology

This United States Service Agreement is entered into by and between Customer and Verizon to establish the terms and pricing under which customer will purchase Services offered by Verizon. The Master Terms below set out the terms and conditions governing all Services. All capitalized terms not otherwise defined in the Agreement have the meanings set forth in the Master Terms Section 19, Definitions. Services are described in Schedule A.

MASTER TERMS

1. SERVICE ORDERING OPTIONS

- 1.1 **Orders.** Customer may place Orders for Service via Verizon's standard process for such Service.
- 1.2 **No Sign SOF (NSS) Process.** When using the NSS Process, Verizon will send the NSS to Customer via email to an address provided by Customer. The NSS has the same effect as a signed Order. Customer has five days from receipt of the NSS to notify Verizon of any errors.

2. CHARGES, PAYMENT, TAXES, AND PURCHASE COMMITMENTS

- 2.1 **Online Pricing.** If the Agreement incorporates online Charges, those Charges may be supplemented by the Charges for new Service options as they become available, such as faster speeds and advanced features. Any such new Charges will be clearly distinguished from existing Charges, which will not be affected. Customer may order such new Service options at the referenced Charges, subject to applicable terms.
- 2.2 **Activation.** Customer is deemed to have accepted Services on the Activation Date. Charges are accrued and invoiced as follows: (a) recurring Charges accrue from the Activation Date and are invoiced in advance; (b) usage based Charges accrue from the Activation Date and are invoiced in arrears; (c) non-recurring Charges accrue from the Commencement Date and are invoiced at any time thereafter; and (d) Third Party Charges are invoiced in accordance with the Order or Service Attachment. For Charges invoiced more than six months after the date a Charge accrues Customer may obtain a credit on request (except in cases involving fraud or Third Party Charges).
- 2.3 **Activation Delays.** If the Activation Date is delayed because Customer: (a) has not done all that is necessary on its part to activate the Services, Verizon may deem a date to be the Activation Date (whether the Services are ready for use or not) by notice to Customer and Charges will accrue in accordance with the clause entitled Activation; or (b) requests a delay; then in either case Customer shall be liable for any third party costs incurred by Verizon relating to the affected Services at a Customer Site during the period of delay.
- 2.4 **Payment.** Customer shall pay Verizon invoices within 60 days of the relevant invoice date.
- 2.5 **Disputed Amounts.** If Customer notifies Verizon of a Disputed Amount by the Due Date, the Disputed Amount may be withheld. If a Disputed Amount is found to be not owed then Verizon will issue a credit. Verizon may elect to apply any credit balance(s) to the account(s) with the oldest unpaid charges. If a Disputed Amount is found to be owed, any withheld amount must be paid within five days after notification by Verizon to Customer of that determination. If Customer does not give Verizon notice of a Disputed Amount with respect to Charges or the application of Taxes within six months after the Due Date, the invoice will be deemed to be correct and binding on Customer.

2.6 : **Past Due Amounts.** Amounts not paid on or before the Due Date are past due, and will accrue interest from the Due Date until payment at the rate of: (a) 1.5% per month (compounded monthly); or, where that rate is not permitted by applicable law or regulation (b) the maximum amount allowed. Without prejudice to any other rights under applicable law or regulation, Verizon may exercise its rights of termination or suspension in accordance with the Agreement with respect to any past due amount other than Disputed Amounts. Customer agrees to pay Verizon its reasonable expenses, including legal and collection agency fees, incurred in enforcing its rights under the clause entitled Charges, Payment, Taxes, and Purchase Commitments.

2.7 Purchase Commitments

2.7.1 Volume Commitments

2.7.1.1 **Volume Commitment Obligations.** Where a Volume Commitment applies, Customer shall pay Verizon the amount of Eligible Charges required to meet the relevant Volume Commitment within the applicable measurement period. If, at the end of any Contract Year or Volume Commitment Period (as applicable), the Eligible Charges Customer has paid are less than the Volume Commitment, then Customer shall pay an Underutilization Charge equal to 75% of the shortfall (or other percentage detailed elsewhere in the Agreement).

2.7.1.2 **Responsible Party.** The Customer entity that is the Party to the USSA (not a Participating Entity) remains responsible in all respects for any failure to meet any Volume Commitment.

2.7.2 **Service Commitment.** For Optimized Services, no Service Commitment applies unless it is stated in the Agreement. For non-Optimized Services, a minimum one year Service Commitment applies unless otherwise stated in the Agreement. For all Services, any Service Commitment stated in an Order will take precedence over conflicting information elsewhere in the Agreement.

2.7.3 **Purchase Commitment Expiry.** Upon expiration of a Volume Commitment Period and/or Service Commitment (as applicable), the associated Service automatically continues until either Party terminates it under the terms of the Agreement.

3. TERM

3.1 **Term.** The Agreement will remain in force and the Services under it will continue to be provided unless and until terminated by either Party in accordance with the Agreement.

3.1.1 **Extended Term.** For standalone Agreements for Optimized Services with a Volume Commitment, upon expiration of a Volume Commitment Period, the Agreement is automatically renewed for a subsequent Volume Commitment Period equal to the expired Volume Commitment Period (including any extensions) ("Extended Term") with a Volume Commitment equal to that which was in effect at the end of the expired Volume Commitment Period, unless a Party provides the other Party with notice of its intent not to auto-renew the Agreement at least 90 days prior to the expiration of the Volume Commitment Period. After expiration of the Extended Term, the Agreement is automatically extended on a month-to-month basis until either Party terminates it upon 60 days written notice. The terms of the Agreement (excluding the Volume Commitment) will continue to apply during any service-specific commitments that extend beyond the Volume Commitment Period.

3.2 **Verizon Termination for Convenience.** Verizon may terminate a Service or the Agreement for Convenience on 60 days' notice to Customer provided all applicable Volume Commitment Periods and/or Service Commitments have expired.

4. **SERVICE SUSPENSION.** Verizon may suspend one or more Services (or a part thereof) if: (a) Customer fails to pay any past due amounts for Services within 10 days after Customer receives notice of such non-payment; or (b) necessary to: (i) prevent or mitigate fraud, (ii) protect persons or property or protect the integrity or normal operation of Verizon Facilities, (iii) comply with law or regulation, or (iv) undertake Emergency Works; or (c) Verizon has reasonable grounds to consider that use of the Services violates the AUP. Verizon will give to Customer reasonable notice of the suspension where practicable, except in relation to suspension pursuant to sub-clause (a) above, where no notice is required beyond the 10 days stated therein. If Verizon exercises its right to suspend the Services, it

will resume the Services as soon as practicable after the reason for suspension no longer exists (subject to the exercise of any termination right on the part of Verizon). If Services are suspended as a consequence of the breach, fault, act or omission of Customer or any Customer Affiliate, Customer shall pay to Verizon all reasonable costs and expenses incurred by the implementation of such suspension and/or reconnection of the Service.

5. **AVAILABILITY OF SERVICES.** If Verizon cannot fulfill an Order (after the Commencement Date) for reasons other than Force Majeure Event, after making commercially reasonable efforts to fulfill such Order, Verizon will notify Customer as soon as possible and where available, Verizon will advise Customer of any alternative Service offerings. In any event Verizon will have no further obligation to provide the Service under that Order.
6. **SERVICE LEVEL AGREEMENT (SLA).** Verizon reserves the right to amend any applicable SLA from time to time effective upon posting of the revised SLA to the URL where the SLA is set out or other notice to Customer, provided that in the event of any amendment resulting in a material reduction of the SLA's service levels or credits, Customer may terminate Services without termination liability (except for payment of all Charges up to the effective date of the termination of any such Services) by providing Verizon at least 30 days' notice of termination during the 30 days following the posting or notice of such amendment, as applicable. Customer is not entitled to terminate if, within 30 days of receipt of Customer's notice, Verizon agrees to amend the relevant SLA so that the affected SLA service levels and credits are not materially reduced for Customer. The SLA sets forth Customer's sole remedies for any claims with respect to Services to which the SLA relates. Verizon records and data are the basis for all SLA calculations and determinations.

7. LIABILITY

7.1. **Liability - Limitations.** Subject to the clauses entitled Liability - Exclusions and Liability - Inclusions:

7.1.1. **Aggregate Liability.** The aggregate liability of either: (a) Customer, its Affiliates and Participating Entities; or (b) Verizon and its Affiliates, to the others collectively for any and all Events in an Annual Period is limited to an amount equal to 12 times the Average Monthly Charges during the Annual Period in which an Event first occurred. For the purpose of this clause and calculation, where: (i) an Event gives rise to a number of separate liabilities, claims or causes of action, and/or (ii) there is a series of connected Events, such will be considered a single Event and will be deemed to have occurred in the Annual Period in which the first Event occurred.

7.2. **CPE Liability.** The entire liability of Verizon and its Affiliates for Events arising in connection with the sale of CPE is limited to the Charges for the specific CPE giving rise to the particular Event. This clause operates independently to (and to the exclusion of) the aggregate liability limitation detailed in the clause entitled Aggregate Liability. **Liability - Exclusions.** Subject to the clause entitled Liability - Inclusions below, neither: (a) Customer, Customer Affiliates and Participating Entities; nor (b) Verizon and Verizon Affiliates, will be liable to the others for any: (i) special damages, (ii) incidental damages, (iii) exemplary damages, (iv) punitive damages, (v) indirect and/or consequential loss, (vi) loss of sales or business, (vii) loss of value, (viii) loss of use, (ix) loss of goodwill, (x) damage to reputation, (xi) loss of data, (xii) loss of anticipated savings, or (xiii) business interruption.

7.3. **Liability - Inclusions.** Nothing in this Agreement operates to exclude or limit any of the following and these amounts will not be counted in assessing whether the aggregate liability limitation in the clause entitled Liability - Limitations has been reached: (a) any liability relating to bodily injury (including death) caused by a Party's negligence; (b) any liability resulting from a party's fraud or fraudulent misrepresentation; (c) any liability that cannot be limited under applicable law or regulation, including but not limited to mandatory local law; (d) any indemnification obligation under the Agreement; (e) damages, including with respect to loss of or damage to real property or tangible personal property, resulting from gross negligence or intentional tortious conduct of a Party; and (f) any liability of Customer and Participating Entity with respect to non-payment, including any claim for interest.

8. CUSTOMER DATA

8.1. Customer Data

- 8.1.1. **Customer Data.** Verizon, and Verizon Affiliates and their respective agents will, by virtue of the provision of Services, come into possession of Customer Data.
- 8.1.2. **Protection Measures.** Verizon will implement appropriate technical and organizational measures to protect Regulated Customer Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against other unlawful forms of processing which measures may for example relate to data handling practices, backup procedures and server, workstation and transmission security for internal communications.
- 8.1.3. **Access.** Customer may access Regulated Customer Data in the possession of Verizon, on notice, and any agreed errors in such Regulated Customer Data will be rectified.
- 8.1.4. **Use of Customer Data.** By entering into the Agreement, Customer expressly and unequivocally consents to Verizon, Verizon Affiliates and their respective agents, using, processing and/or transferring Customer Data (including intra-group transfers and transfers to entities in countries that do not provide statutory protections for personal information) as set forth in the Privacy Policy and as necessary: (a) in connection with provisioning of Services; (b) to incorporate Customer Data into databases controlled by Verizon, Verizon Affiliates or their respective agents for the purpose of providing Services; administration; provisioning; invoicing and reconciliation; verification of Customer identity, solvency and creditworthiness; maintenance, support and product development; fraud detection and prevention; sales, revenue and customer analysis and reporting; market and customer use analysis including in the manner described in the Privacy Policy; and (c) to communicate to Customer regarding services.
- 8.1.5. **Customer Consent.** Customer warrants that it has obtained or will obtain all legally required consents and permissions from relevant Parties (including data subjects) for the use, processing and transfer of Customer Data as described in this clause entitled Customer Data and Confidentiality.
- 8.1.6. **Withdrawal of Consent.** Customer may withdraw consent for such use, processing or transfer of Customer Data as set out above, except as it is required to: (a) provision, manage, account or invoice for Services; (b) carry out fraud detection; or (c) comply with any statutory or regulatory requirement or the order of a court or other public authority, by sending notice to Verizon in the prescribed form, available from Verizon on request.

9. CUSTOMER OBLIGATIONS

- 9.1. **Access.** Where Verizon or its third party providers require access to a Customer Site, Customer will grant or will procure the grant to Verizon or its third party provider such access including all licenses, waivers and consents as necessary to install, construct or use space in the building risers, innerduct, or conduit from the property line to the Customer Site and to operate and maintain Service Equipment at the Customer Site. Customer will advise Verizon in writing of all health and safety rules and regulations and any other reasonable security requirements applicable at the Customer Site.
- 9.2. **Assistance.** Customer will provide Verizon with such facilities, information and co-operation as Verizon may reasonably require to perform its obligations or exercise its rights under the Agreement or an Order, including with respect to Verizon's implementation of new processes or systems.
- 9.3. **Service Equipment.** Where Verizon provides Service Equipment, Customer warrants and undertakes that it will: (a) use the Service Equipment only for the purpose of receiving Services and in accordance with Verizon's reasonable instructions from time to time and/or any Software license that may be provided with the Service Equipment; (b) not move, modify, relocate, or in any way interfere with the Service Equipment or Verizon Facilities; (c) insure and keep insured all Service Equipment against theft and damage; (d) not create or allow any charges, liens, pledges or other encumbrances to be created over the Service Equipment; (e) permit Verizon to inspect, test, maintain

- ; and replace the Service Equipment at all reasonable times; (f) comply with Verizon's reasonable instructions, at Customer's own expense, in relation to the modification of the Customer Equipment to enable Customer to receive Services; and (g) upon termination of any of the Services, follow Verizon's reasonable instructions with respect to the return of the Service Equipment including allowing Verizon access to each Customer Site to remove the Service Equipment. Should any construction or alteration to a Customer Site have occurred to facilitate any Services, Verizon is not obliged to restore that Customer Site to the same physical state as prior to delivery of the Services. Customer is liable for any and all damage to Service Equipment or Verizon Facilities which is caused by: (i) the act or omission of Customer or Customer's breach of the Agreement or an Order, or (ii) malfunction or failure of any equipment or facility provided by Customer or its agents, employees, or suppliers, including but not limited to the Customer Equipment. Verizon is not liable for any costs incurred by Customer arising out of any malfunction or failure of any such equipment or facility, including Customer Equipment.
10. **SOFTWARE AND DOCUMENTATION.** Software not otherwise subject to a separate agreement or license is provided to Customer subject to Verizon's standard Software license terms as follows. In consideration for payment of any applicable fees, Customer is granted a License. Customer may not use the Software either in connection with the products and/or services of any third party or to provide services for the benefit of any third party. Customer may make one copy of the Software, other than the documentation, for archival or back-up purposes only if any copyright and other proprietary rights notices are reproduced on such copy. Customer may make a reasonable number of copies of documentation provided as part of the Software solely in support of its use of the Software and Services. Customer may not: (a) attempt to reverse engineer, decompile, disassemble or otherwise translate or modify the Software in any manner; or (b) sell, assign, license, sublicense or otherwise transfer, transmit or convey Software, or any copies or modifications thereof, or any interest therein, to any third party. All rights in the Software, including without limitation any patents, copyrights and any other intellectual property rights therein, remain the exclusive property of Verizon and/or its licensors. Customer agrees that the Software is the proprietary and confidential information of Verizon and/or its licensors subject to the provisions of the clause entitled Confidentiality. Except to the extent otherwise expressly agreed by the Parties in writing, Verizon has no obligation to provide maintenance or other support of any kind for the Software, including without limitation any error corrections, updates, enhancements or other modifications. The License will immediately terminate upon the earlier of: (i) termination or expiration of any Agreement or Order between Verizon and Customer pertaining to the Software, (ii) termination of the Services with which the Software is intended for use, or (iii) failure of Customer to comply with any provisions of this clause entitled Software and Documentation. Upon termination of any License, at Customer's option, Customer will promptly either: (1) destroy all copies of the Software in its possession; or (2) return all such copies to Verizon, and in either event provide an officer's written certification confirming the same.
11. **RESALE OF SERVICES.** Except as expressly prohibited by law or regulation or as set forth in the Agreement, Customer may not resell, charge, transfer or otherwise dispose of Services (or any part thereof) to any third party.
12. **ACCEPTABLE USE POLICY (AUP).** Use of Verizon IP Services must comply with the AUP of the countries from which Customer uses such Services (in the event no AUP exists for a country, the U.S. AUP will apply). The applicable AUP is available at the following URL: verizonenterprise.com/terms or other URL designated by Verizon. Customer will ensure that each user of the Services complies with the AUP.
13. **IP ADDRESSES.** Any IP addresses assigned to Customer by Verizon must be used solely in connection with the Services for which they are assigned. If such Services are terminated, Customer's right to use the IP addresses ceases immediately and the IP addresses immediately revert to Verizon.
14. **NETWORK MONITORING.** Transmissions passing through Verizon Facilities may be subject to legal intercept and monitoring activities by Verizon, its suppliers or local authorities in accordance with applicable local law and regulatory requirements.
15. **CONTENT DISCLAIMER.** Verizon exercises no control over and has no responsibility for the accuracy, quality, security or other aspect of any Content accessed, received, transmitted, stored, processed or used through Verizon Facilities or any Services (except to the extent particular Services explicitly state

otherwise). Customer accesses, receives, transmits, stores, processes, or uses any Content at its own risk. Customer is solely responsible for selecting and using the level of security protection needed for the Content it is accessing, receiving, transmitting, storing, processing or using, including without limitation Customer Data, individual health and financial Content.

16. GENERAL

- 16.1 **Notices.** Except as set out in the clause entitled Verizon Enterprise Center (VEC) Termination Requirement, all notices (including notices to terminate the Agreement for Convenience) must be in writing and sent to the notice address specified below and for Customer, as specified, or if no such address is specified, the registered address of Customer. Notice may be transmitted via any of email, overnight courier, hand delivery, a class of certified or registered mail that includes proof of receipt or, for Verizon only, via invoice message. Notice sent in accordance with this clause is effective when received, except for email notice, which is effective the Business Day after being sent.

Verizon Business Services 6415-6455 Business Center Drive Highlands Ranch, CO 80130 Attn: Customer Service Email: notice@verizon.com With a subject of "OFFICIAL LEGAL NOTICE"	with a copy to Verizon Business Services 500 Summit Lake Drive Office 4-04 Valhalla, NY 10595 Attn: Vice President, Legal
---	--

- 16.2 **Applicability of Terms.** If any of the provisions of the Agreement are held by any entity of competent jurisdiction to be unenforceable, the remainder of the Agreement remains enforceable. Failure or delay to exercise or enforce any right under the Agreement is not a waiver of that right. Certain provisions are intended by their nature to survive expiration or termination (including, without limitation, Liability and Customer Data and Confidentiality). The Agreement may not be amended except by a written instrument that both Parties agree to be bound by (whether by execution or some other method).
- 16.3 **No Third Party Beneficiaries.** No right or cause of action for any third party is created by the Agreement or any transaction under it.
- 16.4 **Force Majeure.** Any failure by a Party to perform an obligation, (other than a failure to make payment), under the Agreement that is the result of a Force Majeure Event is not a breach of the Agreement. A Party claiming non-performance from a Force Majeure Event must promptly provide the other Party notice of the relevant details, and the obligations of the notifying Party are suspended to the extent caused by the Force Majeure Event. The time for performance of the affected obligation will be extended by the delay caused by the Force Majeure Event. If the affected Party is prevented by the Force Majeure Event from performing its obligation(s) with respect to a Service for 30 days, either Party may in its sole discretion immediately terminate such Service with notice to the other Party; provided that in the case of termination by Customer, Customer first provides Verizon a reasonable opportunity to replace the affected Service with comparable Service(s). Upon such termination, Verizon is entitled to payment of all accrued but unpaid Charges incurred through the date of such termination. The Parties will otherwise bear their own costs and Verizon will be under no further liability or obligation to perform the Service affected by the Force Majeure Event.
- 16.5 **Counterparts and eSign.** Where a signature is required, an Order or the USSA may be executed in one or more counterparts, each of which is be deemed to be an original, but together constitutes one instrument. The Parties agree that an Order or the USSA may be executed by eSign if available.
- 16.6 **Order of Precedence.** In the case of any inconsistency, the USSA takes precedence over Orders. Within the USSA, the order of precedence (in descending priority) is: Master Terms, Service Attachments (Schedule A), and Pricing (Schedule B). Within each of those parts of the Agreement, those terms set out directly into the document to which Customer is a Party take precedence over any online terms.
- 16.7 **Changes to Online Terms.** Verizon may change the Online Master Terms and Service Terms from time to time, effective upon 30 days posting or other notice. By continuing to use Service(s) after a

- change becomes effective, Customer agrees to be bound by the changed terms, which apply to new and previously-ordered Services. It is Customer's responsibility to check the Online Master Terms and Service Terms regularly for changes.
- 16.8 **Entire Agreement.** The Agreement: (a) expresses the entire understanding of the respective Parties with respect to their subject matter; (b) supersedes all prior or contemporaneous representations, solicitations, offers, understandings or agreements regarding their subject matter which are not fully expressed herein; and (c) contains all the terms, conditions, understandings, and representations of the Parties. Any terms and conditions sent to Verizon by Customer as a purchase order or otherwise, are void and of no effect and, will not supersede any terms and conditions in the Agreement.
17. **CUSTOMER CONSENT TO USE OF U.S. CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI).** Verizon desires to give you the best digital and connected experience and the most reliable products and services. Verizon protects all your Customer information, but may need to share your Customer information with our affiliates, and with our partners, vendors, and agents, in order to offer and provide products and services to you, our Customer. The Federal Communications Commission, and various states, require Verizon, and indeed all telecommunications providers, to protect Customer Proprietary Network Information (CPNI). CPNI is information that identifies the quantity, technical configuration, type, destination, location, and amount of use of a Customer's telecommunications and interconnected VoIP services purchased from a provider, and related local and toll billing information. Verizon respects our Customers' rights to the protections afforded by these laws and regulations. By signing the USSA, Customer grants Verizon permission to use, give access to, and share, Customer's CPNI between and among Verizon and its Affiliates, and with their agents, contractors, and partners, solely so Verizon and its affiliates can offer Customer our current and future products and services; and to disclose any of Customer's current and future affiliates' CPNI to Customer upon Customer's request. Additionally, Customer represents that the individual signing the USSA has the authority to grant this permission to Verizon. You, our Customer, may withdraw or limit your consent at any time via email at cpni-notices@verizon.com or at cpni-notices@verizonwireless.com. Please note that your consent will remain valid until Verizon receives a notice withdrawing consent. Withdrawal or limitation of consent will not affect existing service delivery.
18. **PROTECTION OF CUSTOMER U.S. CPNI AND PROVISION OF CUSTOMER CPNI TO AUTHORIZED CUSTOMER REPRESENTATIVES.**
- 18.1 **Access and Use.** Verizon will protect the confidentiality of Customer CPNI in accordance with applicable U.S. laws, rules and regulations. Verizon may access, use, and disclose Customer CPNI as permitted or required by applicable laws, rules, and regulations or the USSA.
- 18.2 **Provision of CPNI Information.** Provided that Customer is served by at least one dedicated Verizon representative under the USSA (that can be reached by Customer by means other than calling through a call center) and as permitted or required by applicable law and regulation, Verizon may provide Customer CPNI (including, without restriction, call detail) to representatives authorized by Customer ("Authorized Customer Representatives" as defined below) in accordance with the following.
- 18.3 **Means of Provision.** Verizon may provide Customer CPNI to Authorized Customer Representatives via any means authorized by Verizon that is not prohibited by applicable laws, rules, or regulations, including, without restriction: to Customer's email address(es) of record (if any) or other email addresses furnished by Authorized Customer Representatives, to Customer's telephone number(s) of record or other telephone numbers provided by Authorized Customer Representatives, to Customer's postal (U.S. Mail) address(es) of record or to other postal addresses furnished by Authorized Customer Representatives, or via Verizon's online customer portal or other online communication mechanism.
- 18.4 **Notice of Authorized Customer Representatives.** Authorized Customer Representatives include Customer employees, Customer agents, or Customer contractors, other than Verizon, who have existing relationships on behalf of Customer with Verizon customer service, account, or other Verizon representatives and all other persons authorized in written notice(s) (including email) from Customer to Verizon. Authorized Customer Representatives shall remain such until Customer notifies Verizon in writing that they are no longer Authorized Customer Representatives as described below. Customer agrees, and will cause Authorized Customer Representatives, to abide by reasonable authentication and password procedures developed by Verizon in connection with disclosure of Customer CPNI to

- 18.5 **Necessary Information.** Customer's notices of authorization or deauthorization must be sent to Verizon's service or account manager, and must contain the following information:
- (a) the name, title, postal address, email address, and telephone number of the person authorized or deauthorized
 - (b) that the person is being authorized, or is no longer authorized, (as applicable), to access CPNI
 - (c) the full corporate name of the Customer whose CPNI (and whose Affiliates' CPNI) the person can access (or can no longer access, if applicable)
- 18.6 **CPNI Authorizers.** At all times that the Agreement is in effect, Customer may designate in a form provided by Verizon and returned to Verizon (all containing the same data elements listed below) up to three representatives ("CPNI Authorizers") with the power to name Authorized Customer Representatives who may access CPNI under the USSA as well as additional CPNI Authorizers. Additions or removals of CPNI Authorizers will be effective within a reasonable period after Verizon has received a signed writing of the change, including the affected person(s)' name, title, postal address, email address and telephone number. The person who executes the Agreement or Order will be a CPNI Authorizer and may add or remove CPNI Authorizers for that Customer and for its Participating Entities.

19. **DEFINITIONS.** Capitalized terms contained in the Agreement are defined as follows:

"+" after a Service name indicates the Service is an Optimized Service.

"Acceptance Date" as used in any Order or Service Attachment, means Activation Date.

"Activation Date" means: (a) with respect to Internet, data and on-network voice Services, the date the hub and telephone circuits are prepared to route packets or cells to a Customer Site; (b) with respect to off-network voice Services, the date the calling line identification is provisioned; (c) with regard to other Services, the earliest of: (i) the date identified in the relevant Service Attachment or Order, (ii) the date that Verizon informs Customer that Services are ready for use, (iii) the date Customer first uses Services or (iv) for CPE deployment services under the CPE Service Attachment, the date on which the deployment acceptance process and Customer signature requirements specified therein are completed; and (d) in the case of existing Services that are renewed, the date that is stated on the Order.

"Affiliate" means any entity or person controlled by, controlling, or under common control with Verizon or Customer, as applicable.

"Agreement" means the USSA together with all Orders entered into pursuant thereto.

"Annual Period" means the 12 month period beginning on the Commencement Date of the USSA, and each anniversary thereafter.

"Annual Volume Commitment" or "AVC" means the total Eligible Charges which Customer must pay during each Contract Year of the Volume Commitment Period.

"AUP" means the applicable Verizon Acceptable Use Policy.

"Average Monthly Charges" means all Charges (save for any Charges relating to the sale of CPE) which: (i) have been invoiced; and (ii) will be invoiced during the relevant Annual Period to Customer and its Participating Entities under the Agreement and calculated as a monthly average across the Annual Period.

"Business Day" means a day other than a Saturday and Sunday, or other customary rest day(s), and national holiday(s) in the jurisdiction of the Customer Site.

"Cancellation of Order Charges" means the charges (if any) specified in the Administrative Charges table in a Service Attachment.

“Cause” means a breach by the other Party of any material provision of the Agreement (including in relation to a particular Order) which: (i) is incapable of remedy; or (ii) if capable of remedy, remains uncured for 30 days from written notice of such breach; or (iii) in the case of Customer’s failure to pay any past due amount, 10 days from notice of such failure.

“Charges” means all amounts owed by Customer relating to the provision of Services as set out in the Agreement, and including Underutilization Charges and Early Termination Charges.

“Commencement Date” means: (a) for the USSA, the date on which both Parties agree to be bound by (whether by execution or some other method) the USSA; (b) for any Order (including in relation to a renewed Service), the date on which both Parties agree to be bound by (whether by execution or some other method) the Order or Verizon commences performance, whichever is the earlier; and (c) for a NSS the date that the Order is acknowledged by Verizon email to Customer.

“Commitment Effective Date” means the first day of the first full month following the Commencement Date.

“Confidential Information” means information (in whatever form): (a) designated as confidential; (b) relating to the Agreement including the existence of the Agreement itself; (c) relating to the Party’s business affairs, customers, products, developments, trade secrets, intellectual property rights, know-how or personnel; or (d) received or discovered at any time that the Agreement is in effect, or otherwise in connection with the Agreement, by a Party (including through an Affiliate or other agent), which information should reasonably have been understood as Confidential Information of the Party (or one of its Affiliates or subcontractors), either because of legends or other markings, the circumstances of disclosure or the nature of the information itself. Confidential Information does not include information that: (i) is in the possession of the receiving Party free of any obligation of confidentiality at the time of its disclosure, (ii) is or becomes publicly known other than by a breach of this provision, (iii) is received without restriction from a third party free to disclose it, or (iv) is developed independently by the receiving Party without reference to the Confidential Information.

“Content” means anything that can be accessed, received, transmitted, stored, processed or used – (whether actively or passively) - including any form of information, audio, image, computer program or other functionality.

“Contract” has the same meaning as Order.

“Contract Year” means the 12 month period beginning on the Commitment Effective Date and each anniversary thereafter, or as set forth in the Agreement.

“Convenience” means termination by a Party for any reason other than: (i) for Cause; (ii) if the other Party experiences an Insolvency Event; or (iii) pursuant to the clauses entitled Service Level Agreement or Force Majeure.

“CPE Services” means CPE related deployment, maintenance, assessment, rental, lease and other service furnished to Customer in connection with the CPE, Software or Customer Equipment.

“Customer” means the non-Verizon entity that agrees to be bound by (whether by execution or some other method) the USSA or an Order, as the context requires.

“Customer Data” means voice and data transmissions (including the originating and destination numbers and IP addresses, date, time, duration of voice or data transmissions, and other data necessary for the establishment, invoicing or maintenance of the transmission), data containing information regarding Customer, its employees and users including personal and/or private information and other data provided to or obtained by Verizon, Verizon Affiliates and their respective agents and employees in connection with the provision of the Services. A reference to Customer Data will include Regulated Customer Data where applicable.

“Customer Equipment” means any equipment, systems, software, cabling and facilities provided by or on behalf of Customer and used in conjunction with the Services at a Customer Site. Ownership of the Customer Equipment will not at any time vest in Verizon or a Verizon Affiliate.

"Customer Premises Equipment" or "CPE" means any equipment, systems, Software, cabling and facilities, including without limitation, handsets and other related materials, which is sold or otherwise furnished by Verizon to Customer as itemized in an Order.

"Customer Site" means the location specified by Customer at which Services are to be provided.

"Disputed Amount" means an amount which Customer disputes. A Disputed Amount may relate to the whole or part of an invoice(s).

"Due Date" means the date on which payment for Service by Customer is to be received by Verizon as set out in the Agreement.

"eSign" means the process designated by Verizon which permits an Agreement or Order to be executed electronically by Customer without the need for a hard copy signature.

"Early Termination Charges" means the charges calculated in accordance with the clause entitled Early Termination Charges.

"Eligible Charges" means all Charges, after application of all discounts and credits, incurred by Customer, specifically excluding: (a) Taxes; (b) Charges for CPE and CPE Services; (c) Third Party charges where Verizon or Verizon Affiliates act as agent for Customer in its acquisition of Services; (d) non-recurring charges; (e) Governmental Charges; (f) other Charges expressly excluded by the Agreement (including in any Service-specific pricing URL). Whether Charges are Eligible Charges does not depend on which Verizon entity is providing the Services. Charges of the same type, incurred by Participating Entities and subject to the Agreement, are treated as Eligible Charges for purposes of satisfying Customer's Volume Commitment(s).

"Emergency Works" mean works, the execution of which, at the time it is proposed to be executed, is required to put an end to, or prevent, the arising of circumstances then existing or imminent that are likely to cause: (a) danger to persons or property; (b) the interruption of any Services provided by the Verizon Facilities; (c) substantial loss to Verizon or any third party; and/or (d) such other works as in all the circumstances it is reasonable to execute with those works.

"Event" means any incident, event, statement, act or omission giving rise to any liabilities, claims or causes of action under or in connection with the Agreement including (but not limited to) contract, warranty, tort (including negligence), strict liability, misrepresentation, breach of statutory duty, breach of warranty or otherwise.

"Force Majeure Event" means an event beyond the reasonable control of the Party affected, including, but not limited to, acts of God, embargoes, governmental restrictions, strikes, riots, insurrection, wars or other military action, civil disorders, acts of terrorism, rebellion, fires, explosions, accidents, floods, vandalism, cable cuts and sabotage. Market conditions or fluctuations are not Force Majeure Events.

An "Insolvency Event" occurs when a Party: (i) files for bankruptcy; (ii) becomes or is declared insolvent, or is the subject of any bona fide proceedings related to its liquidation, administration, provisional liquidation, insolvency or the appointment of a receiver or similar officer for it; (iii) passes a resolution for its voluntary dissolution or liquidation, (iv) has a receiver or manager appointed over all, or substantially all, of its assets; (v) makes an assignment for the benefit of all, or substantially all, of its creditors; (vi) enters into an agreement or arrangement for the composition, extension, or readjustment of all, or substantially all, of its obligations or any class of such obligations; (vii) becomes incapable of paying its undisputed debts when due; or (viii) experiences an event analogous to any of the foregoing in any jurisdiction in which any of its assets are situated

"License" means a personal, non-exclusive, non-transferable, non-sublicensable license to use Software, in object code form only, solely in connection with Services for Customer's internal business purposes on Customer-owned or Customer-leased equipment.

"Master Terms" means the terms and conditions set out in this document including any Addendum to the Master Terms. The Master Terms may also be referred to as the Online Master Terms.

“Normal Business Hours” or “Normal Working Hours” or “Business Hours” means the hours between 8 am and 5 pm on Business Days in the time zone of the Customer Site. Verizon may vary Normal Business Hours by notice to Customer at any time.

“NSS” means No Sign SOF and refers to an Order which is accepted by Verizon via the NSS Process.

“NSS Process” means the process set out in the Agreement in the clause entitled No Sign SOF (NSS) Process.

“Optimized Service” means any Service, Software and CPE (including any CPE Services) optimized for Verizon’s automation platform, which is indicated by ‘+’ after the Service name (e.g., ‘Private IP +’). The ‘+’ is not a part of the Service name.

“Order” means a Customer request for one or more Services that is delivered by Customer to Verizon and effective and binding upon the Commencement Date.

“Participating Entity” means an entity authorized by the Customer entity that agrees to be bound by (whether by execution or some other method) the USSA under Verizon’s processes to contract for Services via an Order in Participating Entity’s own name subject to the terms of the Agreement.

“Party” means the particular Verizon or Customer entity that agrees to be bound by (whether by execution or some other method) the USSA or an Order, as applicable and “Parties” will be construed accordingly.

“Privacy Policy” means the applicable Verizon Privacy Policy set out at <http://www.verizonenterprise.com/privacy/>.

“Purchase Commitment” means a Service Commitment or a Volume Commitment. A Service may be subject to both a Service Commitment and a Volume Commitment if specified in the USSA or Order.

“Regulated Customer Data” means Customer Data the use, processing or transfer of which is regulated by law or regulation as personal data.

“Security” means a cash deposit, director's guarantee, company guarantee, letter of credit from an approved financial institution, or bank guarantee, or any combination of these.

“Services” means the specific services, and CPE (including any CPE Services) provided under the Agreement and may include Third Party Services.

“Service Activation Date” means the same as Activation Date.

“Service Attachment” means an online or paper document containing the terms for one or more Services. A Service Attachment may also be referred to as an Online Service Attachment, an Attachment or Service Terms.

“Service Commitment” means the period of time for which Customer is committed to pay for a particular Service, if any, as set out in the Agreement.

“Service Equipment” means any equipment, Software, systems, cabling and facilities provided by or on behalf of Verizon and used to facilitate provision of the Services at a Customer Site. Ownership of the Service Equipment does not pass to Customer. Service Equipment does not include Verizon Facilities.

“Service Order” or “SOF” has the same meaning as Order.

“Software” means any software and any related documentation provided to Customer as part of the Services and includes both Verizon and Third Party software.

“Subminimum Volume Commitment” means a Service-specific commitment to pay an agreed amount of Eligible Charges in each Contract Year.

“Tariff” means, where applicable, the tariffs on file as amended from time to time with the appropriate national or regional governmental body governing the rates and/or terms and conditions of Services that are subject to tariff filings, as applicable.

“Tax” and “Taxes” means applicable federal, state, local, foreign, sales, use, excise, utility, gross receipts, value-added and other taxes, tax-like charges, and tax-related and other surcharges.

“Third Party” means a third party vendor from whom Verizon sources products and services including CPE and CPE Services.

“Tiered Volume Commitment” means the total Eligible Charges Customer must pay during each Contract Year of the Volume Commitment Period, which amount may vary from Contract Year to Contract Year.

“Total Volume Commitment” or “TVC” means the total Eligible Charges which Customer must pay during the Volume Commitment Period to which Customer has committed under the Agreement.

“Underutilization Charge” means an amount owed by Customer if Customer’s Eligible Charges do not reach the Volume Commitment in any Contract Year and/or by the end of the Volume Commitment Period, as applicable

“United States” or “U.S.” means the 50 states, the District of Columbia, and the U.S. Territories.

“U.S. Governmental Charges” or “Governmental Charges” means charges that Verizon is required or permitted to collect from or pay to others, by a governmental or quasi-governmental authority, which include, but are not limited to, Universal Service Fund charges and payphone use charges, or any successor of any such charges.

“U.S. Service Agreement” or “USSA” means the agreement entered into by Verizon and Customer excluding Orders but including applicable Definitions. The USSA sets out the terms that Customer and Verizon agree will apply to all Orders under it. The USSA may be referred to by another title such as the Master Service Order Form to the U.S. Service Agreement.

“U.S. Services” means Services provided pursuant to an Order where the Verizon entity that executes the Order is legally organized in the U.S.

“Verizon” means the Verizon entity that is the contracting party to the USSA or an Order as the context requires (including by way of permitted assignment). For a standard contract not actually signed by Verizon, the relevant U.S. Verizon entity is identified either in the Service Attachment, or if not, in the rules at verizonenterprise.com/service/g_service_provider_list.htm.

“Verizon Facilities” or “Network” means any network or system, cable, transmission facility owned or leased by Verizon, or operated or managed on behalf of Verizon, excluding Service Equipment.

“Volume Commitment” means the agreed upon Customer commitment to purchase, and may be described as an Annual Volume Commitment, Total Volume Commitment, Tiered Volume Commitment, or Subminimum Volume Commitment.

“Volume Commitment Period” means the period of time that applies to the Volume Commitment beginning on the Commitment Effective Date.

Agreed to by the Parties’ authorized representative below.

Verizon Business Network Services Inc. on behalf of
MCI Communications Services, Inc. d/b/a Verizon Business
Services and the affiliates listed at
www.verizonenterprise.com/service/g_service_provider_list.htm

State of West Virginia, Office of Technology

By: _____

Name: _____

Title: _____

Date: _____

By: _____

Name: _____

Title: _____

Date: _____

**Schedule A
Service Attachments**

Exhibit 8 – WV96/Purchasing Affidavit/Disclosure of Interested Parties to Contracts

**STATE OF WEST VIRGINIA
ADDENDUM TO VENDOR'S STANDARD CONTRACTUAL FORMS**

State Agency, Board, or Commission (the "State"):

Vendor:

Contract/Lease Number ("Contract"):

Commodity/Service:

The State and the Vendor are entering into the Contract identified above. The Vendor desires to incorporate one or more forms it created into the Contract. Vendor's form(s), however, include(s) one or more contractual terms and conditions that the State cannot or will not accept. In consideration for the State's incorporating Vendor's form(s) into the Contract, the Vendor enters into this Addendum which specifically eliminates or alters the legal enforceability of certain terms and conditions contained in Vendor's form(s). Therefore, on the date shown below each signature line, the parties agree to the following contractual terms and conditions in this Addendum are dominate over any competing terms made a part of the Contract:

1. **ORDER OF PRECEDENCE:** This Addendum modifies and supersedes anything contained on Vendor's form(s) whether or not they are submitted before or after the signing of this Addendum. **IN THE EVENT OF ANY CONFLICT BETWEEN VENDOR'S FORM(S) AND THIS ADDENDUM, THIS ADDENDUM SHALL CONTROL.**
2. **PAYMENT** – Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software licenses, subscriptions, or maintenance may be paid annually in advance.

Any language imposing any interest or charges due to late payment is deleted.
3. **FISCAL YEAR FUNDING** – Performance of this Contract is contingent upon funds being appropriated by the WV Legislature or otherwise being available for this Contract. In the event funds are not appropriated or otherwise available, the Contract becomes of no effect and is null and void after June 30 of the current fiscal year. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.
4. **RIGHT TO TERMINATE** – The State reserves the right to terminate this Contract upon thirty (30) days written notice to the Vendor. If this right is exercised, the State agrees to pay the Vendor only for all undisputed services rendered or goods received before the termination's effective date. All provisions are deleted that seek to require the State to (1) compensate Vendor, in whole or in part, for lost profit, (2) pay a termination fee, or (3) pay liquidated damages if the Contract is terminated early.

Any language seeking to accelerate payments in the event of Contract termination, default, or non-funding is hereby deleted.
5. **DISPUTES** – Any language binding the State to any arbitration or to the decision of any arbitration board, commission, panel or other entity is deleted; as is any requirement to waive a jury trial.

Any language requiring or permitting disputes under this Contract to be resolved in the courts of any state other than the State of West Virginia is deleted. All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.

Any language requiring the State to agree to, or be subject to, any form of equitable relief not authorized by the Constitution or laws of State of West Virginia is deleted.
6. **FEES OR COSTS:** Any language obligating the State to pay costs of collection, court costs, or attorney's fees, unless ordered by a court of competent jurisdiction is deleted.
7. **GOVERNING LAW** – Any language requiring the application of the law of any state other than the State of West Virginia in interpreting or enforcing the Contract is deleted. The Contract shall be governed by the laws of the State of West Virginia.
8. **RISK SHIFTING** – Any provision requiring the State to bear the costs of all or a majority of business/legal risks associated with this Contract, to indemnify the Vendor, or hold the Vendor or a third party harmless for any act or omission is hereby deleted.
9. **LIMITING LIABILITY** – Any language limiting the Vendor's liability for direct damages to person or property is deleted.
10. **TAXES** – Any provisions requiring the State to pay Federal, State or local taxes or file tax returns or reports on behalf of Vendor are deleted. The State will, upon request, provide a tax exempt certificate to confirm its tax exempt status.
11. **NO WAIVER** – Any provision requiring the State to waive any rights, claims or defenses is hereby deleted.

- 12. **STATUTE OF LIMITATIONS** – Any clauses limiting the time in which the State may bring suit against the Vendor or any other third party are deleted.
- 13. **ASSIGNMENT** – The Vendor agrees not to assign the Contract to any person or entity without the State’s prior written consent, which will not be unreasonably delayed or denied. The State reserves the right to assign this Contract to another State agency, board or commission upon thirty (30) days written notice to the Vendor. These restrictions do not apply to the payments made by the State. Any assignment will not become effective and binding upon the State until the State is notified of the assignment, and the State and Vendor execute a change order to the Contract.
- 14. **RENEWAL** – Any language that seeks to automatically renew, modify, or extend the Contract beyond the initial term or automatically continue the Contract period from term to term is deleted. The Contract may be renewed or continued only upon mutual written agreement of the Parties.
- 15. **INSURANCE** – Any provision requiring the State to maintain any type of insurance for either its or the Vendor’s benefit is deleted.
- 16. **RIGHT TO REPOSSESSION NOTICE** – Any provision for repossession of equipment without notice is hereby deleted. However, the State does recognize a right of repossession with notice.
- 17. **DELIVERY** – All deliveries under the Contract will be FOB destination unless the State expressly and knowingly agrees otherwise. Any contrary delivery terms are hereby deleted.
- 18. **CONFIDENTIALITY** – Any provisions regarding confidential treatment or non-disclosure of the terms and conditions of the Contract are hereby deleted. State contracts are public records under the West Virginia Freedom of Information Act (“FOIA”) (W. Va. Code §29B-a-1, et seq.) and public procurement laws. This Contract and other public records may be disclosed without notice to the vendor at the State’s sole discretion.

Any provisions regarding confidentiality or non-disclosure related to contract performance are only effective to the extent they are consistent with FOIA and incorporated into the Contract through a separately approved and signed non-disclosure agreement.

- 19. **THIRD-PARTY SOFTWARE** – If this Contract contemplates or requires the use of third-party software, the vendor represents that none of the mandatory click-through, unsigned, or web-linked terms and conditions presented or required before using such third-party software conflict with any term of this Addendum or that is has the authority to modify such third-party software’s terms and conditions to be subordinate to this Addendum. The Vendor shall indemnify and defend the State against all claims resulting from an assertion that such third-party terms and conditions are not in accord with, or subordinate to, this Addendum.
- 20. **AMENDMENTS** – The parties agree that all amendments, modifications, alterations or changes to the Contract shall be by mutual agreement, in writing, and signed by both parties. Any language to the contrary is deleted.

Notwithstanding the foregoing, this Addendum can only be amended by (1) identifying the alterations to this form by using *Italics* to identify language being added and ~~striketrough~~ for language being deleted (do not use track-changes) and (2) having the Office of the West Virginia Attorney General’s authorized representative expressly agree to and knowingly approve those alterations.

Verizon Buss Net Svc Inc on behalf of MCI

State: _____

Vendor: Comm Svc Inc d/b/a Verizon Buss Services

By: _____

By: *OBI Udy Romaine*

Printed Name: _____

Printed Name: OBI ROMAINE

Title: _____

Title: SNR. ANALYST

Date: _____

Date: 08/27/2019

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

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

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

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

DEFINITIONS:

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

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

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

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

WITNESS THE FOLLOWING SIGNATURE: Verizon Business Network Svc Inc. on behalf of MCI

Vendor's Name: Communications Svc Inc, d/b/a Verizon Business Services

Authorized Signature: *Ali Udygomaine* Date: 08/27/2019

State of Oklahoma

County of Tulsa, to-wit:

Taken, subscribed, and sworn to before me this 27th day of August, 2019.

My Commission expires December 01, 2019

AFFIX SEAL HERE

JULIE FARSON
Notary Public, State of Oklahoma
Commission # 15010691
My Commission Expires December 01, 2019

NOTARY PUBLIC

Julie Farson

Purchasing Affidavit (Revised 01/19/2018)

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 \$1 million 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, but does not include publicly traded companies listed on a national or international stock exchange.

"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.

West Virginia Ethics Commission
Disclosure of Interested Parties to Contracts

(Required by W. Va. Code § 6D-1-2)

Verizon Business

Name of Contracting Business Entity: Network Services Inc. **Address:** One Verizon Way
Basking Ridge, NJ 07920

Name of Authorized Agent: Corporation Trust Company **Address:** Corporation Trust Center
1209 Orange Street, Wilmington, DE 19801

Contract Number: _____ **Contract Description:** _____

Governmental agency awarding contract: West Virginia Office of Technology

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: Obi Bomaine Date Signed: 08/27/2019

Notary Verification

State of Oklahoma, County of Tulsa:

I, Obi Bomaine, 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 27th day of August, 2019.

Julie Earsom
Notary Public's Signature

To be completed by State Agency:

Date Received by State Agency: _____

Date submitted to Ethics Commission: _____

Governmental agency submitting Disclosure: _____



Corporate Policy Statement

Policy No.: CPS-103
Issued: December 6, 2010
Subject: Authority to Approve Transactions



**APPENDIX 4
VERIZON TELECOM AND BUSINESS
CPS-103 LETTER OF DELEGATION OF AUTHORITY
FORM 101**

Within the authority granted to me in CPS-103, "Authority to Approve Transactions" and for post-Voluntary Separation Program, I delegate to:

*Michael O'Connor, Assoc Dir-Billing Solutions (VZ ID [REDACTED]);
James Chamlee, Sr Mgr-Billing Solutions (VZ ID [REDACTED]);
Adam S Davis, Sr Mgr-Fin Ops-Billing (VZ ID [REDACTED]);
Obi Romaine, Sr Analyst-Fin Ops-Billing (VZ ID [REDACTED]);
Angel Arrazola, Analyst-Fin Ops-Billing (VZ ID [REDACTED]);
Alix Court, Analyst-Fin Ops-Billing (VZ ID [REDACTED]); and
Nicole Clymer, Analyst-Fin Ops-Billing (VZ ID [REDACTED]).*

the authority to perform the following function:

Execute and deliver Verizon Telecom and Business Customer Contracts and Proposals requiring "wet ink" signatures, including any and all ancillary documents and amendments related thereto, that are duly approved in accordance with then-applicable Verizon Business corporate policies, including the use of stamp bearing facsimile of my signature in accordance with *Security Procedure for Anthony A. Recine, Senior Vice President, Pricing & Contract Management, Blue Ink Stamp Policy,*

and the authority to perform the following function:

the use of electronic signature bearing facsimile of my signature within Verizon Business's Adobe Sign, DocuSign, or any electronic signature system in place and also Customer's signature vendor, in compliance with the current Verizon Business Legal and Controller approved process, to execute and deliver Verizon Business Customer Contracts and Proposals, including any and all ancillary documents and amendments related thereto, that are duly approved with then-applicable Verizon Business corporate policies.

This will be effective beginning on April 22, 2019 and ending on June 30, 2019 when a new Delegation of Authority for Verizon Business Group 2.0 is created, or before if rescinded by me.

(Annual delegations must be completed by July 1st of each respective year and may not exceed one year from their effective date. Delegations with a start date other than July 1st should also include an end date of the subsequent June 30 or earlier.)

Exhibit 9 – Insurance & Indemnification Clarifications

8. INSURANCE: The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below and must include the State as an additional insured on each policy prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Within Thirty (30) days ~~of prior to~~ the expiration of the insurance policies, Vendor shall provide the Agency with a certificate of insurance as proof that the insurance mandated herein has been continued-

~~Upon receipt of notice from its insurer(s) Vendor must also provide Agency with thirty (30) day's prior written notice of immediate notice of any changes in its insurance policies, including but not limited to, policy cancellation of any coverage required herein, policy reduction, or change in insurers.~~

The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether or not that insurance requirement is listed in this section.

Vendor must maintain:

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

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

Professional/Malpractice/Errors and Omission Insurance in at least an amount of: \$1,000,000 per ~~claim and aggregate occurrence~~.

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

Cyber Liability Insurance in an amount of: _____ per occurrence.

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

Pollution Insurance in an amount of: _____ per occurrence.

Aircraft Liability in an amount of: _____ per occurrence.

Notwithstanding anything contained in this section to the contrary, the Director of the Purchasing Division reserves the right to waive the requirement that the State be ~~included named~~ as an additional insured as their interest may appear under this Agreement on one or more of the Vendor's insurance policies, except workers compensation and employer's liability and professional liability/errors and omissions if the Director finds that doing so is in the State's best interest.

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

Verizon takes exception to the above Indemnification requirements but is open to negotiating mutually agreeable indemnity provisions in the final Agreement similar to the following. Verizon will indemnify the Customer, its agents and employees, against any claim, loss, liability, fines, damages costs or expense for injury to or death of any persons and any loss or damage to any real or tangible property (collectively, 'Claim(s)') resulting from the negligent or other tortious acts or omissions of Verizon, its agents, representatives, employees or subcontractors, in the performance of work under this Agreement, except that Verizon, to the fullest extent permitted by applicable law, will not have any liability or responsibility to indemnify any person or entity for any such Claim(s), to the extent the same was caused by any negligent or other tortious act or omission of such person or entity. The person or entity seeking indemnity hereunder must provide Verizon with: (i) prompt written notice of any such Claim, and Verizon shall have the full right and opportunity to conduct the defense of all such Claims; and (ii) full information and all reasonable cooperation in support of such defense, and shall have the right to participate in such defense, but no costs or expenses shall be incurred for either party by the other party without such other party's prior written consent.