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

Header 5

List View

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

Procurement Folder: 2012913
Procurement Type: Central Contract - Fixed Amt
Vendor ID: VS0000037191
Legal Name: NETWORKING FOR FUTURE INC
Alias/DBA:
Total Bid: $614,832.63
Response Date: 08/11/2026
Response Time: 11:49
Responded By User ID: KevinReith
First Name: Kevin
Last Name: Reith
Email: kreith@nffinc.com
Phone: 2023049030

SO Doc Code: CRFQ
SO Dept: 0231
SO Doc ID: OOT2700000002
Published Date: 8/6/26
Close Date: 8/11/26
Close Time: 13:30
Status: Closed
Solicitation Description: Addendum No 4-Governance, Risk and Compliance Auto Platform
Total of Header Attachments: 5
Total of All Attachments: 5

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

State of West Virginia
Solicitation Response

Proc Folder:	2012913
Solicitation Description:	Addendum No 4-Governance, Risk and Compliance Auto Platform
Proc Type:	Central Contract - Fixed Amt

Solicitation Closes	Solicitation Response	Version
2026-08-11 13:30	SR 0231 ESR08112600000000917	1

VENDOR

VS0000037191
NETWORKING FOR FUTURE INC

Solicitation Number: CRFQ 0231 OOT2700000002

Total Bid: 614832.6300000000046566128730 **Response Date:** 2026-08-11 **Response Time:** 11:49:26

Comments: NFF is submitting our solution consisting of a comprehensive Apptega GRC software solution combined with Professional Services delivered in tandem by Apptega and NFF. Our CISO, Alan Edwards, is a specialist in GRC, and is well-versed in the entire solution set, including multi-tenancy and customization of the material. The Year 1 price is inclusive of all the modules, as well as the setup, implementation, and customization, and as a result, carries a higher price due to the aforementioned one-time costs. The additional years include on-going professional services & support, as well as agency support for when additional tenants come online.

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

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

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	GRC Software Maintenance and Support Year One (Initial term)	1.00000	EA	156324.240000	156324.24

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: NFF is submitting our solution consisting of a comprehensive Apptega GRC software solution combined with Professional Services delivered in tandem by Apptega and NFF. Our CISO, Alan Edwards, is a specialist in GRC, and is well-versed in the entire solution set, including multi-tenancy and customization of the material. The Year 1 price is inclusive of all the modules, as well as the setup, implementation, and customization, and as a result, carries a higher price due to the aforementioned one-time costs.

Extended Description:

Enter a grand total lump sum yearly price that is all inclusive of specifications:
4.1 ; 4.2 ; 4.3 ; 4.4 ; 4.5 ; 4.6 ; 4.7 ; 4.8 ; 4.9

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	GRC Software Maintenance and Support Year 2 renewal	1.00000	EA	143421.940000	143421.94

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: NFF is submitting our solution consisting of a comprehensive Apptega GRC software solution combined with Professional Services delivered in tandem by Apptega and NFF. Our CISO, Alan Edwards, is a specialist in GRC, and is well-versed in the entire solution set, including multi-tenancy and customization of the material. The Year 1 price is inclusive of all the modules, as well as the setup, implementation, and customization, and as a result, carries a higher price due to the aforementioned one-time costs.

Extended Description:

Enter a grand total lump sum yearly price that is all inclusive of specifications:
4.1 ; 4.2 ; 4.3 ; 4.4 ; 4.5 ; 4.6 ; 4.7 ; 4.8 ; 4.9

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	GRC Software Maintenance and Support Year 3 renewal	1.00000	EA	152621.470000	152621.47

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: NFF is submitting our solution consisting of a comprehensive Apptega GRC software solution combined with Professional Services delivered in tandem by Apptega and NFF. Our CISO, Alan Edwards, is a specialist in GRC, and is well-versed in the entire solution set, including multi-tenancy and customization of the material. The Year 1 price is inclusive of all the modules, as well as the setup, implementation, and customization, and as a result, carries a higher price due to the aforementioned one-time costs.

Extended Description:

Enter a grand total lump sum yearly price that is all inclusive of specifications:
4.1 ; 4.2 ; 4.3 ; 4.4 ; 4.5 ; 4.6 ; 4.7 ; 4.8 ; 4.9

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	GRC Software Maintenance and Support Year 4 renewal	1.00000	EA	162464.980000	162464.98

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: NFF is submitting our solution consisting of a comprehensive Apptega GRC software solution combined with Professional Services delivered in tandem by Apptega and NFF. Our CISO, Alan Edwards, is a specialist in GRC, and is well-versed in the entire solution set, including multi-tenancy and customization of the material. The Year 1 price is inclusive of all the modules, as well as the setup, implementation, and customization, and as a result, carries a higher price due to the aforementioned one-time costs.

Extended Description:

Enter a grand total lump sum yearly price that is all inclusive of specifications:
4.1 ; 4.2 ; 4.3 ; 4.4 ; 4.5 ; 4.6 ; 4.7 ; 4.8 ; 4.9

Apptega

Apptega, Inc.
1230 Peachtree Street, NE, Unit 2330
Atlanta, GA. 30309

April 21, 2026

This letter serves as confirmation that Networking for Future (NFF) is a partner of Apptega and in good standing. The partnership between NFF and Apptega has existed since 2024 and grants access to resources for serving clients within the US, LATAM, and EMEA.

The Apptega partner program consists of partners with services, skills and knowledge that serve clients with Governance, Risk, and Compliance needs. If you have any questions or require additional information, we would be pleased to respond to inquiries.

Bob Layton
Chief Revenue Officer
Bob.Layton@apptega.com
+1-713-822-2710

NFF
Delivering Net Results

Price Response

State of West Virginia

West Virginia Department of Information Technology (WVOIT)

WVOIT
Governance, Risk and Compliance (GRC) Automation Platform
Request for Quote CRFQ 0231 OOT2700000002

Prepared by:
Networking For Future, Inc.
700 12th Street, NW
Suite 700
Washington, DC 20005

eMM: 00012433
Federal Tax ID: 54-1819774
Phone: 202.783.9011
Fax: 202.783.9019

August 11, 2026

Price Response

Commodity	Price
GRC Software Maintenance and Support Year One (Initial term)	$156,324.24
GRC Software Maintenance and Support Year 2 renewal	$143,421.94
GRC Software Maintenance and Support Year 3 renewal	$152,621.47
GRC Software Maintenance and Support Year 4 renewal	$162,464.98
Total	$614,832.62

Networking For Future, Inc. • 700 12th Street NW, Suite 700 • Washington, DC 20005 • 202-783-9011 • www.nffinc.com

Apptega GRC Platform — RFQ Requirements Crosswalk

Legend: **Yes** (shaded green) = Apptega capability confirmed.

#	Requirement	Apptega Capability
SECTION A — Required Compliance Frameworks & Standards		
A1	ISO/IEC 20243-1:2023 (O-TTPS Supply Chain Risk Management)	**Yes**
A2	CMMI (Capability Maturity Model Integration)	**Yes**
A3	CMMC Level 1	**Yes**
A4	CMMC Level 2	**Yes**
A5	ISO 9001 (Quality Management)	**Yes**
A6	ISO/IEC 27001:2022	**Yes**
A7	PCI DSS	**Yes**
A8	ISO/IEC TS 20000-11:2021 (ITSM / cloud guidance)	**Yes**
A9	SOC 2	**Yes**
SECTION B — 4.1 Software Maintenance, Support & Deployment Sizing		
4.1.1	Deployment sizing: central hub + 125 fully segregated child workspaces natively included	**Yes**
4.1.2	Initial contract term of one (1) year	**Yes**
4.1.3	Up to 3 optional 1-year renewals (4-yr total), same pricing/terms	**Yes**
4.1.4	On-demand workspace expansion at fixed unit price, prorated mid-term billing, full rate at renewal	**Yes**
SECTION B — 4.2 Training Deliverables		
4.2.1	Formal train-the-trainer program: virtual, instructor-led sessions for central administrators	**Yes**
4.2.2	On-demand digital training materials, video tutorials, or manuals for local end users	**Yes**
SECTION B — 4.3 Architectural, RBAC & Dashboard Requirements		
4.3.1	Central hub dashboard: CISO-level aggregate real-time compliance/risk posture across all entities	**Yes**
4.3.2	Granular RBAC enforcing strict data isolation — local entities see only their own workspace	**Yes**
4.3.3	Predefined + custom roles: workspace security officer, read-only external auditor (specific files), dashboard-only executive observer, global admin	**Yes**
4.3.4	Automated executive dashboard & audit export: compliance summaries, SSPs in PDF, Excel, CSV	**Yes**
SECTION B — 4.4 Platform Authentication & SSO		
4.4.1	Native SAML 2.0 AND OpenID Connect (OIDC) SSO, with MFA	**Yes**
4.4.2	Native integration with WVOT's Microsoft Entra ID tenant for state-issued credential auth	**Yes**
SECTION B — 4.5 Tiered & Modular Licensing		
4.5.1	Core tier (every workspace): framework libraries incl. custom + NIST, audit logging, RBAC, SSO, custom questionnaire engine	**Yes**
4.5.2	CCM add-on: native API evidence collection from Entra ID, Google Workspace, Palo Alto Networks, SentinelOne, Active Directory	**Yes**
4.5.3	Vendor solely responsible for maintaining native API connectors at no added cost, for contract life	**Yes**

#	Requirement	Apptega Capability
4.5.4	TPRM add-on: selectively enabled per workspace for vendor risk tracking + questionnaire automation	**Yes**
4.5.5	Dedicated implementation professional services for initial API integrations to core security stack	**Yes**
SECTION B — 4.6 Custom Assessments & Questionnaire Engine		
4.6.1	Custom questionnaire builder: design, schedule, and distribute custom risk assessments to any workspace	**Yes**
4.6.2	Single answer + evidence auto-scores, cross-maps, and updates maturity baselines across ALL selected frameworks simultaneously (WVCSF + NIST, etc.)	**Yes**
SECTION B — 4.7 Hybrid Environment Tracking (Cloud & On-Prem)		
4.7.1	Concurrent hybrid (cloud + on-premises) compliance tracking inside a single sandboxed workspace	**Yes**
4.7.2	Automated evidence ingestion (dynamic config checks) from AWS, Azure, GCP, Active Directory, Cisco, Palo Alto Networks	**Yes**
4.7.3	Manual, workflow-driven evidence upload portals for legacy/on-prem systems (SSPs, physical security proofs, CSV exports)	**Yes**
SECTION B — 4.8 Risk Register & POAM Management		
4.8.1	Centralized Risk Register generating and tracking POA&Ms	**Yes**
4.8.2	Formal Risk Exception workflow: local agencies submit exception + justification for central CISO review/approval	**Yes**
SECTION B — 4.9 Service Level Agreement (SLA) & Support		
4.9.1	Minimum 99.9% guaranteed system uptime	**Yes**
4.9.2	Standard technical support 8:00 AM–5:00 PM EST, Mon–Fri, with defined critical-outage response times	**Yes**

NFF
Delivering Net Results

Quote Response

State of West Virginia

West Virginia Department of Information Technology (WVOIT)

WVOIT
Governance, Risk and Compliance (GRC) Automation Platform
Request for Quote CRFQ 0231 OOT2700000002

Prepared by:
Networking For Future, Inc.
700 12th Street, NW
Suite 700
Washington, DC 20005

eMM: 00012433
Federal Tax ID: 54-1819774
Phone: 202.783.9011
Fax: 202.783.9019

August 11, 2026

Table of Contents

Networking For Future, Inc. • 700 12th Street NW, Suite 700 • Washington, DC 20005 • 202-783-9011 • www.nffinc.com

Cover Letter

August 11, 2026

Dear Proposal Evaluation Committee,

Networking for Future Inc. (NFF) is pleased to submit a concise and cost-effective proposal in response to the State of West Virginia Governance, Risk and Compliance (GRC) Automation Platform, Request for Quote (RFQ) CRFQ 0231 OOT2700000002 . Careful attention has been given in reviewing the requirements and providing a relevant and informative response.

As a technology solutions provider, NFF's core business practices align perfectly with the requirements of the RFQ. Our core NFF business strengths, coupled with over 30 years of IT compliance and solutions experience, provide the right combination of experience and capabilities to deliver current and future temporary staffing services to WVOIT.

NFF has read, understood, and will comply with all provisions of the RFQ with no exceptions or deviations taken or conditional assumptions made with respect to the requirements of the solicitation.

The NFF business information is:

Name:	Networking For Future Inc.
Address:	700 12th Street, NW Suite 700 Washington, DC 20005
Telephone:	202.783.9011
Federal Tax ID:	54-1819774
Small Business #:	LSZX32750102022

Please feel free to contact us should you have any questions.

Sincerely,

Kevin Reith

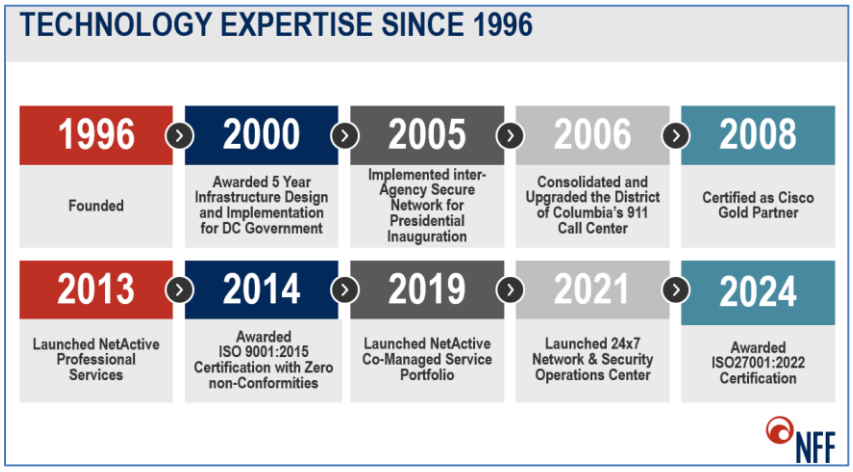
Kevin Reith
Client Engagement Executive – West Virginia
Networking For Future Inc.
233-D Heavner Avenue
Elkins, WV 26241
kreith@nffinc.com
202 304 9030

Experience and Qualifications of NFF

Brief Overview of NFF

Networking For Future (NFF) is a Washington, DC-based company, with offices in West Virginia, Maryland and Virginia, offering a performance-focused approach to delivering transformational IT business solutions.

Founded in 1996, our expertise includes GRC, solutions for Artificial Intelligence Enablement, Data Center & Cloud, Intelligent Networks, Secure, Connected IoT Technologies, Professional and Managed Services, and Zero Trust Strategies.



We are an accomplished technology consulting and professional services firm with a proven track record of delivering innovative, high-performance IT solutions to clients across government and commercial sectors. What sets us apart is our foundation as a hands-on, technically driven organization backed by deep industry partnerships and a broad portfolio of certifications – at both the company and individual levels. This combination of experience and credibility allows us to respond with confidence and precision to complex technical challenges.

NFF employs approximately 80 people, our primary marketplace focus is State and local government, Federal Government and Education. Since inception, NFF has successfully managed over $130M worth of performance-based task order hardware, software and services contracts.

NFF Corporate ISO Certifications

NFF's ISO 9001:2015 certification is a testament of our commitment to providing the highest degree of quality and improving our client business efficiency in every product, solution, service, and endeavor of our company. The NFF management processes, as well as its project and program delivery procedures, have been repeatedly audited and certified to ISO 9001 standards. **Our last audit was in 2024 without any nonconformities.**

NFF's ISO 27001:2022 certification demonstrates our commitment to the highest levels of information security, emphasizing the quality, professionalism, and reliability of our work. This is more than just a compliance check mark, it's a testament to the strength of our processes, the dedication of the NFF team, and the trustworthiness of our services. For our clients, it reinforces confidence that their data is handled with the utmost care and security.

NFF Clients

CLIENTS

STATE AND LOCAL GOVERNMENT

- Botetourt County, VA
- City of Raleigh, NC
- District of Columbia Government
  - Chief Technology Officer (OCTO)
  - Chief Financial Officer (OCFO)
  - Child and Family Services
  - Court System
  - Dept. of Behavioral Health
  - Dept. of Employment Services
  - Dept. of General Services
  - Dept. of Human Services
  - Department of Transportation
  - Fire and EMS
  - Homeland Security Agency
  - Housing Authority
  - Metropolitan Police Department
  - Office of the DC Auditor
  - Office of Unified Communications (OUC)
- Loudoun County, Virginia
- Prince William County, Virginia
- Virginia Innovation Partnership Corp. Va. Smart Community Testbed
- West VA. Board of Osteopathic Medicine
- West VA. Dept of Education
- West VA. Dept of Environ. Protection
- West VA. Dept of Highways
- West VA. Dept of Homeland Security
- West VA. Dept of Human Services
- West VA. Dept. of Transportation
- West VA. Div. of Financial Institutions
- West VA. Office of Technology (WVOT)
- West VA. State Police

EDUCATION AND LIBRARIES

K-12 AND LIBRARIES

- Cabell County West Va Public Schools
- District of Columbia Public Schools
- District of Columbia Public Libraries
- E.W. Stokes Public Charter School
- French International School
- Prince George's County, MD Library
- Prince William County, VA Library
- Quantico Middle/High School
- Saint Stephen's & Saint Agnes School
- The Boy's Latin School of Maryland
- Trinity Christian School of Fairfax
- Tyler County West VA. Public Schools
- Washington International School

HIGHER EDUCATION

- Allegany College of Maryland
- Georgetown University & Law Center
- George Washington University (CAAREN)
- Marshall University
- Marymount University
- Morgan State University
- New Jersey Institute of Technology
- Notre Dame of Maryland University
- St. Johns College
- The Catholic University of America
- University of Maryland
  - Applied Research Laboratory
  - Baltimore County (UMBC)
  - Center for Environmental Science
- University of the District of Columbia
- W.Va. School of Osteopathic Medicine

CLIENTS

FEDERAL GOVERNMENT	COMMERCIAL AND ENTERPRISE	TRANSPORTATION & CRITICAL INFRASTRUCTURE	HEALTHCARE & NON-PROFIT
■ Embassy of Australia	■ Acme Paper Supply Company	■ DC Dept. of Transportation	■ American Institute of Architects
■ The MITRE Corporation	■ Cisco Systems	■ DC Water and Sewer Authority	■ American Nurses Association
■ United States Government Agencies	■ Cabling Systems	■ Metropolitan Washington Airports Authority (MWAA)	■ Concord St. Andrews Church
➢ Census Bureau	■ CSSI Inc.	■ Pr. William County Service Authority	■ DC Bar Association
➢ Court of Appeals for Veteran Claims	■ Donohoe Construction	■ Washington Metropolitan Area Transit Authority (WMATA)	■ DC Government Dept. of Health
➢ Director of National Intelligence (ODNI)	■ FEI Construction Company	■ Washington Suburban Sanitary Commission (WSSC)	■ DC Government Dept. of Health Care Finance
➢ Federal Reserve System	■ HITT Construction Company	■ West VA Dept. of Transportation	■ DC Government Health Benefit Exchange Authority
➢ General Services Administration (GSA)	■ IET Corporation	■ West VA. Division of Highways	■ Global Giving Foundation
➢ Institute of Peace	■ Smoot Construction		■ Metropolitan Washington Council of Governments
➢ Mine Safety/Health Review Commission			■ National Parks Conservation Assn
➢ Occupational Safety & Health Comm.			■ United Medical Center
➢ Postal Regulatory Commission			
➢ Smithsonian Museum			
➢ US Surface Transportation Board			
➢ US Tax Court			

Key NFF Partners

NFF Letter of Authorization - Apptega

Apptega

Apptega, Inc.
1230 Peachtree Street, NE, Unit 2330
Atlanta, GA. 30309

April 21, 2026

This letter serves as confirmation that Networking for Future (NFF) is a partner of Apptega and in good standing. The partnership between NFF and Apptega has existed since 2024 and grants access to resources for serving clients within the US, LATAM, and EMEA.

The Apptega partner program consists of partners with services, skills and knowledge that serve clients with Governance, Risk, and Compliance needs. If you have any questions or require additional information, we would be pleased to respond to inquiries.

Bob Layton
Chief Revenue Officer
Bob.Layton@apptega.com
+1-713-822-2710

P: 888-221-3911
Apptega.com

NFF – Vender Preference Form for Small Business

WV-10
Approved / Revised
06/08/18

State of West Virginia

VENDOR PREFERENCE CERTIFICATE

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

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

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

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

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

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

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

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

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

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

8. **Application is made for reciprocal preference.**
☐ Bidder is a West Virginia resident and is requesting reciprocal preference to the extent that it applies.

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

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

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

Bidder: Networking For Future (NFF) **Signed:** Christopher Peabody

Date: 8/7/2026 **Title:** Chief Strategy Officer

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

NFF maintains the following Washington, DC Department of Small and Local Business Development (DSLBD) certifications:

- Certified business enterprise (CBE)
- Small business enterprise (SBE)
- Longtime resident business (LRB)
- Local business enterprise (LBE)
- Local business enterprise, principal offices located in an enterprise zone (DZE)

DEPARTMENT OF SMALL AND LOCAL BUSINESS DEVELOPMENT

CBE Number: LSZX55657082028
Certification Period: 08/08/2025 – 08/08/2028

BUSINESS CERTIFICATION DIVISION
441 4TH Street, N.W., Suite 850N
Washington, D.C. 20001

Date Issued: 08/08/2025
Certification Categories: LBE, SBE, DZE, LRB

CERTIFICATE OF BUSINESS CERTIFICATION

This acknowledges that

NETWORKING FOR FUTURE INC.

Has fulfilled the requirements to be considered a Certified Business Enterprise (CBE). A CBE is a business that is headquartered in the District of Columbia and meets all Local Business Enterprise (LBE) requirements. Businesses with CBE certification receive preference in procurement and contracting opportunities. Pursuant to 2-218.63 this certification can be revoked if a business is found to have violated the laws that govern the CBE program.

DSLBD
DEPT. OF SMALL & LOCAL BUSINESS DEVELOPMENT

DIRECTOR
Rosemary Suggs-Evans

GOVERNMENT OF THE DISTRICT OF COLUMBIA
MURIEL BOWSER, MAYOR

NFF Bid Document Signatures

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.

(Printed Name and Title) Kevin Reith, Sales Director – WV State/Local/Education

(Address) 233 - D Heavner Avenue. ELKINS, WV 26241

(Phone Number) / (Fax Number) (202) 304 - 9030 // (202) 783 - 9019

(email address) kreith@nffinc.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through *wv*OASIS, I certify that: I have reviewed this Solicitation/Contract 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/Contract 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 this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; 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; 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.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Networking For Future (NFF), Inc
(Company)

Kevin J. Reith
(Signature of Authorized Representative)

Kevin Reith, Sales Director – WV State/Local/Education
(Printed Name and Title of Authorized Representative) (Date)

(202) 304 - 9030 // (202) 783 - 9019
(Phone Number) (Fax Number)

kreith@nffinc.com
(Email Address)

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

Contract Manager: Alan Edwards

Telephone Number: (202) 266 - 4741

Fax Number: (202) 783 - 9019

Email Address: aedwards@nffinc.com

NFF Addendum Acknowledgements

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ OOT27*002

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

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

Addendum Numbers Received:
(Check the box next to each addendum received)

[X]	Addendum No. 1	[ ]	Addendum No. 6
[X]	Addendum No. 2	[ ]	Addendum No. 7
[X]	Addendum No. 3	[ ]	Addendum No. 8
[X]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	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.

Networking For Future (NFF)
Company

Kevin Reith
Authorized Signature

8/9/2026
Date

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

NFF Certificate of Insurance

Client#: 1894154 NETWOFOR4

ACORD™ CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 5/06/2026

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer any rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME: Shannon Cole
USI Insurance Services LLC 101 West Main St Suite 900 Norfolk, VA 23510	PHONE (A/C, No, Ext): 757-663-4030 FAX (A/C, No): 610-537-4196 E-MAIL ADDRESS: shannon.cole@usi.com

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A : National Fire Insurance Co. of Hartford	20478
INSURER B : Continental Casualty Company	20443
INSURER C : Continental Insurance Company	35289
INSURER D : Hanover Insurance Company	22292
INSURER E :	
INSURER F :	

INSURED
Networking for Future, Inc.
700 12th St. NW
Ste 700
Washington, DC 20005

COVERAGES CERTIFICATE NUMBER: REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X COMMERCIAL GENERAL LIABILITY			7092168501	05/06/2026	05/06/2027	EACH OCCURRENCE	$2,000,000
	CLAIMS-MADE X OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	$1,000,000
							MED EXP (Any one person)	$15,000
							PERSONAL & ADV INJURY	$2,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$4,000,000
	X POLICY PRO-JECT LOC						PRODUCTS - COMP/OP AGG	$4,000,000
	OTHER:							$
A	AUTOMOBILE LIABILITY			BUA7092168482	05/06/2026	05/06/2027	COMBINED SINGLE LIMIT (Ea accident)	$1,000,000
	ANY AUTO						BODILY INJURY (Per person)	$
	OWNED AUTOS ONLY / SCHEDULED AUTOS						BODILY INJURY (Per accident)	$
	X HIRED AUTOS ONLY / X NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$
								$
B	X UMBRELLA LIAB X OCCUR			CUE7092168465	05/06/2026	05/06/2027	EACH OCCURRENCE	$10,000,000
	EXCESS LIAB CLAIMS-MADE						AGGREGATE	$10,000,000
	DED X RETENTION $10000							$
C	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N			WC792168529	05/06/2026	05/06/2027	X PER STATUTE OTH-ER	
	ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? Y	N / A					E.L. EACH ACCIDENT	$1,000,000
	(Mandatory in NH)						E.L. DISEASE - EA EMPLOYEE	$1,000,000
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - POLICY LIMIT	$1,000,000
B	E&O w/ Cyber Liab			7092170569	05/06/2026	05/06/2027	$5,000,000 / $25K DED	
D	3rd Party Crime			BDRH60533005	05/06/2026	05/06/2027	$5,000,000 / $25K DED	
D	EPLI w/ 3rd Party			LHRH65290505	05/06/2026	05/06/2027	$1,000,000 / $25K DED	

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
EPLI = Employment Practices Liability

CERTIFICATE HOLDER
Networking For Future, Inc.
700 12th Street NW, Suite 700
Washington, DC 20005

CANCELLATION
SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE
Shannon Snyder Cole

ACORD 25 (2016/03) 1 of 1 #S54064616/M54059843 The ACORD name and logo are registered marks of ACORD TAGZP

NFF GRC Program Manager For West Virginia

ALAN EDWARDS
EdwardsAlanJ@gmail.com
(703) 623-1763

CHIEF INFORMATION SECURITY OFFICER

Clearance Level: Public Trust

Executive technology leader and business partner with CIO/CISO level success driving IT strategic planning, cyber security, organization design, operations, enterprise IT governance, capacity/cost projections, help desk, application support, and service delivery in dynamic, high-growth environments. Broad-based experience, from infrastructure engineer to entrepreneur to CIO/CISO-level executive leadership.

SKILLS

- Microsoft Windows (2008/2012/2016/2019/2022)
- Windows Desktop (7/8/10/11)
- Windows Terminal Services
- VMware
- HyperV
- MacOS
- Android
- IoS. AWS
- MS Azure Microsoft Active Directory (AD)
- Azure AD
- Kaseya
- Connectwise Automate
- Comodo Dragon StorageCraft
- StorageGUARD
- Intronis
- Backbone
- eFolder
- Carbonite Labtech
- GFI Max
- Ninja RMM
- Zendesk
- IT Glue SolarWinds Product Suite
- Mailprotector
- Proofpoint
- Spam Titan
- Avanon
- Ironscales
- McAfee
- Comodo
- BitDefender Cisco/HP/Aruba/Unifi Switches
- TCP/IP
- DNS
- DHCP
  FTP
- VPN
- Cisco Phones
- Cisco Unified Communications Manager
- Ruckus/Unifi Wireless
- WatchGuard/Sophos/Caliptix/pfSense Firewalls
- VoIP Broadview/CoreDial/8x8/LogMeIn ITIL
- NIST
- COBIT
- PCI
- HIPAA
- PII
- HITECH
- SOX
- CMMC
- ISO 27001 / 9001
- Malwarebytes
- AVG
- Kaspersky
- Symantec
- Panda

1

ALAN EDWARDS
EdwardsAlanJ@gmail.com
(703) 623-1763

CHIEF INFORMATION SECURITY OFFICER

- Microsoft Security Baseline Analyzer (MBSA) Webroot

CERTIFICATIONS

- CISSP
- CISM
- CMMC Practitioner
- ITIL Foundations

EDUCATION

BSc Honors — **1991**
Lancaster University, UK
Physics / Electronics

PGCE / MSc — **1992**
Lancaster University, UK
Secondary Education (Physics, Chemistry, Biology, Mathematics)

WORK EXPERIENCE

Chief Information Security Officer | **Networking for Future, Inc.** | **November 2022 - Current**

- Brought in as NFF's CISO to expand the security practice and obtain MSP Verify, SOC2, ISO9001, and ISO27001 compliance.
- Quadrupled their Microsoft 365 score and got them through an 18-month evidence-based compliance certification in under 12 months.
- Identified areas of improvement for security, evaluated dozens of products, and implemented a suite of tools to increase security for NFF and the client base. The decision criteria were cost, efficacy, ease of implementation, support requirements, and scalability.
- Built a security practice for the NFF client base of state and local government, higher education, and other highly regulated organizations.
- Present analysis of issues, solutions, and results to executives and board members.

Chief Information Officer (CIO) | **Computerware Inc.** | **May 2015 – November 2022**

- Led a $20M IT service provider for business, government, education, finance, and healthcare organizations, offering IT security, Cloud software/hardware, and managed services, providing primary IT services for 80 firms.
- Joined as CIO to revitalize a stagnant IT services division.

2

ALAN EDWARDS
EdwardsAlanJ@gmail.com
(703) 623-1763

CHIEF INFORMATION SECURITY OFFICER

- Served as company CIO, CISO, and Enterprise Architect, delivering enterprise-level IT support and solutions focused on uniform delivery, service optimization, cybersecurity, risk mitigation, and innovation to meet business growth goals.
- Relieved technology-induced pain points and improved operations efficiency, productivity, reliability, security, compliance, cost control, and user experience.
- Developed technology roadmaps to maximize IT investments and provide secure IT infrastructures.
- Facilitated C-suite meetings, conducted technology assessments, managed project implementations and vendor relations, and delegated resources.
- Managed internal and outsourced project teams.
- Rectified a cybersecurity flaw in Webroot Antivirus management portal used to distribute ransomware to over 600 systems. Worked with clients, cyber insurance, threat actors, and the FBI to recover systems, ensuring security and business continuity for 15 companies. Reverse engineered a decryption tool and provided it to the FBI; invited to join FBI InfraGard.
- Devised an innovative IoT solution providing predictive analytics to protect freezers for large-scale food storage, ensuring USDA compliance, reducing costs, and improving quality control for a major food manufacturer.
- Identified lack of internal controls, implemented process changes in accounting functions, saving 30% in non-salary costs, and improved transparency in contracts, invoices, and payments.
- Tripled Managed Services business by optimizing systems, automation, and service/product standardization, increasing contract value and client engagement. Designed tools to reduce time, avoid sales errors, and increase revenue.
- Designed and built a scalable, secure, HIPAA- and PCI-compliant infrastructure for healthcare practice, expanding to 9 locations across 3 states.

President + Virtual Chief Information Officer (CIO) & Chief Technical Officer (CTO)	**Whitehorse Technology Solutions LLC**	**July 2004 – May 2015**

- Managed IT service provider to healthcare, law, financial, hospitality firms, and government contractors.
- Launched and led an IT security and services consultancy; successfully sold to Computerware.
- Provided IT strategy, direction, and oversight for the design, development, operation, and support of IT systems and programs, including enterprise architecture, application management, security and risk management, infrastructure, networks, operations support, and project management.

3

ALAN EDWARDS
EdwardsAlanJ@gmail.com
(703) 623-1763

CHIEF INFORMATION SECURITY OFFICER

- Prepared clients for PCI, SOX, and HIPAA compliance audits and implemented standard frameworks (NIST, ITIL) to reduce risk profiles.
- Negotiated with third-party partners and vendors, managing relationships and service agreements.
- Hired and managed four engineers, administrative staff, and an outsourced helpdesk expansion.
- Supported over 40 organizations and managed a $2.5M budget.
- Built an IT services company using expertise in enterprise system management and sales acumen. Created economies of scale and reduced management tasks by treating different organizations as branches of a single entity.
- Forged relationships with senior-level stakeholders, serving as a trusted advisor to 60 unique clients (embassies, publicly traded corporations, and nonprofits) in the US and UK. Communicated business cases, cost/benefit analyses, and risk assessments.
- Headed the IT organization as outsourced CIO at a large embassy with 250 staff, rectifying a history of publicly reported data breaches and achieving zero incidents over 8 years despite being a target for foreign government compromises.
- Established IT infrastructure, security frameworks, and systems for a startup, expanding to nearly 20 sites with standardized setup and implementation procedures. Transitioned IT support to an in-house team as the company grew to 200 nationwide sites, maintaining the architecture and security frameworks.
- Instrumental in exposing and aiding the prosecution of a tech theft ring at Atlanta airport by collaborating with law enforcement.
- Successfully sold the firm to Computerware and merged operations seamlessly between the two companies

IT Manager	Capri Global Capital Ltd.	2001 – 2005

- Oversaw system and network administration, infrastructure, information security, IT asset management, incident management, and remote help desk for a $3 billion mortgage company with 50 employees.
- Integrated 3 sites into a unified management and reporting structure, ensuring the company met federal reporting deadlines and audit standards.
- Ensured security and operational functionality across the organization.
- Managed a 3-person IT team across 3 locations.

Presales Engineer	Orsus Solutions	2000 – 2001

- Technical expert in early-stage startups and industry leader in Wireless Markup Language (WML) development, delivering mobile-friendly web capabilities.

4

ALAN EDWARDS
EdwardsAlanJ@gmail.com
(703) 623-1763

CHIEF INFORMATION SECURITY OFFICER

- Presented to C-suite executives, translating technical concepts into nontechnical terms to better understand their businesses and challenges.
- Developed and built mobile applications to showcase the development environment to clients.

Presales Engineer	**IBM (Tivoli)**	**1999 – 2000**

- Supported the enterprise remote management platform that was managing the IT for the US Army globally and the IRS.

Network Engineer	**United Nations**	**1993 – 1999**

- Rwanda, Serbia, Croatia postgenocide Department of Peace Keeping Operations (DPKO)
- Supporting all UN and associated military contingents' IT and cybersecurity needs.

Teacher	**Starehe Boy's Center and School**	**1992 – 1993**

- Physics, Chemistry, Biology, and Mathematics teacher for high school and 1st-year college levels.
- Instructed laboratory technicians on mechanical engineering and electronics for equipment repair and maintenance.

5

NFF – Apptega Solution for West Virginia OIT

1. NFF Compliance Matrix For West Virginia GRC Requirements

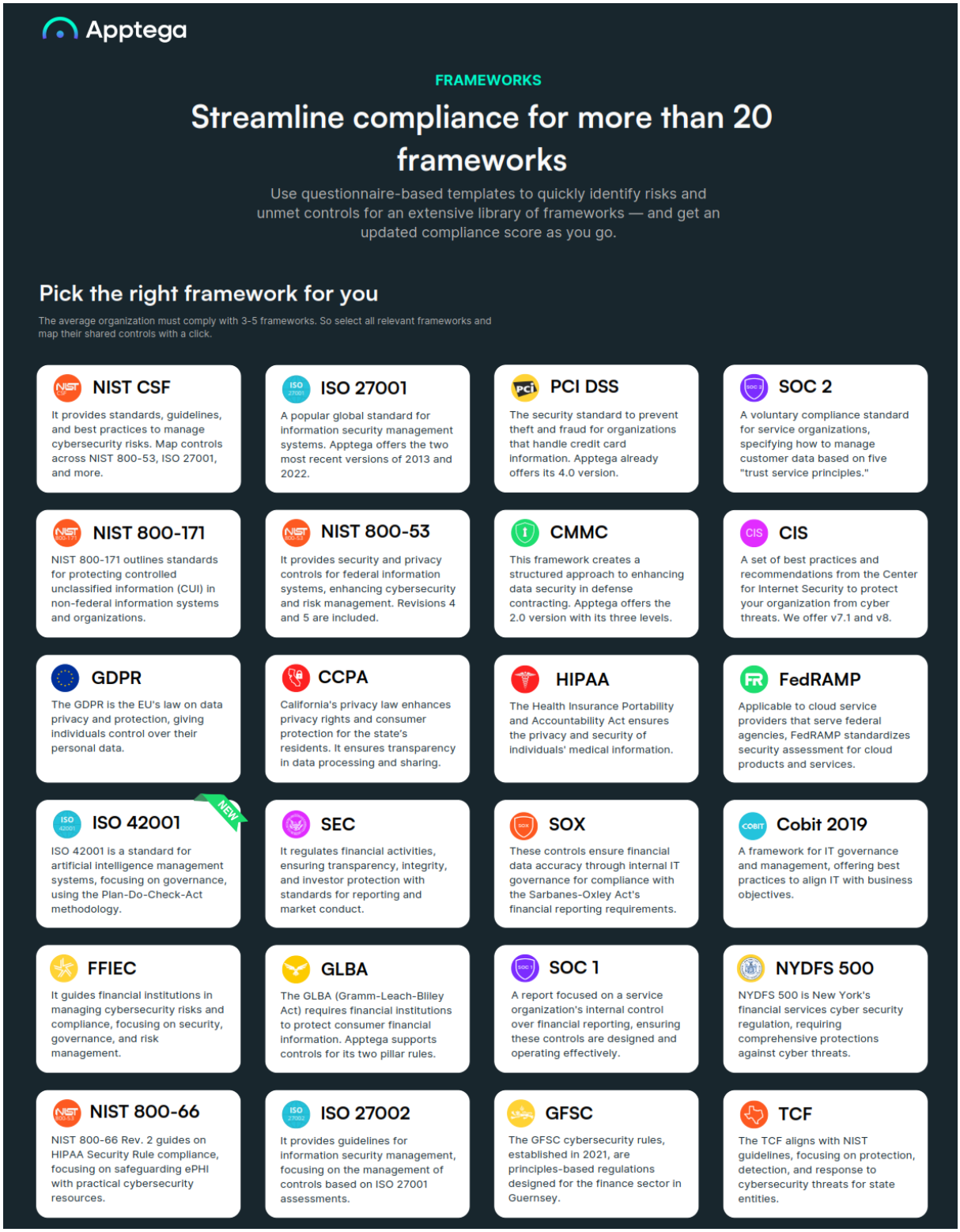
NFF / Apptega GRC Platform — RFQ Requirements Crosswalk

Legend: **Yes** (shaded green) = Apptega capability confirmed.

#	Requirement	Apptega Capability
SECTION A — Required Compliance Frameworks & Standards		
A1	ISO/IEC 20243-1:2023 (O-TTPS Supply Chain Risk Management)	**Yes**
A2	CMMI (Capability Maturity Model Integration)	**Yes**
A3	CMMC Level 1	**Yes**
A4	CMMC Level 2	**Yes**
A5	ISO 9001 (Quality Management)	**Yes**
A6	ISO/IEC 27001:2022	**Yes**
A7	PCI DSS	**Yes**
A8	ISO/IEC TS 20000-11:2021 (ITSM / cloud guidance)	**Yes**
A9	SOC 2	**Yes**
SECTION B — 4.1 Software Maintenance, Support & Deployment Sizing		
4.1.1	Deployment sizing: central hub + 125 fully segregated child workspaces natively included	**Yes**
4.1.2	Initial contract term of one (1) year	**Yes**
4.1.3	Up to 3 optional 1-year renewals (4-yr total), same pricing/terms	**Yes**
4.1.4	On-demand workspace expansion at fixed unit price, prorated mid-term billing, full rate at renewal	**Yes**
SECTION B — 4.2 Training Deliverables		
4.2.1	Formal train-the-trainer program: virtual, instructor-led sessions for central administrators	**Yes**
4.2.2	On-demand digital training materials, video tutorials, or manuals for local end users	**Yes**
SECTION B — 4.3 Architectural, RBAC & Dashboard Requirements		
4.3.1	Central hub dashboard: CISO-level aggregate real-time compliance/risk posture across all entities	**Yes**
4.3.2	Granular RBAC enforcing strict data isolation — local entities see only their own workspace	**Yes**
4.3.3	Predefined + custom roles: workspace security officer, read-only external auditor (specific files), dashboard-only executive observer, global admin	**Yes**
4.3.4	Automated executive dashboard & audit export: compliance summaries, SSPs in PDF, Excel, CSV	**Yes**
SECTION B — 4.4 Platform Authentication & SSO		
4.4.1	Native SAML 2.0 AND OpenID Connect (OIDC) SSO, with MFA	**Yes**
4.4.2	Native integration with WVOT's Microsoft Entra ID tenant for state-issued credential auth	**Yes**
SECTION B — 4.5 Tiered & Modular Licensing		
4.5.1	Core tier (every workspace): framework libraries incl. custom + NIST, audit logging, RBAC, SSO, custom questionnaire engine	**Yes**
4.5.2	CCM add-on: native API evidence collection from Entra ID, Google Workspace, Palo Alto Networks, SentinelOne, Active Directory	**Yes**
4.5.3	Vendor solely responsible for maintaining native API connectors at no added cost, for contract life	**Yes**

#	Requirement	Apptega Capability
4.5.4	TPRM add-on: selectively enabled per workspace for vendor risk tracking + questionnaire automation	**Yes**
4.5.5	Dedicated implementation professional services for initial API integrations to core security stack	**Yes**
SECTION B — 4.6 Custom Assessments & Questionnaire Engine		
4.6.1	Custom questionnaire builder: design, schedule, and distribute custom risk assessments to any workspace	**Yes**
4.6.2	Single answer + evidence auto-scores, cross-maps, and updates maturity baselines across ALL selected frameworks simultaneously (WVCSF + NIST, etc.)	**Yes**
SECTION B — 4.7 Hybrid Environment Tracking (Cloud & On-Prem)		
4.7.1	Concurrent hybrid (cloud + on-premises) compliance tracking inside a single sandboxed workspace	**Yes**
4.7.2	Automated evidence ingestion (dynamic config checks) from AWS, Azure, GCP, Active Directory, Cisco, Palo Alto Networks	**Yes**
4.7.3	Manual, workflow-driven evidence upload portals for legacy/on-prem systems (SSPs, physical security proofs, CSV exports)	**Yes**
SECTION B — 4.8 Risk Register & POAM Management		
4.8.1	Centralized Risk Register generating and tracking POA&Ms	**Yes**
4.8.2	Formal Risk Exception workflow: local agencies submit exception + justification for central CISO review/approval	**Yes**
SECTION B — 4.9 Service Level Agreement (SLA) & Support		
4.9.1	Minimum 99.9% guaranteed system uptime	**Yes**
4.9.2	Standard technical support 8:00 AM–5:00 PM EST, Mon–Fri, with defined critical-outage response times	**Yes**

2. NFF – Apptega Solution Overview



NFF – Apptega Risk Manager Overview

When It Comes to Risk, Half the Picture Isn't Enough

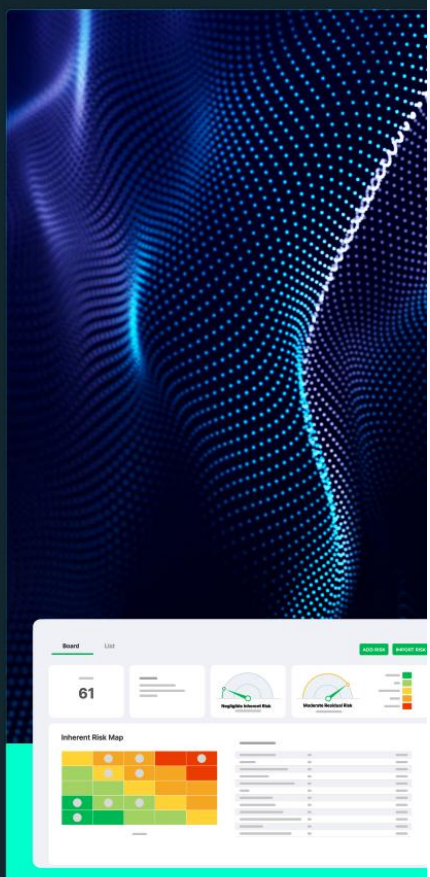
Apptega assesses and visualizes risk from a high level all the way down to individual sub-controls — so you can get a full view into your exposure.

Take the "Risk" out of Risk Management

The risk landscape changes on a dime. And when considered in the context of tightening compliance, privacy, and regulatory expectations, getting your arms around your risk profile and the steps that must be taken to keep it in check starts to feel overwhelming. If you're still addressing risk management with spreadsheets and Word docs, odds are you're not getting the full picture of your exposure or accurately stack-ranking by severity. This lack of visibility can slow remediation and pose additional risk. Luckily, Apptega has the antidote.

With Apptega Risk Manager, you can seamlessly:

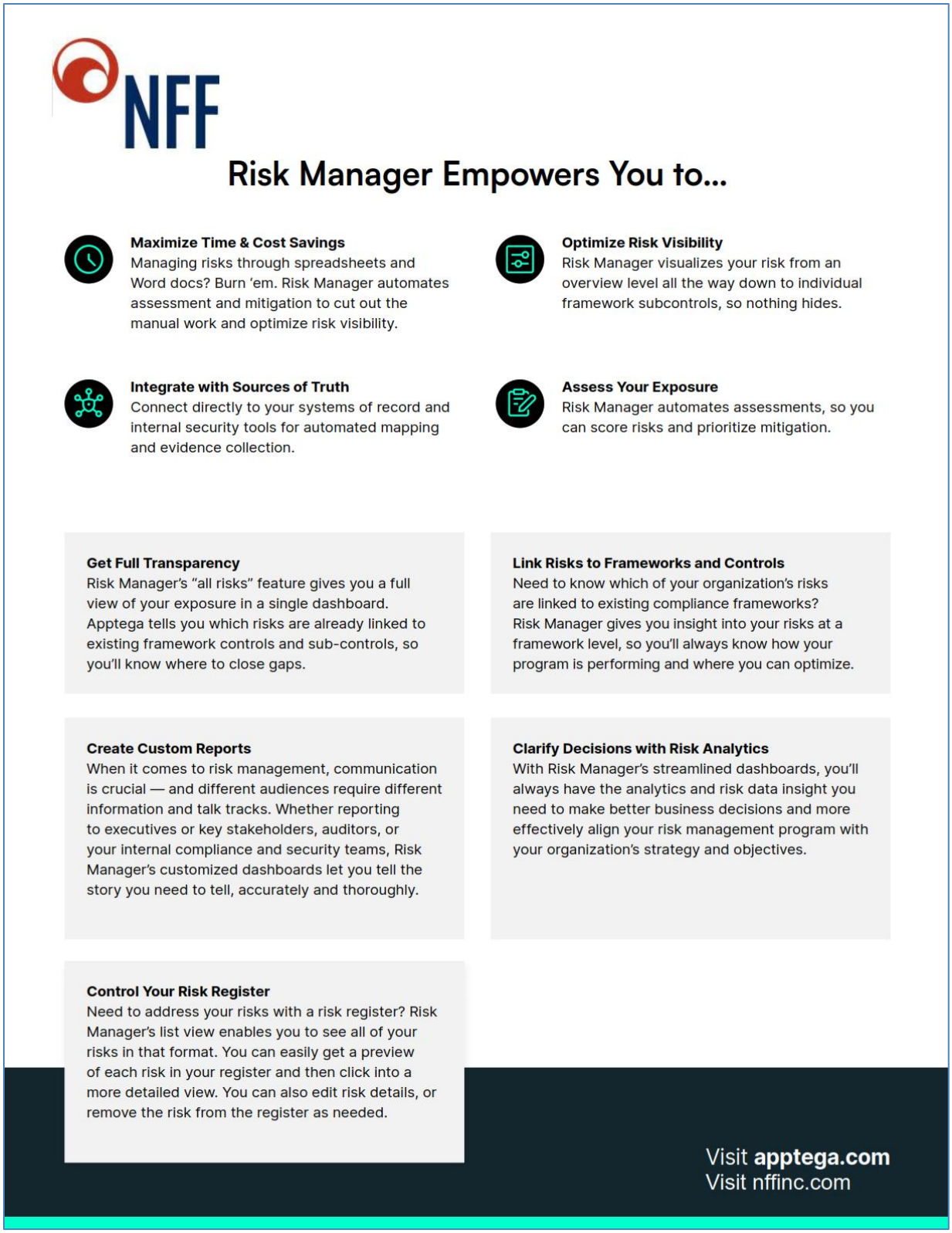
- Get a full picture of your risk profile with risks ranked by score
- Assign a risk rating
- Decide which frameworks address risks, and which don't
- Identify gaps in your risk management process
- Document risk title, risk owners, date identified, response due date, response plans, and potential impact on your organization
- Create custom reports and dashboards, and easily create a risk register
- Assess and mitigate risks at the control and sub-control levels
- Streamline risk management with built-in guidance, documents and templates
- Drive better decisions by speaking a risk language your executives and key stakeholders understand
- Align vendor practices with industry-recognized compliance frameworks
- Enable custom scoring for your questionnaires
- Easily share vendor assessments and reports with key stakeholders



Apptega Risk Manager saves you money, automates processes, and ensures you always have accurate, real-time insight into your evolving risk landscape.

Want to see it in action?

Get a Demo

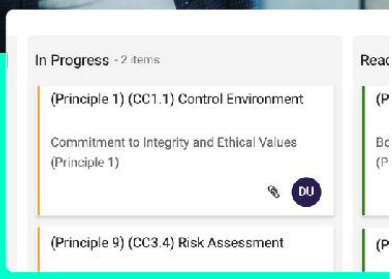

NFF
Risk Manager Empowers You to...
Maximize Time & Cost Savings
Managing risks through spreadsheets and Word docs? Burn 'em. Risk Manager automates assessment and mitigation to cut out the manual work and optimize risk visibility.
Optimize Risk Visibility
Risk Manager visualizes your risk from an overview level all the way down to individual framework subcontrols, so nothing hides.
Integrate with Sources of Truth
Connect directly to your systems of record and internal security tools for automated mapping and evidence collection.
Assess Your Exposure
Risk Manager automates assessments, so you can score risks and prioritize mitigation.
Get Full Transparency
Risk Manager's "all risks" feature gives you a full view of your exposure in a single dashboard. Apptega tells you which risks are already linked to existing framework controls and sub-controls, so you'll know where to close gaps.
Link Risks to Frameworks and Controls
Need to know which of your organization's risks are linked to existing compliance frameworks? Risk Manager gives you insight into your risks at a framework level, so you'll always know how your program is performing and where you can optimize.
Create Custom Reports
When it comes to risk management, communication is crucial — and different audiences require different information and talk tracks. Whether reporting to executives or key stakeholders, auditors, or your internal compliance and security teams, Risk Manager's customized dashboards let you tell the story you need to tell, accurately and thoroughly.
Clarify Decisions with Risk Analytics
With Risk Manager's streamlined dashboards, you'll always have the analytics and risk data insight you need to make better business decisions and more effectively align your risk management program with your organization's strategy and objectives.
Control Your Risk Register
Need to address your risks with a risk register? Risk Manager's list view enables you to see all of your risks in that format. You can easily get a preview of each risk in your register and then click into a more detailed view. You can also edit risk details, or remove the risk from the register as needed.
Visit apptega.com
Visit nffinc.com

NFF – Apptega Audit Manager Overview

NFF | Apptega

Ace Your Audit, Every Time

Apptega's Audit Manager streamlines cybersecurity & compliance programs, from assessment through to the final stamp of approval.



Pass Cybersecurity Audits with Ease

"Audit." The word alone can raise your blood pressure. But cybersecurity and compliance audits don't have to be complex, difficult or frustrating. Audit Manager streamlines the process by assessing your current state, centralizing all artifacts and documentation, automating auditor requests and more.

Our end-to-end platform meets you where you are, and empowers you to:

- Assess your compliance posture and identify gaps
- Collect evidence, artifacts and documentation in a single, central repository
- Quickly fulfill auditor requests for documentation and evidence
- Eliminate manual grunt work and spreadsheets from your audit process

Navigating audits with Apptega results in faster response times, fewer follow-up questions, and more confidence you'll pass the test.

Want to see Audit Manager in action?

Check out a short demo video.

Watch demo

Apptega

NFF

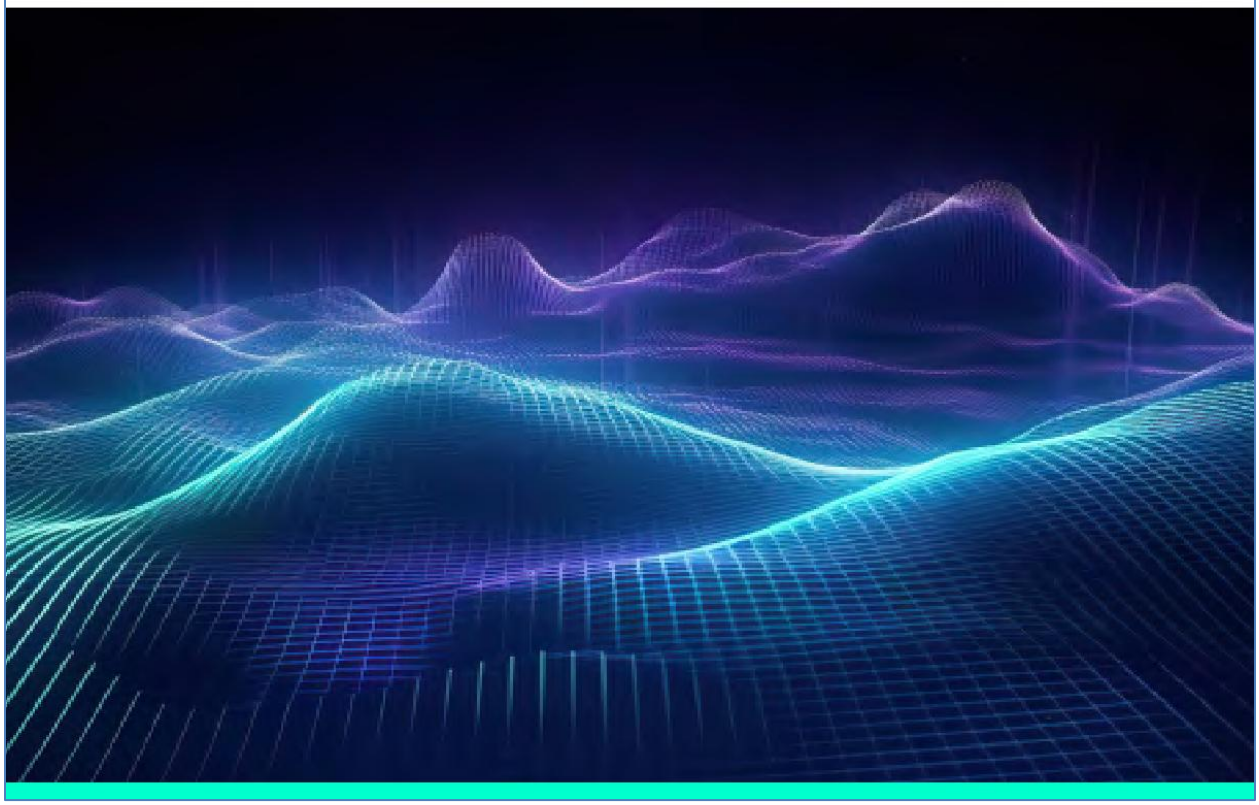
With the Power of Audit Manager, you can...

Beat the Deadline
Automatically link evidence from your compliance programs to the audit, speeding fulfillment of evidence requests and ensuring thoroughness.

Cut Costly Overhead
With a single platform, you can navigate the entire audit from soup to nuts, housing evidence in one location and facilitating responses.

Maximize Visibility
Visualize your progress with a Kanban-style board that shows you exactly where you are, and where you need to go. Provide auditors with a filtered view — showing them only what you need to.

Increase Control and Collaboration
Assign tasks directly to internal team members, and alert stakeholders when appropriate. Then ping your auditor when you've responded to evidence requests.



Apptega

From Assessment to Audit in Four Simple Steps

Upload Auditor Requests
Map requests directly into the platform so you can track fulfillment and provide proof of compliance.

Assess Compliance
Easily compile documentation to see where you're compliant and where you're gapped.

Manage Evidence Requests
Leverage the easily-readable project management board to move tasks through from request to collection to completion.

Pass Your Audit
Ahhh yeah! Savor that warm 'n fuzzy feeling of passing your audit with ease, while maintaining your program throughout the year to prepare for the next.

Simplify Your Audit Process
Security doesn't have to be hard, but it needs to be effective. Audit Manager lets you streamline the entire compliance process from assessment to audit. Work collaboratively with auditors to easily document and provide proof of your cybersecurity compliance. Then share the results through audience-specific reports and dashboards.

Capitalize on Our 100+ Years of Expertise
We've got your back with a team of certified, world-class cybersecurity experts to support you throughout your entire compliance journey — from quarterly reviews to audit advice whenever you need it. Our expertise is your expertise, at no extra charge.

Eliminate the Guesswork
Important information often gets buried in the cells of spreadsheets. So we built Apptega with visual cues that show gaps, next steps, and your progress to date. With Apptega, you can also surface critical evidence and documentation within one central repository for a source of truth you can bank on.

Increase Visibility & Manage Deadlines
Take Audit Manager's dashboards to your next executive meeting to show your progress and next steps in a way everybody can understand. And when it comes to hitting deadlines, reference in-app task assignments and ping your teams on critical next steps with automated notifications.

Collaborate with Auditors
Take advantage of customized user roles to share with auditors only what they need to see – while your team manages your process privately behind the scenes.

Visit **apptega.com**
Visit nffinc.com

NFF – Apptega Vendor Risk Manager Overview


NFF
Apptega
With the Power of Vendor Risk Manager...
Track Vendor Compliance
Associate questionnaires directly with vendor contacts so you can monitor responses.
Simplify Questionnaire Creation
Leverage our library of pre-built questionnaire templates, or create your own to address your organization's specific needs.
Ace Your Next Audit
Auditors and regulators increasingly include vendors in security and compliance evaluations. Make sure you have all the information at your fingertips. You'll need it.
Make Sense of the Data
Transform inscrutable vendor data into easily-digestible dashboards that clearly identify your risks and align results to your business goals. Quickly export reports for sharing with third parties and key stakeholders.
Import Questionnaires, Export Response
Have your own questionnaires? Import and convert them to templates in seconds. You can also export vendor responses into spreadsheets for sharing.
Track Back-Up Vendors
Keep track of questionnaires for your backup vendors. If you have to quickly replace a vendor for not meeting your standards, you'll know who's up next and have confidence they'll better meet your needs.
Manage Vendor Risk
Keep tabs on responses and quickly follow up so you have full visibility into vendor risks and the status of mitigation.
Want to see it in action?
See how you can make cybersecurity and compliance easy.
Request a demo
Or visit apptega.com/get-demo
nffinc.com

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

State of West Virginia
Centralized Request for Quote
Info Technology

Proc Folder: 2012913			**Reason for Modification:**
Doc Description: Governance, Risk and Compliance Automation Platform			
Proc Type: Central Contract - Fixed Amt			
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2026-07-15	2026-07-30 13:30	CRFQ 0231 OOT2700000002	1

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code: VS0000037191
Vendor Name : Networking For Future (NFF), Inc.
Address : 700 12th Street NW, Suite 700
Street : Washington, DC 20005
City :
State : DC **Country :** USA **Zip :** 20005
Principal Contact : Kevin Reith
Vendor Contact Phone: 202-304-9030 **Extension:**

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor Signature X Kevin J. Reith **FEIN#** 54-1819774 **DATE** 08 / 11 / 2026

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

ADDITIONAL INFORMATION
The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) to establish a contract for the purchase of Enterprise Governance, Risk, and Compliance (GRC) as more fully described in the specifications contained herein.

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	GRC Software Maintenance and Support Year One (Initial term)	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Enter a grand total lump sum yearly price that is all inclusive of specifications:
4.1 ; 4.2 ; 4.3 ; 4.4 ; 4.5 ; 4.6 ; 4.7 ; 4.8 ; 4.9

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	GRC Software Maintenance and Support Year 2 renewal	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Enter a grand total lump sum yearly price that is all inclusive of specifications:
4.1 ; 4.2 ; 4.3 ; 4.4 ; 4.5 ; 4.6 ; 4.7 ; 4.8 ; 4.9

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	GRC Software Maintenance and Support Year 3 renewal	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Enter a grand total lump sum yearly price that is all inclusive of specifications:
4.1 ; 4.2 ; 4.3 ; 4.4 ; 4.5 ; 4.6 ; 4.7 ; 4.8 ; 4.9

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	GRC Software Maintenance and Support Year 4 renewal	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Enter a grand total lump sum yearly price that is all inclusive of specifications:
4.1 ; 4.2 ; 4.3 ; 4.4 ; 4.5 ; 4.6 ; 4.7 ; 4.8 ; 4.9

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Questions are due by 3:00 p.m.	2026-07-22

	Document Phase	Document Description	Page 4
OOT2700000002	Draft	Governance, Risk and Compliance Automation Platform	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

INSTRUCTIONS TO VENDORS SUBMITTING BIDS

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

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

3. **PRE-BID MEETING:** The item identified below shall apply to this Solicitation.

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

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

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

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

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.

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 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 non-binding.

Submitted emails should have the solicitation number in the subject line. Question

Submission Deadline: July 22, 2026 @ 3:00 p.m.

Submit Questions to: Toby L Welch
2019 Washington Street, East Charleston, WV 25305
Fax: (304) 558-3970
Email: Toby.L.Welch@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 on or before the date and time of the bid opening listed in section 7 below. Vendors can submit bids electronically through *wv*OASIS, in paper form delivered to the Purchasing Division at the address listed below either in person or by courier, or in facsimile form by faxing to the Purchasing Division at the number listed below. Notwithstanding the foregoing, the Purchasing Division may prohibit the submission of bids electronically through *wv*OASIS at its sole discretion. Such a prohibition will be contained and communicated in the *wv*OASIS system resulting in the Vendor's inability to submit bids through *wv*OASIS. The Purchasing Division will not accept bids or modification of bids via email.

Bids submitted in paper, facsimile, or via *wv*OASIS must contain a signature. Failure to submit a bid in any form without a signature will result in rejection of your bid.

A bid submitted in paper or facsimile form should contain the information listed below on the face of the submission envelope or fax cover sheet. Otherwise, the bid may be rejected by the Purchasing Division.

VENDOR NAME:
BUYER: Toby L Welch
SOLICITATION NO.: CRFQ OOT2700000002
BID OPENING DATE: Thursday July 30, 2026
BID OPENING TIME: 1:30 p.m.
FAX NUMBER: 304-558-3970

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.

Bid Delivery Address and Fax Number:
Department of Administration, Purchasing Division 2019 Washington Street East
Charleston, WV 25305-0130
Fax: 304-558-3970

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 *wv*OASIS (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 or via delivery by mail).

Bid Opening Date and Time: 07/30/2026 @ 1:30 p.m.

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 Acknowledgement Form. 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 **shall** clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the equality of the alternate items. Failure to provide information for alternate items **may** be grounds for rejection of a Vendor's bid.

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

11. **COMMUNICATION LIMITATIONS:** In accordance with West Virginia Code of State Rules §148-1-6.6.2, 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.

12. **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.

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

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

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

15. **SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESSES:** For any solicitations publicly advertised for bid, in accordance with West Virginia Code §5A-3-37 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.

16. **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 § 148-1-4.7.

17. **ELECTRONIC FILE ACCESS RESTRICTIONS:** Vendor must ensure that its submission in *wv*OASIS 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.

18. **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."

19. **ACCEPTANCE/REJECTION:** The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules § 148-1-4.6. and § 148-1-6.3."

20. **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 § 148-1-4.7. This authority does not apply to instances where state law mandates receipt with the bid.

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

22. **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.

GENERAL TERMS AND CONDITIONS:

1. CONTRACTUAL AGREEMENT: Issuance of an Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance by the State of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid, or on the Contract if the Contract is not the result of a bid solicitation, 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: The Initial Contract Term will be for a period of One (1) Year. The Initial Contract Term becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and the Initial Contract Term ends on the effective end date also shown on the first page of this Contract.

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

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

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

[ ] **Fixed Period Contract:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within _____days.

[ ] **Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within _____ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that:

[ ] the contract will continue for _____ years;

[ ] the 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).

[ ] **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.

[ ] **Construction/Project Oversight:** This Contract becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and continues until the project for which the vendor is providing oversight is complete.

[ ] **Other:** Contract Term specified in _____

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

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

[ ] **Open End Contract:** Quantities listed in this Solicitation/Award Document 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.

[ ] **Construction:** This Contract is for construction activity more fully defined in the specifications.

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

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

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

[ ]

[ ]

[ ]

[ ]

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

8. INSURANCE: The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below 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 that insurance requirement is listed in this section.

Vendor must maintain:

[☑] **Commercial General Liability Insurance** in at least an amount of: $1,000,000.00 per occurrence.

[ ] **Automobile Liability Insurance** in at least an amount of: _____per occurrence.

[ ] **Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: _____per occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

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

[ ] **Cyber Liability Insurance** in an amount of: _____ 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.

[ ]

[ ]

[ ]

[ ]

9. WORKERS' COMPENSATION INSURANCE: 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. VENUE: 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.

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.

[✓] Liquidated Damages Are Not Included in this Contract.

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: 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 maintenance, licenses, or subscriptions may be paid annually in advance.

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

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

17. ADDITIONAL FEES: Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia, included in the Contract, 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. 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.

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.

20. TIME: Time is of the essence regarding 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 www.state.wv.us/admin/purchase/privacy.

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 NON-CONFLICT: Neither Vendor nor its representatives are permitted to have any interest, nor shall they 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.

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

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

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

37. NO DEBT CERTIFICATION: 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. By submitting a bid, or entering into a contract with the State, Vendor is affirming 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, neither the Vendor nor any related party owe a debt as defined above, and neither the Vendor nor any related party are in employer default as defined in the statute cited above unless the debt or employer default is permitted under the statute.

38. 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.

39. 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.division@wv.gov.

40. BACKGROUND CHECK: In accordance with W. Va. Code § 15-2D-3, 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.

41. 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.

c. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:

    1. 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

    2. 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.

42. 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.

43. 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 disclosure of interested parties prior to beginning work under this Contract. Additionally, the Vendor must submit a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-work 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.

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

45. VOID CONTRACT CLAUSES: This Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

46. ISRAEL BOYCOTT: Bidder understands and agrees that, pursuant to W. Va. Code § 5A-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.

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

(Printed Name and Title) Kevin Reith, Sales Director – WV State/Local/Education

(Address) 233 - D Heavner Avenue. ELKINS, WV 26241

(Phone Number) / (Fax Number) (202) 304 - 9030 // (202) 783 - 9019

(email address) kreith@nffinc.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through *wv*OASIS, I certify that: I have reviewed this Solicitation/Contract 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/Contract 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 this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; 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; 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.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Networking For Future (NFF), Inc
(Company)

Kevin J. Reith
(Signature of Authorized Representative)

Kevin Reith, Sales Director – WV State/Local/Education
(Printed Name and Title of Authorized Representative) (Date)

(202) 304 - 9030 // (202) 783 - 9019
(Phone Number) (Fax Number)

kreith@nffinc.com
(Email Address)

SPECIFICATIONS

1. **PURPOSE AND SCOPE:** The The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) to establish an open-end contract for an Enterprise Governance, Risk, and Compliance (GRC) or Compliance Automation Platform. This solution will serve as the centralized risk management and automated evidence collection platform for WVOT and its supported state agencies, boards, and commissions.

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

   2.1 "Licenses" means Agency's licenses to utilize software.

   2.2 "Pricing Page" means the pages contained wvOASIS or attached hereto as Exhibit A, upon which Vendor should list its proposed price for the software maintenance and support.

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

3. **QUALIFICATIONS:** Vendor, or Vendor's staff if requirements are inherently limited to individuals rather than corporate entities, shall have the qualifications listed below. Compliance will be determined prior to contract award by the State through documentation provided by the Vendor with its bid or upon request, Vendor must provide any documentation requested by the State to assist in confirmation of compliance with this provision. References, documentation, or other information to confirm compliance with this experience requirement are preferred with the bid submission but may be requested after bid opening and prior to contract award.

   3.1. Vendor must be authorized by GRC software company to provide software maintenance and support for the Licenses and provide proof of authorization upon request.

4. **MANDATORY REQUIREMENTS:**

The Vendor must provide a SaaS-based platform that meets or exceeds the following technical specifications:

4.1 Software Maintenance and Support: Vendor must provide maintenance and support for the platform licenses as follows:

4.1.1 Deployment Sizing: The baseline platform license must natively include the central WVOT hub and 125 fully segregated child workspaces (tenants) upon deployment.

4.1.2Initial Contract Term: The contract awarded from this Solicitation shall be for an initial period of one (1) year.

4.1.3 Renewal Term Clauses: The contract may be renewed upon mutual written consent of the Agency and the Vendor, and approval of the Purchasing Division, for up to three (3) optional one-year renewal periods (for a total potential contract life of 4 years), under the same pricing, terms, and conditions as specified herein. Each subsequent term will run consecutively to the prior term.

4.1.4 On-Demand Workspace Expansion: The platform must support the dynamic provisioning of additional workspace licenses via a fixed, on-demand unit price structure. Any additional workspace licenses added mid-term must be billed on a prorated basis for the remainder of the active contract year, and shall renew at the full annual unit rate at the start of the subsequent renewal term.

4.2 Training Deliverables

4.2.1 Train-the-Trainer Program: Vendor must provide a formal program consisting of virtual, instructor-led sessions for central WVOT administrators.

4.2.2 **On-Demand Materials:** Vendor must provide on-demand digital training materials, video tutorials, or manuals for local agency-level end users.

4.3 Architectural, RBAC & Dashboard Requirements:

4.3.1 Central WVOT Hub: The platform must provide a centralized dashboard for the WVOT Chief Information Security Officer (CISO) to view the aggregate, real-time compliance and risk posture of all state entities.

4.3.2 **Granular, Role-Based Access Control (RBAC):** The platform must enforce strict RBAC to ensure that local agency entities can only view, edit, or manage data within their own sandbox workspace. Agency users must be restricted to their own specific audit information, risk assessments, evidence lockers, and remediation plans.

4.3.3 **Predefined Platform Roles:** The platform must support predefined and custom roles, including *Agency Security Officer* (read/write internal), *External Auditor* (read-only to specific audit files), and *Executive Observer* (dashboard view only). Central WVOT administrators must retain global master access across all workspaces.

4.3.4 **Executive Dashboards & Audit Exporting:** The platform must include automated report generation capabilities, allowing WVOT and agencies to export executive dashboards, compliance summaries, and System Security Plans (SSPs) in standard formats (e.g., PDF, Excel, CSV) for external auditors and executive leadership.

4.4 **Platform Authentication & Single Sign-On (SSO):**

4.4.1 **Native Integration:** The platform must natively support SAML 2.0 and OpenID Connect (OIDC) protocols to allow seamless federated Single Sign-On (SSO). MFA must be supported for the platform.

4.4.2 **WVOT Tenant Authentication:** The system must integrate directly with WVOT's centralized Microsoft Entra ID tenant to allow state-issued corporate credentials to authenticate users.

4.5 **Tiered and Modular Licensing Requirements:**

4.5.1 **The Core Tier (Mandatory for All Workspaces):** Every workspace must include access to the core framework libraries (including WVCSF, NIST, and other industry-recognized standards), audit logging, RBAC, Entra ID SSO authentication, and the custom questionnaire engine.

4.5.2 **Continuous Control Monitoring (CCM) Add-On Module:** The platform must allow WVOT to enable native API automated evidence collection strictly for select workspaces. The platform must natively support and pull configuration data from the State's existing infrastructure, which includes Microsoft Entra ID, Google Workspace, Palo Alto Networks, SentinelOne, and Active Directory.

4.5.3 **Native Integration Maintenance:** The Vendor is solely responsible for maintaining and updating these native API connectors throughout the life of the contract at no additional cost to the State.

4.5.4 **Third-Party Risk Management (TPRM) Add-On Module:** The platform must allow WVOT to selectively enable the Vendor Risk Management module (for external vendor compliance tracking and questionnaire automation) for specific workspaces.

4.5.5 **Implementation Timeline & Support:** Vendor must provide dedicated implementation professional services to assist WVOT with the initial API integrations to the core security stack.

4.6 **Custom Assessments & Framework Questionnaire Engine:**

4.6.1 **Custom Questionnaire Builder:** The platform must feature a flexible, custom questionnaire engine allowing WVOT administrators to design, schedule, and distribute custom risk assessments to any activated workspace.

4.6.2 **Framework Specific Assessment Alignment:** The tool must allow WVOT to map these custom questionnaires directly to the controls of the West Virginia Cyber Security Framework (WVCSF) as well as industry-standard frameworks such as NIST. When an agency answers a custom question and attaches evidence, the system must automatically score, cross-map, and update that agency's active maturity baselines across all selected frameworks simultaneously.

4.7 **Hybrid Environment Tracking (Cloud & On-Premises):**

4.7.1 Hybrid Operations Baseline: The platform must support concurrent hybrid compliance tracking capability inside individual sandboxed workspaces.

4.7.2 Automated Evidence Ingestion: Ability to ingest dynamic configuration checks from AWS, Azure, GCP, Active Directory, Cisco, and Palo Alto networks environments.

4.7.3 **On-Premises Workflow Portals:** Clean, workflow-driven portals for manual evidence gathering for legacy systems that cannot utilize direct automated validation checks to manually upload physical security proofs, System Security Plans (SSPs), and text/CSV configuration exports.

4.8 **Risk Register & POAM Management:**

4.8.1 **POAM Tracking:** The platform must include a centralized Risk Register capable of generating and tracking Plans of Action and Milestones (POAMs).

4.8.2 **Exception Workflows:** The platform must support a formal Risk Exception workflow, allowing local agencies to submit exception requests and justification documentation for central WVOT CISO review and approval.

4.9 **Service Level Agreement (SLA) & Support:**

4.9.1 **System Uptime:** The proposed SaaS platform must guarantee a minimum 99.9% system uptime.

4.9.2 **Support Availability:** The Vendor must provide standard technical support (minimum 8:00 AM – 5:00 PM EST, Monday through Friday) for central WVOT administrators, with defined response times for critical system outages.

4.9.3 **Agreement Submission:** Vendor must provide a copy of all applicable maintenance, support, and SaaS subscription agreements prior to contract award for review and approval by the State of West Virginia.

5 CONTRACT AWARD:

5.1 Contract Award: The Contract will be awarded to the Vendor that provides the Software Maintenance and Support meeting the required specifications for the lowest total contract cost as shown on the Pricing Pages.

5.2 Pricing Page: Vendor should complete the Pricing Page by providing the information on Exhibit A and signing the page or entering pricing in OASIS.

Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified. Vendor should type or electronically enter the information into the Pricing Pages through wvOASIS, if available, or as an electronic document.

6 **PAYMENT:** Agency shall pay as shown on the Pricing Pages, for all Software Maintenance and Support. Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.

7 **FACILITIES ACCESS:** In the event that performance of Software Maintenance and Support requires access to Agency facilities, access cards and/or keys may be required to gain entrance. In the event that access cards and/or keys are required:

7.1 Vendor must identify principal service personnel which will be issued access cards and/or keys to perform service.

7.2 Vendor will be responsible for controlling cards and keys and will pay replacement fee, if the cards or keys become lost or stolen.

7.3 Vendor shall notify the Agency immediately of any lost, stolen, or missing card or key.

7.4 Anyone performing under this Contract will be subject to Agency's security protocol and procedures.

7.5 Vendor shall inform all staff of Agency's security protocol and procedures.

8 **VENDOR DEFAULT:**

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

8.1.3 Failure to perform Contract Services in accordance with the requirements contained herein.

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

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

8.1.6 Failure to remedy deficient performance upon request.

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

8.2.3 Immediate cancellation of the Contract.

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

8.2.5 Any other remedies available in law or equity.

9 MISCELLANEOUS:

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

Contract Manager: Alan Edwards

Telephone Number: (202) 266 - 4741

Fax Number: (202) 783 - 9019

Email Address: aedwards@nffinc.com

CRFQ OOT2700000002

Governance, Risk and compliance Automation Platform

APPENDIX A: WV SOFTWARE AS A SERVICE ADDENDUM

begins on next page.

Software as a Service Addendum

1. Definitions:

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

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

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

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

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

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

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

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

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

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

Restricted data means personal data and non-public data.

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

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

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

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

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

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

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

b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.

c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.

d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.

e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.

f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.

g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to *store* public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

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

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

a) Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.

b) Security Incident Reporting Requirements: The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.

c) Breach Reporting Requirements: Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and the public jurisdiction point of contact for general contract oversight/administration.

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

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

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

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

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

7. Termination and Suspension of Service:

a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.

b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.

c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

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

d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.

e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

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

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

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

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

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

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

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

14. Security:

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

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

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

c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

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

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

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

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

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

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

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

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

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

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

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

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

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

AGREED:

Name of Agency:_____	Name of Vendor: Networking For Future (NFF), Inc
Signature:_____	Signature:_____
Title:_____	Title:_____
Date:_____	Date: 07 / 28 / 2026

Appendix A

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

Name of Service Provider/Vendor: _____

Name of Agency:_____

Agency/public jurisdiction's required information:

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

   Name: _____

   Email address: _____

Vendor/Service Provider's required information:

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

   Name: _____

   Email address: _____

   Phone Number: _____ _____