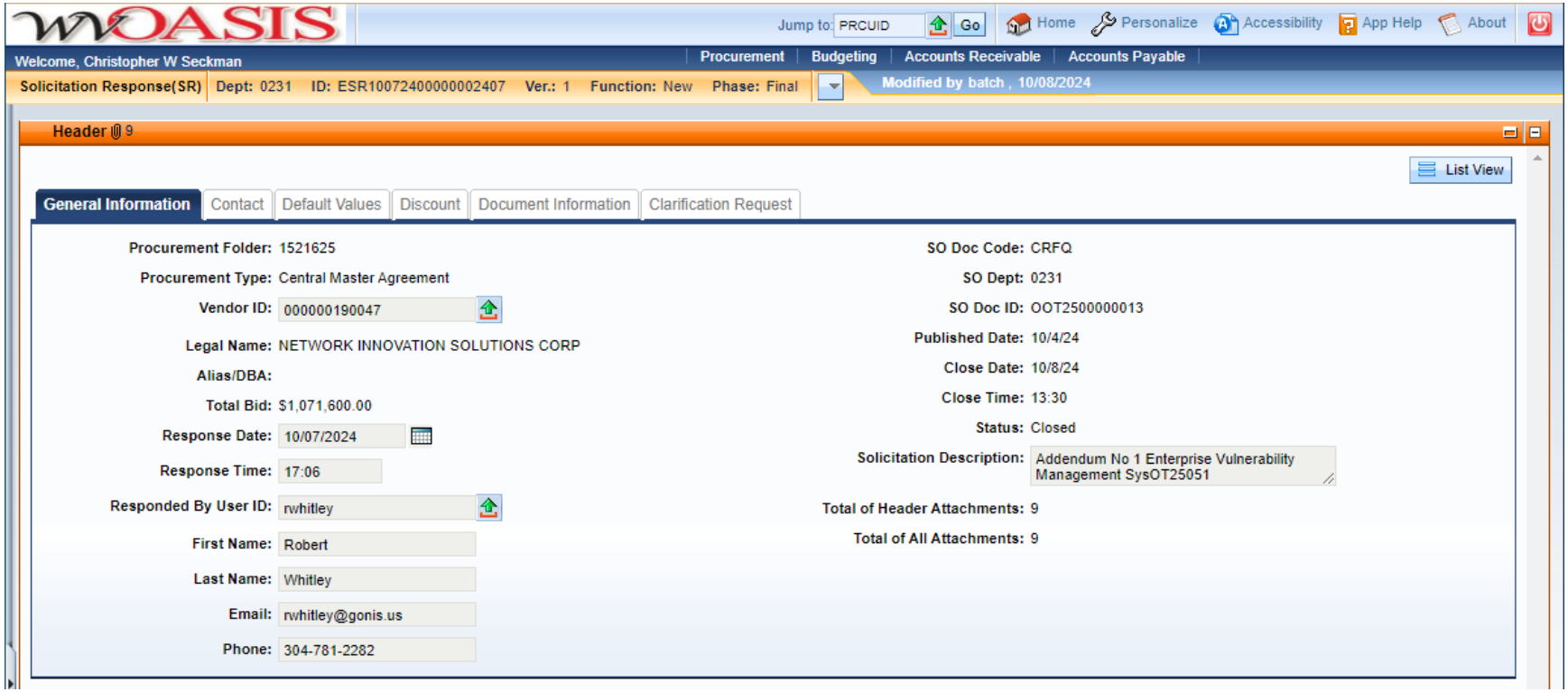
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency 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.


wvOASIS
Jump to: PRCUID
Go
Home
Personalize
Accessibility
App Help
About
Welcome, Christopher W Seckman
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR)
Dept: 0231
ID: ESR10072400000002407
Ver.: 1
Function: New
Phase: Final
Modified by batch , 10/08/2024
Header 9
List View
General Information
Contact
Default Values
Discount
Document Information
Clarification Request
Procurement Folder: 1521625
Procurement Type: Central Master Agreement
Vendor ID: 000000190047
Legal Name: NETWORK INNOVATION SOLUTIONS CORP
Alias/DBA:
Total Bid: $1,071,600.00
Response Date: 10/07/2024
Response Time: 17:06
Responded By User ID: rwhitley
First Name: Robert
Last Name: Whitley
Email: rwhitley@gonis.us
Phone: 304-781-2282
SO Doc Code: CRFQ
SO Dept: 0231
SO Doc ID: OOT2500000013
Published Date: 10/4/24
Close Date: 10/8/24
Close Time: 13:30
Status: Closed
Solicitation Description: Addendum No 1 Enterprise Vulnerability Management SysOT25051
Total of Header Attachments: 9
Total of All Attachments: 9

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:	1521625
Solicitation Description:	Addendum No 1 Enterprise Vulnerability Management SysOT25051
Proc Type:	Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2024-10-08 13:30	SR 0231 ESR10072400000002407	1

VENDOR

000000190047
NETWORK INNOVATION SOLUTIONS CORP

Solicitation Number: CRFQ 0231 OOT2500000013

Total Bid: 1071600 **Response Date:** 2024-10-07 **Response Time:** 17:06:51

Comments: Discounting will be placed at time of purchase on the optional 5,000 additional licenses.

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	3.1.1 - Enterprise Vulnerability Management Service - Year 1	1.00000	EA	207900.000000	207900.00

Comm Code	Manufacturer	Specification	Model #
43222503			

Commodity Line Comments: Includes External Scanning Service

Extended Description:

Contract Item #1: Enterprise Vulnerability Management Service (EVMS), 35,000 licenses, with required hardware, training and support

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	3.1.1 - Enterprise Vulnerability Management Service - Year 2	1.00000	EA	207900.000000	207900.00

Comm Code	Manufacturer	Specification	Model #
43222503			

Commodity Line Comments: Includes External Scanning Service

Extended Description:

Contract Item #1: Enterprise Vulnerability Management Service (EVMS), 35,000 licenses, with required hardware, training and support

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	3.1.1 - Enterprise Vulnerability Management Service - Year 3	1.00000	EA	207900.000000	207900.00

Comm Code	Manufacturer	Specification	Model #
43222503			

Commodity Line Comments: Includes External Scanning Service

Extended Description:

Contract Item #1: Enterprise Vulnerability Management Service (EVMS), 35,000 licenses, with required hardware, training and support

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	3.1.1 - Enterprise Vulnerability Management Service - Year 4	1.00000	EA	207900.000000	207900.00

Comm Code	Manufacturer	Specification	Model #
43222503			

Commodity Line Comments: Includes External Scanning Service

Extended Description:

Contract Item #1: Enterprise Vulnerability Management Service (EVMS), 35,000 licenses, with required hardware, training and support

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
5	3.1.1.1.6.1 - Additional 5,000 License Increments - Year 1	1.00000	EA	60000.000000	60000.00

Comm Code	Manufacturer	Specification	Model #
43222503			

Commodity Line Comments: Discounts may apply at the time of purchase. The listed price reflects the maximum cost, with any applicable discounts applied during time of purchase.

Extended Description:

3.1.1.1.6.1 At the State's discretion, the Vendor must provide additional licenses in 5,000 increments.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
6	3.1.1.1.6.1 - Additional 5,000 License Increments - Year 2	1.00000	EA	60000.000000	60000.00

Comm Code	Manufacturer	Specification	Model #
43222503			

Commodity Line Comments: Discounts may apply at the time of purchase. The listed price reflects the maximum cost, with any applicable discounts applied during time of purchase.

Extended Description:

3.1.1.1.6.1 At the State's discretion, the Vendor must provide additional licenses in 5,000 increments.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
7	3.1.1.1.6.1 - Additional 5,000 License Increments - Year 3	1.00000	EA	60000.000000	60000.00

Comm Code	Manufacturer	Specification	Model #
43222503			

Commodity Line Comments: Discounts may apply at the time of purchase. The listed price reflects the maximum cost, with any applicable discounts applied during time of purchase.

Extended Description:

3.1.1.1.6.1 At the State's discretion, the Vendor must provide additional licenses in 5,000 increments.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
8	3.1.1.1.6.1 - Additional 5,000 License Increments - Year 4	1.00000	EA	60000.000000	60000.00

Comm Code	Manufacturer	Specification	Model #
43222503			

Commodity Line Comments: Discounts may apply at the time of purchase. The listed price reflects the maximum cost, with any applicable discounts applied during time of purchase.

Extended Description:

3.1.1.1.6.1 At the State's discretion, the Vendor must provide additional licenses in 5,000 increments.

insightVM Deployment Handbook

Thank you for Advancing Securely with Rapid7. Within this document, you'll find system, network, and functional requirements, a project plan, and additional resources. If you have any additional questions, please send those to your Project Manager or your Security Consultant.

Preparing for Deployment:

In order for your insightVM deployment to be successful, you **MUST** have the following resources in place prior to the first day or your deployment:

Change Control

It is common for many organizations to employ a change control process around their IT environments. To ensure a successful deployment, change controls must be approved prior to Deployment, to enable implementation and testing of product functionality. Consider mitigation action, for example: if change control has been submitted, but not approved, or an emergency change is required, what course of action can be taken to keep the deployment moving?

Multi-Team Stakeholder Participation

Cybersecurity often involves teams outside of the direct security team deploying the software. For example, an IT team can speak to existing hardware – whereas a provisioning team can speak to how new hardware is onboarded. Managerial staff can additionally provide context around key performance indicators ("KPI")s and required compliance that must be met for things like data retention.

Having several teams involved in the deployment of insightVM will ensure a successful rollout within your environment, allow for cross training and improved understanding of findings.

We recommend that you have representatives from the following teams available during the deployment. They do not need to be present during the entire deployment timeframe, but need to have the flexibility to join at relatively short notice.

- Cybersecurity Managerial staff, providing guidance around KPI's, priorities and reporting needs
- System Administrator capable of provisioning service accounts **OR** ensure accounts identified in Additional Resources are pre-configured
- Vulnerability Management Administrator (should be available throughout)
- Network Administrator: capable of modifying and troubleshooting routing or access controls

- Security Administrator: capable of modifying and troubleshooting security devices or software that may be interfering with insightVM functionality (e.g. Network Firewalls or Endpoint Security Protection)

Technical Preparation

Virtual Machine Requirements

insightVM requires the establishment of compute resources within your internal environment. Without these machines, the deployment will be unable to proceed.

Based on your environment, you will need:

- 1 machine to be used as a console
- a minimum of 1 machine to be used as an engine

These machines should match the following criteria

System	Asset Count	Proc / Core Count	RAM (GB)	Disk
Console	< 5,000	4	16	1 TB
Console	< 20,000	12	64	2 TB
Console	< 150,000	12	128	4 TB
Console	< 400,000	12	256	8 TB
Engine	< 5,000 / day	4	8	100 GB
Engine	< 20,000 / day	8	16	200 GB

Recommended Operating Systems for Console and Engines

Rapid7 recommends that you deploy your Security Console and Engines onto one of the following operating systems *

- English operating system with English/United States regional settings
- 64-bit versions of the following platforms are recommended:
    - Ubuntu Linux 20.04 LTS
    - Microsoft Windows Server 2022 (Desktop Experience / “Core” version not supported)

- Microsoft Windows Server 2019 (Desktop Experience / “Core” version not supported)
- Red Hat Enterprise Linux Server 8
- Red Hat Enterprise Linux Server 7
- Oracle Linux 8
- Oracle Linux 7
- SUSE Linux Enterprise Server 12

* You will be able to find additional supported operating systems here: https://www.rapid7.com/products/insightvm/system-requirements/

Connectivity Preparations

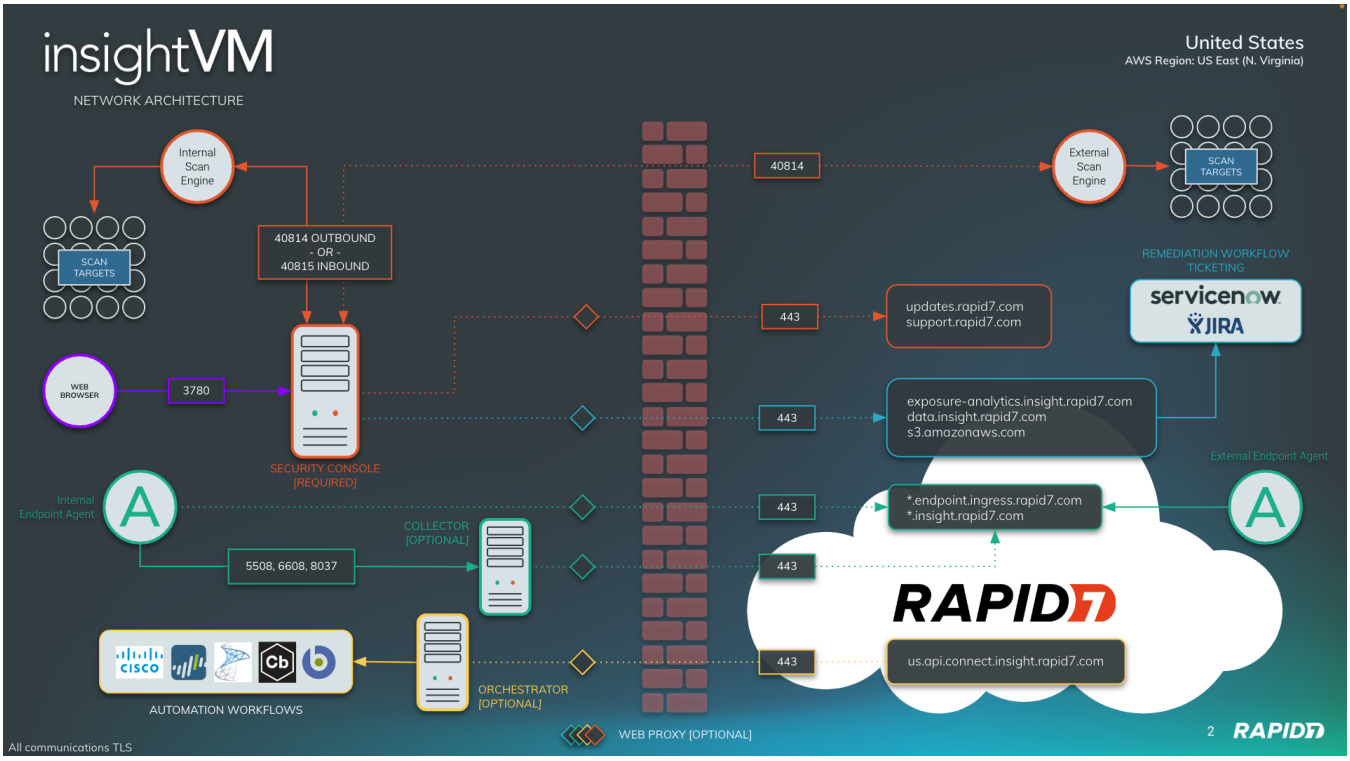
Your Insight Platform Account

Before the deployment can commence, an Insight Platform account is required. Please visit this URL and verify that you have an account provisioned: insight.rapid7.com/login.

If you do not have access, please contact your Rapid7 representative before the deployment, to ensure that the account is created in-time for your deployment.

Firewall Rules and Network Connectivity Requirements

In order to ensure a successful deployment, your team must either have the required firewall rules and credentials established ***prior*** to the engagement, **OR** have the appropriate resources on the call to establish these during the deployment sessions. If you require extensive lead times or change controls to make the adjustments to your configuration, they MUST be completed prior to the engagement.



SOURCE	DESTINATION	PORT	NOTES
Security Console	updates.rapid7.com	TCP 443	System updates and license activation
Security Console	support.rapid7.com	TCP 443	Required to upload logs to R7 Technical Support (Logs need to be manually uploaded by the customer)
Security Console	exposure-analytics.insight.rapid7.com (US 1) us2.exposure-analytics.insight.rapid7.com (US 2) us3.exposure-analytics.insight.rapid7.com (US 3) s3.amazonaws.com (US 1) s3.us-east-2.amazonaws.com (US 2) s3.us-west-2.amazonaws.com (US 3) data.insight.rapid7.com (US 1) us2.data.insight.rapid7.com (US 2)	TCP 443	Only whitelist the URL's that correspond to your Data storage region. I.e. if you are storing your data in the US, only whitelist the relevant (US) entries. Customers are only able to select a single data storage region per console.

	us3.data.insight.rapid7.com (US 3) ca.exposure-analytics.insight.rapid7.com (CA) ca.data.insight.rapid7.com (CA) s3.ca-central-1.amazonaws.com (CA) eu.exposure-analytics.insight.rapid7.com (EU) eu.data.insight.rapid7.com (EU) s3.eu-central-1.amazonaws.com (EU) ap.exposure-analytics.insight.rapid7.com (JAP) ap.data.insight.rapid7.com (JAP) s3-ap-northeast-1.amazonaws.com (JAP) s3.ap-northeast-1.amazonaws.com (JAP) eu.exposure-analytics.insight.rapid7.com (AUS) eu.data.insight.rapid7.com (AUS) s3-ap-southeast-2.amazonaws.com (AUS) s3.ap-southeast-2.amazonaws.com (AUS)		
Security Console	Your internal SMTP Relay	TCP 25 or 465	If report distribution through an SMTP relay is enabled, the Security Console must be able to communicate through these channels to reach the relay server
Security Console	insightVM Scan Engine(s)	TCP 40814	Management of scan activity on Scan Engines and the retrieval of scan data
insightVM Admins	Security Console Server	TCP 3780	Connectivity between the Administrator's machine(s) and the Security Console. To allow connection to insightVM Web Interface
insightVM Scan Engine(s)	Security Console Server	TCP 40815	This is an alternative communication method for scan engines, if you choose not to use TCP 40814. It works in the opposite direction, from engine > console.
Scan Engine(s)	Scan Targets	All TCP & UDP Ports	Scan Engines require unimpeded access to any port that may be open (visible) on your scan targets. You do not have to specifically open all ports, but any port that is already open to the network should be accessible to the scan engine(s), so that the port can be scanned for vulnerabilities.

Collector Server	https://data.insight.rapid7.com (US) https://s3.amazonaws.com (US) https://eu.data.insight.rapid7.com (EMEA) https://s3.eu-central-1.amazonaws.com (EMEA) https://ca.data.insight.rapid7.com (CA) https://s3.ca-central-1.amazonaws.com (CA) https://au.data.insight.rapid7.com (AU) https://s3.ap-southeast-2.amazonaws.com (AU) https://ap.data.insight.rapid7.com (AP) https://s3.ap-northeast-1.amazonaws.com (AP)	TCP 443	Communication between the Collector and the Insight Platform Similar to the previous section, only whitelist the URL's that correspond to your Data storage region. I.e. if you are storing your data in the US, only whitelist the relevant (US) entries.

Insight Agent connectivity requirements

The Insight Agent requires properly configured assets and network settings to function correctly. Since the method of agent communication varies by product, additional configuration may be required depending on which Insight products you plan to use. Before you deploy the Insight Agent, make sure that the Agent can successfully connect and transfer data to the Insight Platform by fulfilling the following requirements

SSL Decryption Exclusion

The Insight Agent will not work if your organization decrypts SSL traffic via Deep Packet Inspection technologies like transparent proxies

Source	Destination	Port	Notes
Insight Agents	*.endpoint.ingress.rapid7.com	TCP 443	Agent messages, beacons, update requests, and file uploads for collection
Insight Agents	*.insight.rapid7.com	TCP 443	Configuration files for deployment
Insight Agents (Optional)	Collector Server	TCP 5508 TCP 6608	Optional: These ports only need to be opened between the agents and the collector server, if the agents should push their traffic via the collector. If they can go directly to the platform, this step can be skipped.

		TCP/UDP 8037	5508/8037: Agent messages and beacons 6608: Agent update requests and file uploads for collection
Insight Agent	52.64.24.140 13.55.81.47 13.236.168.124	TCP 443	Australia Insight Cloud Instances
Insight Agent	103.4.8.209 18.182.167.99	TCP 443	Japan Insight Cloud Instances

As an alternative to configuring a firewall rule that allows traffic for this URL, you can instead configure firewall rules to allow traffic to the following IP addresses and CIDR blocks for your selected region.

United States-1	United States-2	United States-3	Canada	Europe	Japan	Australia
34.226.68.35	13.58.19.32	44.242.59.199	52.60.40.157	3.120.196.152	103.4.8.209	52.64.24.140
54.144.111.231	3.131.127.126	52.41.171.59	52.60.107.153	3.120.221.108	18.182.167.99	13.55.81.47
52.203.25.223	3.139.243.230	54.213.168.123		18.192.78.218		
34.236.161.191						
193.149.136.0/24						

Optional Ticketing & Container Registry connections

Rapid7 provides the following optional list of static IP addresses that you may use to allow traffic originating from the Insight Platform to your on-premises JIRA or container registries:

NOTE

This does not address agent proxying use cases or scenarios relating to communication originating from customer environments to the Insight Platform.

United States-1	United States-2	United States-3	Canada	Europe	Japan	Australia
52.87.0.92	3.132.61.192	44.235.43.237	35.182.161.111	52.28.227.72	13.113.44.15	13.55.206.11
34.203.6.73	3.137.118.102	52.10.164.197	52.60.69.60	52.58.219.32	52.69.171.127	13.54.208.29
34.202.19.138	3.14.210.196	52.88.123.237				52.63.226.244
52.2.37.56						

Scan Authorization

During the deployment your consultant will ask you to run discovery and vulnerability scans of your environment. Before the deployment, please make sure you have the proper permissions to scan your environment, even if it's just a single VLAN. Even if approval is not typically required for initiating scans, we recommend alerting the necessary service teams that scanning will be taking place. You can feel free to kick off scans before the deployment, or wait for your consultant to run scans with you.

The scan results will be used to further cover aspects of the console such as report generation and remediation projects. Without vulnerability data, these parts of the product will not be able to be covered in as much detail.

Alternatively, agents can be deployed prior to the insightVM deployment to allow them to collect vulnerability data about your environment.

Scan Credentials

Detecting all of your vulnerabilities to a high degree of confidence requires access to parts of the operating system that are usually protected through administrative controls. Running successful vulnerability scans therefore requires the same level of administrative permissions.

Rapid7 has some flexibility around how this can be accomplished, and your Rapid7 Security Consultant will provide further guidance on this topic during the deployment.

From a high level, the following options are available to you in regards to achieving administrative level access to your assets:

1. Perform network based scans, using full administrative credentials and privileges, without any restrictions (for further information see the credentialed scanning section)

2. You may deploy the Insight Agent to as many assets as possible. The Agent is able to run with local administrative privileges, and therefore does not require a domain based account. (Not all operating systems are supported however)

3. You may use the Scan Assistant, which is a *lightweight agent*, and allows the scanning of assets from the network, without the use of domain based administrative credentials.

What to Expect During Deployment:

- Project Plan
- Links to self-serve resources

Project Plan

We include below a sample project plan for an insightVM Deployment. Timing and order may be customized to your specific environment and needs, by your Rapid7 consultant during deployment.

Your deployment will be split into a minimum of 2x deployment sessions:

Project Kick-Off
Project Kick Off Call, covering the following topics: • Prerequisites discussion • Confirm that customer is able to login to the Insight Platform and can navigate to User Management, to confirm Platform Admin permissions and product access • Firewall rules complete OR verified ability to configure them during deployment calls • Service accounts in place for scanning OR admin scheduled to attend deployment calls • Change Management approvals for scanning and infrastructure changes • Server/s provisioned and accessible
First Deployment Session
Review insightVM Architecture and components
Review goals for Deployment
Install IVM Console and Scan Engine(s) & Pair the Scan Engine(s)
Ensure console is connected to platform and user accounts are properly provisioned
Insight Agent & Scan Assistant: Discuss and optionally demonstrate sample deployment of the Insight Agent and/or the Scan Assistant, including requirements and options
Verify that all access needed is in place (Firewall rules and ACL's)
Configure scan credentials
Scan template set up
Configure DHCP Discovery (if applicable)
Start Scanning: Discovery Scans & Vulnerability Scans across as many network regions as practical
Set up pre-defined assets groups and asset tags Categorize assets based on function to organization / logical grouping
Subsequent Deployment Session(s)
Ensure scans are evenly distribute across scan engines Rebalance if needed
Validate scan coverage and credentials
Reporting: Run preliminary build in reports to test credibility of scan data
User Set Up (and AD/LDAP/SAML integration)

Overview of cloud functions: - Dashboards, Cards & Reports - Remediation Projects - Query Builder - Policy Builder
Maintenance: Automation of back-up & maintenance tasks
Discuss process for disaster recovery
Review progress on next steps
Discuss next steps: How to expand insightVM coverage and features in-line with objectives determined during the deployment sessions.
Review next steps in deployment and take away tasks to be completed prior to next call
Finalize remaining configuration and deployment items
Documentation (Status Updates and insightVM Quick Start Guide)
Optional Integrations
Integrations: ● Determine the two (2) integrations available to the package ● Scoping discussions to validate integration details

Supplemental Resources

The following resources are provided to cover any additional questions you may have.

(OPTIONAL) Considerations for Proof of Concept (or OVA) consoles

I have a Proof of Concept (PoC) Console

The Proof-of-Concept (PoC) console used during your pre-sales calls was used to demonstrate the scanning, reporting, and other functions of the product. It was not configured with best practices in mind or with a full understanding of your organization's needs. Please see “Deactivating my Console” below.

OVA Console

The OVA is a quick way to stand up the insightVM console, however it is not intended to be used in production. The disks are not expanded to the full volume, default passwords exist, and the nomenclature implies Rapid7 maintains the appliance, whereas your organization will be responsible for scanning, updating, and patching the operating system of these consoles. Please see “Deactivating my Console” below.

Deactivating my Console

THIS PROCESS NEEDS TO BE COMPLETED 48 HOURS BEFORE YOUR DEPLOYMENT

Deactivating your console will remove all Insight Platform data, such as dashboards, remediation projects, and Goals & SLAs. Your existing agent associations will remain.

Steps:

- Log into your current console
- Navigate to Administration > Global and Console Settings > Console > Administer > Insight Platform and click “Deactivate”.
- Stand up the hardware for the new console but do not install insightVM at this time.

At this point you may back up your security console and discuss onboarding that during your engagement. Your consultant will advise if the console should be built from scratch.

Credentialed Scanning

For the most accurate results during scans, credentials should be supplied to insightVM in order to authenticate with the target assets. Without credentials, you will find significantly less vulnerabilities and the OS and system fingerprinting won't be as accurate.

If for whatever reason you can not obtain credentials for your devices, you can always deploy agents or the scan assistant to the target machines. Just remember that you should perform scans using your scan engines in addition to the agents to get maximum visibility into the target assets.

Please refer to the following links for additional information regarding Windows and Linux scan credentials:

Resources
Windows Authentication: Best Practices
Linux Authentication: Best Practices

Insight Agent Deployment

Agents can be installed on any Windows, Linux or Mac device on your network. The Insight Agent collects information about the target system, sends that data to the Insight Platform, and from there the data is sent to your insightVM Console. The main benefits of using the Agent are for any remote devices that can't be reached by an engine or aren't online during regular scanning, assets with heavy scanning restrictions, or assets that you don't have credentials for.

Collectors can also be installed throughout your environment if the devices that have agents on them aren't connected to the internet. Collectors act as an intermediary proxy between the agent and the internet, routing traffic through itself for environments such as a DMZ.

Additional information for deploying agents and collectors can be found at the following links:

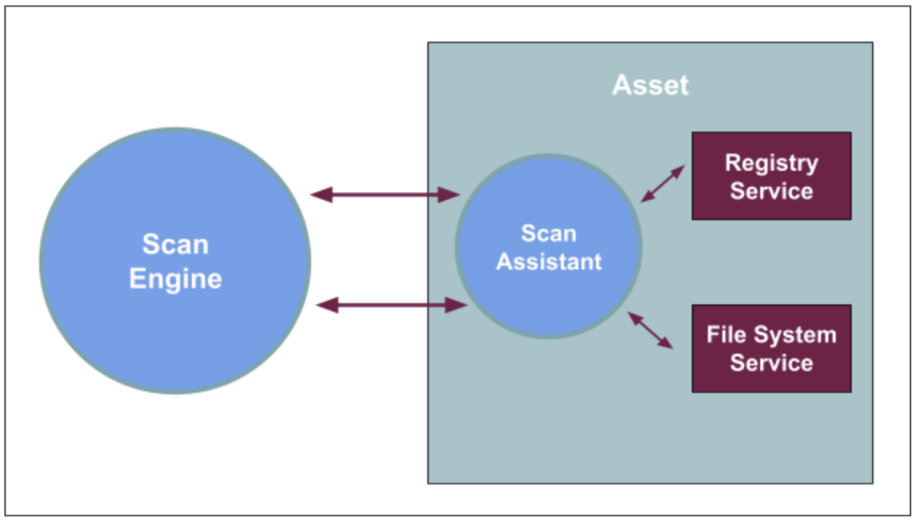
Resources
Insight Agent Overview & Help Pages

Insight Agent Installation
Mass Deployment of the Insight Agent
Collectors in insightVM

Using the Rapid7 Scan Assistant

The Scan Assistant achieves the same results as a credential scan without the need for administrative credential management and provides accurate, granular vulnerability fingerprinting and assessment for assets. The Scan Assistant allows the Scan Engine to connect directly to an endpoint in order to collect data without the need for additional credentials. A secure connection is created between the Scan Engine and the Scan Assistant by using elliptic curve asymmetric encryption (ECDSA) and advanced encryption standard (AES).

Once installed, the Scan Assistant provides Registry and File System services on the local asset and only runs when scans are performed.



You can find further information about the Scan Assistant here:
https://docs.rapid7.com/insightvm/scan-assistant/

Post-Deployment Support and Feature Requests

At the conclusion of your deployment, please use the Support link within the Insight platform. Rapid7 values input in product improvement and direction from our customers. If you have suggestions for improvements, please let your consultant know of these items so they can be added to our internal feature lists. For ongoing support of your products, please log into the Insight platform and click the question mark icon in the top right of the screen. Click “Contact Support” to create a support request.

Support and Enhancements Page: www.rapid7.com/for-customers/

Health Check

To ensure your team is using insightVM to its fullest potential, schedule a yearly health check. Rapid7 consultants will review your scanning coverage, credential usage, scan configurations, and how you are reacting to vulnerabilities.

RAPID7 | insightVM

PRODUCT BRIEF

Live Vulnerability Assessment and Endpoint Analytics

As modern networks evolve, your risk exposure changes by the minute. Each year you see the amount of data grow exponentially, the threat of attacks become more sophisticated, and the challenges of minimizing risk and optimizing operations are becoming more challenging. It sometimes feels like a never-ending battle, but overcoming risk is possible by understanding it. How? Through shared visibility, analytics, and automation—principles core to the practice of SecOps.

Utilizing the power of Rapid7's Insight platform and the heritage of our award-winning Nexpose product, InsightVM provides a fully available, scalable, and efficient way to collect your vulnerability data, turn it into answers, and minimize risk. InsightVM leverages the latest analytics and endpoint technology to discover vulnerabilities in a real-time view, pinpoint their location, prioritize them for your business, facilitate collaboration with other teams, and confirm your exposure has been reduced.

Secure Your Modern Network

Adapt to your modern network with full visibility of your ecosystem, prioritization of risk using attacker-based analytics, and SecOps-powered remediation. Pair that with unparalleled, ongoing research of the attacker mindset, and you'll be ready to act before impact.

Collect Data Across Your Ecosystem

- **Continuous Endpoint Monitoring Using the Insight Agent**
  The Rapid7 Insight Agent automatically collects data from all your endpoints, even those from remote workers and sensitive assets that cannot be actively scanned, or that rarely join the corporate network. Pair InsightVM with Rapid7 InsightIDR to get a complete picture of the risks posed by your endpoints and their users.

- **Live Dashboards**
  Drawing from fresh vulnerability data, InsightVM Dashboards are live and interactive by nature. You can easily create custom, tailored cards and full dashboards for anyone—from sysadmins to CISOs—and query each card with simple language to track progress of your security program. Visualize, prioritize, assign, and fix your exposures more easily than ever before.

> **Rapid7 has already implemented what VRM will look like in the future.**
>
> The Forrester Wave™: Vulnerability Risk Management, Q1 2018

Prioritize Using Attacker Analytics

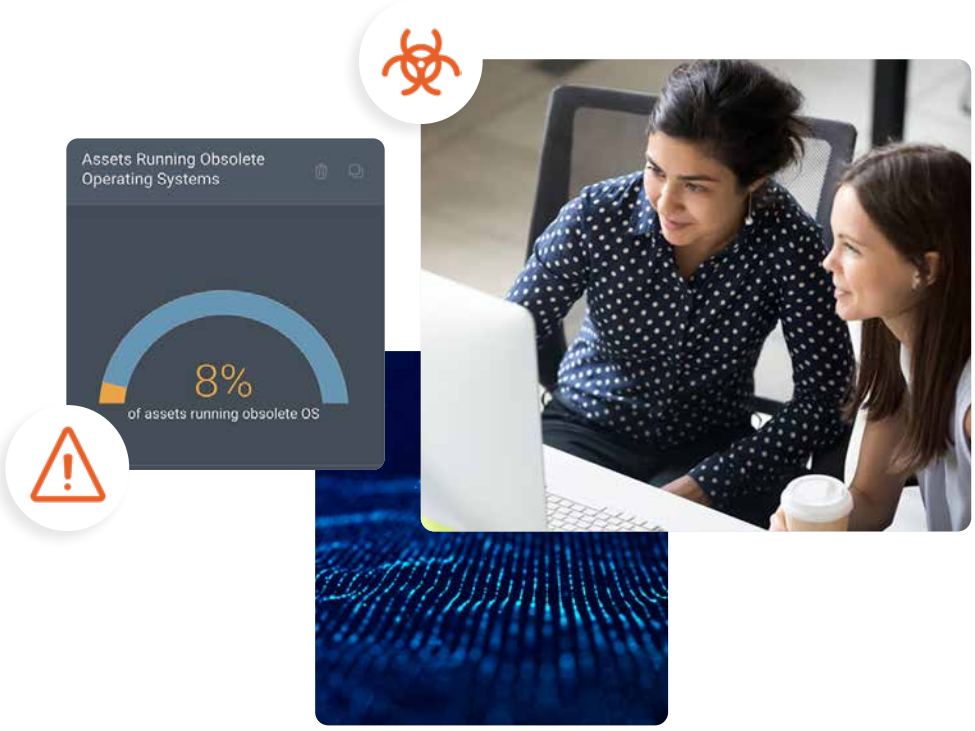
- **Attacker-Based Risk Analysis**
  Active Risk is Rapid7's vulnerability risk-scoring methodology designed to help security teams prioritize the vulnerabilities that are actively exploited or most likely to be exploited. Our approach takes into account the latest version of the Common Vulnerability Scoring System (CVSS) available for a vulnerability and enriches it with multiple threat intelligence feeds, including proprietary Rapid7 research, to provide security teams with a threat-aware vulnerability risk score.

- **Live Remediation Planning**
  Once the most critical vulnerabilities are brought to the surface, assign and track remediation duties in real time with Remediation Projects. InsightVM integrates with IT ticketing solutions like Atlassian Jira and ServiceNow, making it easy for IT to take action.

Remediate with SecOps Agility

To move faster and more securely, you need to go beyond scanning in silos. InsightVM is built to enable collaboration with IT operations and developers through shared visibility, analytics, and automation.

What does this look like in practice? InsightVM integrates with IT's existing ticketing systems to provide remediation instructions with context, thus accelerating remediation, and provides actionable reporting on program progress for every audience—from IT and compliance to the C-Suite.



"These dashboards are the best view we have of our security posture, and remediation workflows make it easy for IT to incorporate remediation into the rest of their work.

Sierra View Medical Center

Compliance and Secure Configurations, Without the Headaches

Show auditors how your environment has changed over time, demonstrating how you're compliant against PCI DSS, NERC CIP, FISMA (USGCB/FDCC), HIPAA/ HITECH, Top 20 CSC, DISA STIGS, and CIS standards for risk, vulnerability, and configuration management. Take it one step further and harden your systems based on industry best practices like CIS and DISA STIG to get your network in shape.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

rapid7.com/contact

To learn more or start a free trial, visit: **https://www.rapid7.com/try/insight/**

Additional information can be obtained at

https://docs.rapid7.com/insightvm/security-console-overview/

AGREED:

Name of Agency:_____	Name of Vendor: Network Innovation Solutions Corp
Signature:_____	Signature:_____
Title:_____	Title: CEO
Date:_____	Date: 10-7-2024

7.2.3 Any other remedies available in law or equity.

8. MISCELLANEOUS:

8.1 No Substitutions: Vendor shall supply only Contract Items submitted in response to the Solicitation unless a contract modification is approved in accordance with the provisions contained in this Contract.

8.2 Vendor Supply: Vendor must carry sufficient inventory of the Contract Items being offered to fulfill its obligations under this Contract. By signing its bid, Vendor certifies that it can supply the Contract Items contained in its bid response.

8.3 Reports: Vendor shall provide quarterly reports and annual summaries to the Agency showing the Agency's items purchased, quantities of items purchased, and total dollar value of the items purchased. Vendor shall also provide reports, upon request, showing the items purchased during the term of this Contract, the quantity purchased for each of those items, and the total value of purchases for each of those items. Failure to supply such reports may be grounds for cancellation of this Contract.

8.4 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: Robert Whitley
Telephone Number: 304-781-3410
Fax Number:
Email Address: rwhitley@gonis.us

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ OOT25*013

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)

[✓]	Addendum No. 1	[ ]	Addendum No. 6
[ ]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	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.

Network Innovation Solutions Corp
Company

Authorized Signature

10-07-2024
Date

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

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) Robert Whitley CEO

(Address) 1060 Cedar Crest Dr Huntington, WV 25705

(Phone Number) / (Fax Number) 304-781-3410

(email address) rwhitley@gonis.us

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.

Network Innovation Solutions Corp

(Company)

(Signature of Authorized Representative)

Robert Whitley CEO 10-07-2024

(Printed Name and Title of Authorized Representative) (Date)

304-781-3410

(Phone Number) (Fax Number)

rwhitley@gonis.us

(Email Address)

	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: 1521625 **Doc Description:** Addendum No 1 Enterprise Vulnerability Management SysOT25051 **Proc Type:** Central Master Agreement			**Reason for Modification:** Addendum No 1 is issued to publish questions and answers
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2024-10-04	2024-10-08 13:30	CRFQ 0231 OOT2500000013	2

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code:

Vendor Name : Network Innovation Solutions Corp

Address : 1060 Cedar Crest Dr

Street :

City : Huntington

State : WV **Country :** US **Zip :** 25705

Principal Contact : Robert Whitley

Vendor Contact Phone: 304-781-3410 **Extension:**

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

Vendor Signature X **FEIN#** 47-1734617 **DATE** 10-7-2024

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

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.

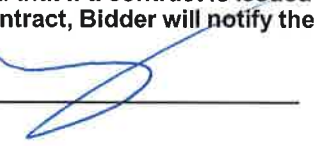
7. **Application is made for preference as a non-resident small, women- and minority-owned business, in accordance with *West Virginia Code* §5A-3-59 and *West Virginia Code of State Rules*.**
☐ Bidder has been or expects to be approved prior to contract award by the Purchasing Division as a certified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

Date: 10-7-2024 **Title:** CEO

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