

Public Records Request #2833

The following materials have been gathered in response to public records request #2833. These materials include:

- Root9B Response to RFP #269-2019-109
- Pricing Worksheet & Specifications

This information was provided as a response to a public records request on 11/18/19 and is current to that date. There is a possibility of more current information and/or documents related to the stated subject matter.

Further Information

For further information about this request or the Citywide Records Program, please contact:

Cheyenne Flotree
Citywide Records Program Manager
City of Charlotte/City Clerk's Office
600 East 4th Street, 7th Floor
Charlotte, NC 28202
Cheyenne.Flotree@charlottenc.gov

Amelia Knight
Public Records Specialist
City of Charlotte/City Clerk's Office
600 East 4th Street, 7th Floor
Charlotte, NC 28202
Amelia.Knight@charlottenc.gov



City of Charlotte Managed Security Services

Original



RFP Number#:269-2019-109
Date: July 12, 2019

COVER LETTER

Ms. Elizabeth Barnard
City of Charlotte
City Procurement
600 East 4th Street, CMGC 9th Floor
Charlotte NC 28202

REF: RFP 269-2019-109 June 13, 2019

Addendum 1 – June 28, 2019

Dear Ms. Barnard:

root9B, LLC (R9B) is pleased to provide the City of Charlotte (City) with the following proposal. Our proposal meets all City of Charlotte requirements. We address the Core Service Requirements, which includes Security Operations Center (SOC) operations, security event management, security event analysis, security incident response (IR). We also address management, as well as the Additional Service Requirements in the areas of analytics platform operations, email threat monitoring and analysis, cyber intelligence support, compromise assessment, and security system support. We understand the additional services are preferred but may not be awarded depending on cost and funding availability.

To satisfy the City's core service requirements, we offer our Intelligence-led Managed Security Service (MSS) offering with the inclusion of a Digital Forensics Incident Response (DFIR) Retainer that will facilitate the provision of security monitoring and incident management should the City need it.

As a comprehensive solution, fulfilling both the core and additional service requirements, R9B offers our Threat Intelligence-led Managed Detection and Response (MDR) service. The key differentiator to other providers is the inclusion of Threat Intelligence as an integral component of the service and not an add-on service with additional costs. R9B's MDR delivers 24/7 monitoring, management, detection, and analysis, in addition to lightweight incident response services and threat hunting. This service leverages a combination of technologies deployed at the host and network layers.

As a current provider of Security Assessments to the City of Charlotte, R9B has gained valuable knowledge of the City's security environment. This existing knowledge is beneficial in the onboarding of our services, substantially reducing the risk inherent when transitioning to a new service provider.

The information contained in the Proposal or any part thereof, including its Exhibits, Schedules, and other documents and instruments delivered or to be delivered to the City, is true, accurate, and complete. This proposal includes all information necessary to ensure the statements herein do not in whole or in part mislead the City as to any material facts.

R9B's proposal is valid for 180 calendar days per the requirement in 1.6.5. We take no exceptions to the City's sample terms included within the RFP. All costs related to the delivery of the services to satisfy the requirements of this RFP have been included and are clearly disclosed. No additional fees or charges will be incurred by the City of Charlotte other than those described in the pricing worksheet.

Sincerely,

John Harbaugh, Chief Operating Officer
root9B, LLC
90 S. Cascade Ave., Suite 800
Colorado Springs, CO 80903
719-368-3686
John.Harbaugh@root9b.com



Page intentionally left blank.

TABLE OF CONTENTS

Cover Letter	i
Table of Contents	iii
Executive Summary	1
Proposed Solution	2
A.1 Part 1- Security Operations Services (RFP 3.2)	2
A.1.1 Transition Support (RFP 3.2 [1]).....	2
A.1.2 SOC Operations, Facilities, Personnel, and Communication (RFP 3.2 [2])	4
A.1.3 Systems Access (RFP 3.2 [3]).....	5
A.1.4 Reporting (RFP 3.2 [4])	5
A.1.5 Security Event Management and Communication (RFP 3.2 [5]).....	6
A.1.6 Security Event Analysis (RFP 3.2 [6]).....	6
A.1.7 Security IR (RFP 3.2 [7])	6
A.1.8 Changes to Information Security Systems (RFP 3.2 [8]).....	8
A.1.9 Additional Service Requirements (RFP 3.2 [9])	8
A.1.10 Email Threat Monitoring and Analysis (RFP 3.2 [10]).....	9
A.1.11 Cyber Intelligence Support (RFP 3.2 [11]).....	9
A.1.12 Security System Support (RFP 3.2 [12])	10
A.1.13 Onsite Services (RFP 3.2 [13]).....	10
A.1.14 Threat Hunting (RFP 3.2 [14]).....	10
A.1.15 Compromise Assessment (RFP 3.2 [15])	11
Conclusion	12
Forms	13



This page intentionally left blank.

EXECUTIVE SUMMARY

root9B, LLC (R9B) is pleased to provide the City of Charlotte (the City) with this proposal to meet your core requirements for 24/7 monitoring and management of your network through the implementation of our Managed Security Service (MSS).

Operating from our integrated Adversary Pursuit Center (APC) in Colorado Springs, Colorado, our Security Operations Center (SOC) delivers 24/7 threat monitoring and detection



R9B's Security Operations Center

services leveraging a combination of technologies deployed at the host and network layers.

R9B's proposal satisfies the City's SOC requirements and fully meets all identified security requirements with our MSS solution. Our MSS suite allows for advanced analytics, threat intelligence, and human expertise in incident investigation. R9B provides incident validation, offers lightweight remote response services, such as threat containment, and support to restore your environment back to a form of "known good." Our MSS service uses all the information available on the network to provide a holistic view of events happening within your network. Such information includes Security Information and Event Management (SIEM) data, system-generated logging, agent-based logging, and network traffic data.

To satisfy the City's need for additional service requirements we offer our MDR solution which handles both the detection of threats and the mitigation of those threats using our proprietary threat hunting platform, ORION. Our platform inclusion gives us a unique capability to meet the response actions presented in the RFP, as well as proactively hunting for unknown and unidentified threats. Our MDR solution surpasses other vendors through delivery of managed cybersecurity services with consideration of your business context, relevant threat vectors, and Machine Learning (ML) integration. Working in concert with traditional network defense appliances and applications, R9B's MDR service delivers a flexible, active protection platform to identify, pursue, and mitigate cyber threats while managing all aspects of your cybersecurity infrastructure. R9B operators tie these various sources of data together to build a timeline of activities and correlate potentially malicious events across your enterprise. The addition of ML to the processing stack elevates R9B's technology solution to the next level. Unlike competitors' solutions, we use an explainable Artificial Intelligence (AI) which acts as an expert system to model analytics and which has operated on millions of records in real time. Our engineers can quickly tune the AI to your configurations, tailored to your unique needs. Our AI has delivered a 1000x decline in false positives in operational networks.

With a network defense strategy of pursuit and deterrence in mind, R9B developed this combination of managed security and adversary pursuit as the tailored solution for cybersecurity teams. Adversary pursuit provides the ability to aggressively hunt intruders across the network while managing and leveraging already deployed security devices.

PROPOSED SOLUTION

A.1 Part 1- Security Operations Services (RFP 3.2)

A.1.1 Transition Support (RFP 3.2 [1])

Change paves the way for innovation and fresh perspectives. However, when not handled efficiently or accurately, change can lead to unexpected interruptions in operations. R9B understands the importance of seamless transition from one contractor to another, focusing on operations and people. As an experienced cybersecurity solution provider, we have successfully transitioned several clients from their existing service providers to initiate new R9B services. Our unique experience allows us to ask the right questions and has historically enabled us to create a workflow beneficial to a well-ordered transition.

R9B will, in coordination with the City's current MSS Provider, utilize our proven, structured transition of services approach to reduce risk to the City during this critical time. At the onset, R9B assigns a dedicated Service Delivery Lead (SDL) to your account. To provide continuity of all R9B services, we will maintain Peggy Pasaol as your dedicated SDL. Our transition approach is a task-driven schedule detailing the primary and supporting task owners. Your SDL manages the transition plan, SOC resource scheduling, schedule tasks, milestones, and communication and reporting requirements. We provide details of the proposed transition plan on Form 8.

At conclusion of services, R9B works with either the identified City personnel or incoming contractor to ensure a smooth transition of data and services. We develop and provide to the City a final transition plan in accordance with established timelines. We approach the final transition of services with the high-quality professionalism and detail for the City's long-term benefit.

A.1.1.1 MSS or MDR Service Initiation

At the initiation of services, your SDL coordinates the project kick-off meeting with the transition team. This team includes the City, R9B's Technical Lead and SOC support personnel, the current MSS Provider, and the Network Operations Center (NOC) provider after contract execution. We design the kick-off meeting to discuss the engagement overview, major activities, risk planning, and timeline. Following the initial kickoff, we send to the City an in-depth MSS Onboarding plan. The SDL schedules a recurring weekly meeting with the City and the transition team to support ongoing activity.

R9B utilizes a structured, multi-phased approach for all MSS or MDR transition projects. This approach provides a framework for communication, reporting, and project delivery. We conduct the following service initiation activities at the start of the project. The duration of each activity is driven by the scope of services, to include the following:

- Security Provisioning
- Discovery
- Log Recognition and Normalization
- Service Framework Exercise

Phase 1 – Security Provisioning

We provide security provisioning if management or co-management services are included in the engagement. These services may include, but are not limited to:

- Creation of named accounts for our personnel within your network and security solutions identified as being co-managed by R9B
- Establish Virtual Private Network (VPN) (Internet Protocol Security [IPSec]) services for our personnel and/or services

Security provisioning activities may be required before Discovery can begin. We work with you to identify and prioritize tasks. This means we can accomplish some tasks in parallel with the initial discovery phase. Based on your current network configurations and the selected services, the import/provisioning of an appliance inside your network may be necessary.

Phase 2 – Discovery

The discovery phase allows the R9B Team the opportunity to review the City's current cybersecurity stance. We produce a report with our findings following the Discovery process. The entire process encompasses the following:

- Review and validate your existing security program, policies, and tools
- Confirm existing configurations of in-scope endpoints, network devices, and security appliances
- Validate existing log sources and data feeds into a SIEM
- Identify specific escalation criteria, client responsibilities, and communication procedures
- Identify gaps and provide a Discovery Report with implementation recommendations

Phase 3 – Log Recognition and Normalization

Your staff and R9B's Team (as needed) implement Phase 2 change recommendations defined in the Discovery Report. This includes:

- Modifications to existing data feeds and forwarders into your SIEM
- Establishing new data feeds of critical systems identified during Discovery
- Modifications to existing Firewall rules
- Modifications to existing Group Policy Objects/Preferences

Log Recognition, R9B's actions:

- Validate proper transport of logs from in-scope endpoints and network security appliances to your SIEM and ensure data is classified correctly
- Perform initial statistical analysis of aggregated logs and begin defining queries specific to your network
- Evaluate audit-level settings of in-scope Operating Systems (OSs), applications, services and recommend or make necessary changes
- Define and script new SIEM alerts for response to specific events and thresholds and define reporting criteria for each type of alert
- Create and edit dashboards tailored to your organization

Normalization, R9B's actions:

- Generate statistical analysis and work with you to establish threshold criteria
- Review and update tags associated with sets of fields and value pairs associated with data
- Manage and design data models and data summaries

- Map software errors and establish a client-specific baseline
- Working in concert with your team, finalize the client-specific escalation matrix and alert classification scheme

At the conclusion of Phase 3:

- Initiate and exercise limited monitoring, management, and analysis services (8 hours per day/5 days per week)
- Begin to route alerts to our APC for further investigation

Phase 4 –Service Framework Exercise

The Service Framework Exercise assesses that all service requirements are in place, including technical implementations, processes, procedures, and operational lines of communication. The one-half to full-day exercise tests these aspects in a table-top style exercise with several scenarios ensuring the team is at full operational capability.

Service Framework Exercise, R9B's actions:

- Develop exercise framework and scenarios
- Conduct exercise
- Exercise Alert Escalation based on agreed client process flow
- Continue to tune baseline settings to maintain optimal system performance

Continuous Monitoring, Management, and Analysis

Upon completion of Phase 4, R9B's services enter a sustained phase of security event monitoring and security infrastructure management on your network. Activities include, but are not limited to:

- Full 24/7 monitoring, management, and analysis services for all in-scope endpoints, network security appliances, and services
- Routing alerts within our APC Team for further investigation
- Escalating alerts appropriately based on agreed process flow
- Continued tuning of baseline settings to maintain optimal system performance

Note: During continuous operations, it may be necessary to revisit normalization activities if there is a material shift in event patterns or when you make changes to your network environment. Examples include adding new firewalls or new logging sources not previously logged.

A.1.2 SOC Operations, Facilities, Personnel, and Communication (RFP 3.2 [2])

R9B provides end-to-end security services to reduce the time, cost, and risk associated with securing your enterprise. We combine the industry-leading ORION HUNT platform with tailored MSS to provide your cybersecurity teams a unique ability to hunt across your enterprise and neutralize cyberattacks in a comprehensive MDR solution. We developed this concept to give security engineers full control of the network-operating environment to monitor, characterize, and eliminate cyber threat activity. Additionally, adversary pursuit facilitates interactive network surveys, asset management, vulnerability assessments, penetration testing, and remote live memory analysis.

Operating from our integrated 24/7 APC in Colorado Springs, R9B's SOC provides services to protect, detect, respond, and recover from cyber security threats. R9B maintains a secondary SOC located in San Antonio, TX providing continuity of operations in the event of a natural or manmade disaster.

R9B has the highest concentration of Department of Defense (DoD) certified Master Operators in the commercial space. Master Operators were certified by the DoD to recognize their expertise in multiple disciplines in the computer security domain. It is the highest certification available to operators in computer network operations. Those personnel and others on the team have decades of collective experience engaging

the most sophisticated cyber adversaries in the world. Our staff maintains leading industry certifications, as well as holding several PhDs and Master of Science degrees. As a result of this experience and expertise, we attract talent of all skill levels in this highly competitive economy and train the next generation of cyber warriors.

As part of our commitment to strong communication, R9B will notify the City of changes to any name resources. Finally, many of our MSS and MDR team possess security clearances, which demonstrates the ability to meet and pass the Criminal Justice Information Services (CJIS) requirement.

A.1.3 Systems Access (RFP 3.2 [3])

See answer for A.1.2 above.

A.1.4 Reporting (RFP 3.2 [4])

R9B maintains a weekly meeting schedule with our clients which is facilitated by the SDL. These meetings cover operational and logistical items to include the on-boarding or off-boarding of personnel from R9B attached to the project. We conduct weekly meetings and provide monthly Key Performance Indicator (KPI) metrics. As necessary, we provide significant activities reports. We conduct Quarterly Business Reviews (QBR) onsite or virtually with the City, as well as provide an annual summary report. In addition to our standard reports, R9B provides ad hoc reporting as needed. Your SDL will work with you to identify your specific reporting needs and requirements, customizing our reporting as requested.

As part of our MSS or MDR service, monthly and quarterly reporting generally focuses on significant actions taken over the time period, such as the noted KPI measurements, Service Level Agreement (SLA) adherence, and open issues to tune the service. R9B's reporting includes trend analysis, as a result we anticipate that we will immediately improve the trend of 600+ IR escalations the City is dealing with yearly through our experience and ability to quickly triage and reduce false positives.

R9B maintains a ticketing platform to track all client communications. This platform allows for auditable tracking of all incidents and allows City personnel the ability to view information regarding ongoing events. Communications with this platform are the highest current security (TLS 1.2) in transit, and the system allows granular Role-Based Access Control (RBAC) to isolate customers, as well as analysts, from others' data. Additionally, the service we use is hosted in Amazon Web Services (AWS) which uses AES256 to encrypt data at rest.

R9B's ticketing system is highly configurable and supports the following fields:

- Event summary
- Severity
- Event date and time, including time zone (in UTC)
- SOC Point of Contact
- Current status
- Attack vector
- Indicators of attack (e.g., raw logs, hashes, file names, registry entries)
- Other related incidents
- Actions taken by SOC
- Chain of custody (if applicable)
- Impact assessment
- Source hostname, IP, port, and protocol
- Destination hostname, IP, port, and protocol
- OS, including version

- Endpoint protection software versions
- Impacted department
- Identification method
- References
- Resolution

Communications with the City occur via R9B's ITSM ticketing platform (Freshservice) to maintain a system of record. For technical discussions which are not conducive to ticket-based dialog, we utilize Microsoft Teams. However, we are flexible and will utilize any platform the City prefers. We view ourselves as an integrated team member for City's cyber defense and view communication as a critical piece of our provided service.

A.1.5 Security Event Management and Communication (RFP 3.2 [5])

See section A.1.4.

A.1.6 Security Event Analysis (RFP 3.2 [6])

As part of our core service offering, MSS delivers 24/7 threat monitoring, detection and notification. If the City elects to bundle this with our MDR offering, that suite delivers these services along with management and lightweight response services leveraging a combination of technologies deployed at the host and network layers. Our MDR suite allows for advanced analytics, threat intelligence, malware triage, and human expertise in incident investigation and response. Working in concert with traditional network defense appliances and applications, R9B's HUNT platform and MDR deliver a flexible, active protection platform to identify, pursue, and mitigate cyber threats while managing all aspects of your cybersecurity infrastructure.

As previously discussed, our MDR service includes R9B's unique, industry-changing, proactive HUNT service solution. HUNT, powered by our ORION platform, preemptively identifies and counters adversaries who may already reside inside your environment. Unlike the majority of MSS security vendors, R9B's HUNT is far more than a better, more efficient log analysis. R9B's HUNT puts an active human defender in your network space to search for and respond to imminent or previously undetected compromises. Our methodology allows R9B to hunt on systems which may not be able to log to traditional security systems, giving an added layer of security to devices which may not parse or communicate with the SIEM.

Our MDR service uses all the information available on the network, including SIEM data, system-generated logging, agent-based logging, and network traffic data. Coupled with our agentless HUNT capability, we provide a holistic view of events happening within your network. R9B operators tie these various sources of data together to build a timeline of activities and correlate potentially malicious events across your enterprise.

The addition of AI to R9B's technology solution brings detection and identification to the next level. Our engineers can quickly tune the AI to your configurations, tailored to your unique needs. Our AI has delivered a 1000x decline in false positives in operational networks. We developed over 120 playbooks based on real-world events and can design custom playbooks to meet the City's needs.

A.1.7 Security IR (RFP 3.2 [7])

As part of our core offering, R9B has included an incident response retainer. Retainer Service will provide the City with access to a range of Incident Response (IR) capabilities that enable a rapid and effective response to critical cybersecurity incidents. Our Retainer Service aligns proactive IR preparedness and reactive IR engagement services to meet your unique cybersecurity demands. DFIR Retainer services cover both Incident Readiness and Incident Response with options for investigative legal support throughout.

R9B will exercise our proprietary Pre-Response Engagement Planning (PREP) methodology during onboarding to ensure full working knowledge and support of the City's overall IR capability. We pass our

PREP results to the SOC for response planning. We leverage the power of our integrated teams, which focus on Threat Intelligence and IR to achieve the highest level of security. This planning enables full synchronization of response actions between the SOC and the City to ensure systems, networks, and applications are secure.

When the SOC believes a security event warrants a DFIR event response, they will send an Incident Engagement Request (IER) to notify R9B of the potential cyber incident. Our Response Service team will spring into action to deliver the personnel and execute the methods summarized below needed to decrease the event's duration and impact.

- **DFIR Engagement Service Activation and Initial Incident Assessment.** Upon receipt of the IER, our response team will seek to confirm that the event meets the criteria for classification as a cyber incident, assess its significance, and develop an initial response plan with a recommended prioritization and estimated level of resources needed.

R9B will provide DFIR event response services remotely from our APC, onsite via a combination of the optional onsite Cybersecurity Analyst or fly-away response teams as appropriate, or through a hybrid approach as needed to resolve the incident.

- **DFIR Operations Management.** A R9B Incident Response Lead (IRL) will initiate and lead the event analysis, forensics, and malware investigative analysis teams. The IRL will coordinate with you to identify resources, implement the PREP-defined event management structure, and deploy the remote DFIR operations and communication capabilities established during PREP. The IRL will institute a response schedule, decide whether the incident warrants an on-site response, and establish a status update cadence.
- **Triage.** R9B analysts establish an evidence preservation process while they determine the tactical approach to initiate chain-of-custody, identify indicators of compromise, and conduct incident scoping. Information gained through event Triage informs forensic collection and analysis, as well as containment and threat mitigation procedures.
- **Tactical Forensic Collection and Analysis.** Analysts conduct forensic acquisition and analysis of attack artifacts using the chain-of-custody and evidence preservation procedures agreed upon during Triage. These activities consist of live system artifact collection, forensic imaging and analysis, host and network log aggregation and analysis, malware detection and sample collection, and data compromise/extraction assessment. R9B analysts will use these results to make an evidence-based determination of the attack's potential to have resulted in sensitive data exfiltration.
- **Attack Containment and Threat Mitigation.** This task involves analysis of threat behavior within the attack area. Our analysts will propose a containment and eradication strategy to aid you in immediate data asset protection efforts by isolating the attack area, monitoring threat activity, conducting deep-dive analyses as appropriate, and making eradication strategy recommendations.
- **Remote Network Interrogation.** Based on the state of network security and preliminary evidence obtained during PREP, Initial Incident Analysis, and DFIR Operations Management activities, R9B may conduct remote investigative operations on in-scope critical systems, nodes, and endpoints. These activities may occur as part of Initial Incident Analysis or later during the DFIR effort to speed system interrogations.
- **Threat Intelligence (TI).** R9B will conduct all-source intelligence research and investigation into threat actor capabilities and identity. When needed, we may perform TI profiling to focus intelligence research on your organization and industry, past event history, and other relevant indicators of potential threat targeting.

- **Malware Analysis and Reverse Engineering.** R9B analysts use static and dynamic analysis techniques to examine the effects of any malware discovered on the filesystem and in memory. Using these results, we will generate a detailed report that describes the attributes and behaviors of the malware and its impact on your environment.
- **Incident Reporting.** To develop a basis of fact for subsequent legal actions, our IRL will develop a record of the DFIR event addressing all event/incident management, response, analysis, and mitigation activities with recommendations to improve your security posture. The report will include an event/incident summary, fact-based attack narrative, forensic discovery record and timeline, TI summary, malware summary, and post-incident recommendations.

When the City selects the MDR suite, R9B's ORION platform is a force multiplier, allowing the SOC to seamlessly escalate alerts to our HUNT team to quickly validate possible threats and investigate the systems affected. ORION allows for a multitude of actions, to include vulnerability assessments of affected systems such as port scanning, service and software identification, and configuration review, as well as much more fine-grained memory analysis necessary to find advanced threats. A special feature of ORION is the ability for R9B to conduct proactive HUNT on systems searching for unreported or advanced attacks that may bypass current Tools, Tactics, and Procedures (TTPs) of other vendors. Additionally, the ORION tool allows for execution of system configuration changes to enable a containment and eradication strategy. This is augmented by our operational experience in leveraging third-party tools to support this effort as we maintain a tool agnostic approach to security.

We understand the importance of capturing lessons learned. Our processes and procedures around incident handling include the use of After Action Reports (AARs) to improve our TTPs, and will recommend changes to the City policy, process, or technology to prevent further incidents. R9B follows ITIL-based ITSM processes and has an ITIL v3 Expert on staff. Root Cause Analysis (RCA) is a key component of the AAR process, and R9B documents those lessons learned not only for incidents with the City, but for our other clients as well. This means the City receives intelligence information and planning from across many verticals giving a much broader aperture to the defense posture.

A.1.8 Changes to Information Security Systems (RFP 3.2 [8])

R9B's Security Watch Officer and SDL are available for 24x7x365 security changes. It is their responsibility to communicate and coordinate any changes of the City's information systems with the City. Responses to the requirements are handled in accordance with SLAs established by both parties during the onboarding process. We conduct the coordination of tasks in consultation with the City's change review and management board and in collaboration with the NOC.

A.1.9 Additional Service Requirements (RFP 3.2 [9])

Analytics Platform Operations

This service is part of R9B's core MSS offering. We have many years of SIEM management, development, and operations experience. Our data-agnostic ingestion connectors bring event, threat, and risk data together. This experience and the tools we utilize provide strong security intelligence, rapid incident response, seamless 24/7 log management, and extensible compliance reporting. We manage and monitor capabilities (e.g., IP flow statistics and raw packet data) via our cloud SIEM, located in the continental US (CONUS), for analysis of sensor and other data from your network devices in real time via secure channels. From the SIEM management console we also capture event/task information to generate event tickets and initiate remediation activities for any security event. We leverage these capabilities to direct events to other security services, including any dedicated third-party monitoring, for further analysis and/or incident response activities. When providing management services, we configure, maintain, and operate your SIEM. This allows us to optimize and incorporate rule sets used for automating alerts and to create event tickets for tracking. SIEM data in raw and processed format are stored for 365 days in cold storage, and we maintain a 30-day hot storage window for analysis.

By running in a cloud environment (AWS), R9B can scale to new log volumes with coordination from the City in very short order. Our experience in this type of SIEM is of value to the City to rapidly support new onboarding of data sources (less than 30 days), as well as our experience in alerting you when data outages occur. Our SIEM engineers on staff have training from Elastic search for implementing a SIEM solution, and our Platinum support license with Elastic search allows us to resolve any management, maintenance, or technical issues in less than 24-hours. This solution allows for RBAC for City personnel to log in and Single Sign On (SSO) services with Active Directory (AD) integration.

A.1.10 Email Threat Monitoring and Analysis (RFP 3.2 [10])

As part of our optional services included within MDR, we currently provide email threat monitoring services and will provide an email address specifically for reporting suspicious emails to the City. Our solution uses both automated and manual analysis of the potentially malicious email. By integrating our TI team with our Intelligence-led MDR team, we provide a unique and rapid view of the emails which are flagged as suspicious and triaged to the appropriate level by MDR. Our TI team provides enrichment and analysis of critical emails, providing actionable intelligence for the City and our MDR team.

A.1.11 Cyber Intelligence Support (RFP 3.2 [11])

We designed our focused and integrated TI analysis to identify likely threat actors, vectors, and objectives specific to you. When selected as part of the optional services, we conduct analysis through a full review of the City's business context via an extensive questionnaire and Open Source research, proprietary sources, subscription tools, and incident reports/alerts. Unlike our competitors, our integrated TI includes:

- 1) Identifying Threat Actors, Vectors, and Objectives
 - Using the City's business context to identify likely threat actors, vectors, and objectives
 - Developing threat profiles (e.g., criminal elements, hackers, Nation-State sponsored threats)
 - Identifying threat actor motivations, actor sophistication, unique threat signatures, and threat tactics
 - Reviewing the threat against the City's business context to determine impact (risk)
- 2) Actionable Intelligence Threat Escalation
 - TI discovery of critical threat information, such as indications of an imminent threat or threat already in progress, initiates an immediate Intelligence Alert to R9B's MDR analysts and the City's security staff. The alert cites the type, nature, and immediacy of the threat. The alert triggers the MDR response process to investigate and provide mitigations and/or countermeasures, as applicable.
- 3) Intelligence Hygiene
 - Periodic reviews of specific areas of Dark Web, Deep Web, and the Internet to discover external Indicators of Compromise (IoC) or targeting of the City's network. This includes regular scans of social media accounts associated with specific hacker adversary groups, searches for leaked network credentials, tailored exploits designed specifically for use against your infrastructure, and typo-squatted domains which appear to purposefully mimic the Fully Qualified Domain Name (FQDN).
 - Discovery of these indicators results in an immediate investigation into the source of the indicator. Investigation results provide greater context into the IoC, with the goal being to link it to a specific threat actor, exploit, or motivation to monitor for indications of targeting or attempts to exploit your network.

A.1.12 Security System Support (RFP 3.2 [12])

Due to our extensive experience in the security realm, we can support any services brought forth by the City. This includes Common Vulnerabilities and Exposures (CVE) monitoring, firewall configuration and support, antivirus (AV) and anti-bot solutions to include Endpoint Detection and Response (EDR) systems, VPN security monitoring and analysis, and security configuration. Given the depth of our experience, we can easily handle any of the following actions through our optional MDR suite:

- Configuration changes
- Tuning
- Rule updates
- Custom rule crafting
- CVE and OS monitoring (a Threat Intelligence specialty at R9B)
- VPN tuning and configuration
- Firewall policies
- Rules
- Media Access Controls (MACs)

As we are a solution agnostic provider, we pride ourselves on our cyber excellence in breaking down vendor tools and capabilities to their core components and seamlessly supporting those technologies. For any other services, R9B will work collaboratively with the City's IT services company to address the requirements.

Our personnel have a wide and deep range of skills and experience. Our staff have designed, architected, developed, and deployed a real-time Distributed Denial of Service (DDoS) detection system to protect DoD networks globally. Supporting the City's DDoS system and coordinating with vendors is a function we are well-positioned to support due to our experience in incidents, debugging, coordination, blacklisting, and custom signature creation.

We are leaders in Security Operations, Analytics, and Reporting (SOAR). Our ORION HUNT tool offers many automation and orchestration features, including integration with Ansible. We leverage our cadre of personnel to conduct and support DevSecOps functions such as automating DMZ creation, firewall updates, and DDoS blacklisting. We also offer the ability to monitor these implementations.

A.1.13 Onsite Services (RFP 3.2 [13])

As part of our additional services, R9B can provide the City with qualified Tier 3 Infrastructure Security Engineer and Tier 3 Cyber Security Analyst candidates for approval to staff the optional full-time onsite positions. The candidates will meet the requirements set forth in the RFP. We will transition the individuals within 30 days following City approval. We have deep experience supporting onsite staffing requirements. We currently staff positions in the private sector and Government agencies, including cyber operations supporting national agencies. We maintain a professional recruiting staff and have an excellent pipeline of candidates to meet the requirements from our training and military backgrounds. Due to this pipeline of candidates, the supplied Tier 3 personnel have unmatched experience in the real-world fighting cyber adversaries, including specialized training in Cyber Threat Intelligence which allows the analyzing and synthesis of data.

A.1.14 Threat Hunting (RFP 3.2 [14])

Threat Hunting is a key component to our MDR suite. It is about people, processes, and technology. Technology alone does not solve this problem. Instead, HUNT enables a thinking network defender to actively engage the adversary. A human network defender generates a response that is not automated, that the adversary could not calculate, and that limits or destroys an adversary's capabilities. HUNT is about gaining an advantage when the adversary tries to bring the fight to your network. We view HUNT as an observable, measurable, and repeatable four-step process beginning with a clear goal or hypothesis and ending with knowledge gained and an action taken.

Step 1 – Focused Collection: We generally use Step 1 to identify the activity on your network infrastructure. This assumes or helps build an understanding of the operating environment. This step consists of learning how your environment truly lives, breathes, and moves. Once we have built a “baseline” of the environment, everything else becomes anomalous. This is not an attempt to hunt everything at the same time. Instead, the goal is to understand the technologies that support your key business operations and identify the adversary’s motive(s) and begin the search there. We conduct focused HUNTs on the system or systems identified during the escalation process.

Step 2 - Identification of IOC: Step 2 occurs when something outside of the known-good baseline is identified. It can be a benign, previously unidentified business application or it may be malicious code operating in your environment. This could be created by insider threats, hacktivist groups, script kiddies, or advanced threats.

Step 3 – Target Collection and Analysis: The identification of an IOC generates “patient 0” – a starting point to begin an investigation, grow a hypothesis, and remove uncertainty. This step is a human-driven step. As we define a human’s normal workflow, we look for ways to automate repetitive tasks with expert SOAR products that introduce efficiencies. Until those can be implemented, the human is discovering the “evidence” to collect - and then using that newly discovered “artifact” to scan the remainder of the network. No longer are we playing “whack-a-mole.”

Step 4 – Response: This is the real differentiation in our definition of HUNT operations. We are not using the word “response” as the post-incident, forensic investigation of the activity. Instead, participate in a “cyber knife fight”, actively engaging the human on the other end of the wire for control of your network asset(s). This requires thought, adaptive response activities, and an understanding (intelligence) of how your adversary maneuvers (techniques). This is bringing the fight to the attacker and damaging their freedom of movement in your controlled environment.

At R9B, we build technologies and offer services with the above-defined process in mind. It is important to understand whether other technologies or platforms support your internal defensive processes or simply add to the noise. Any considered technologies or platforms must support a better understanding of the operating environment. They should enable you to pass on additional cost to the adversary by forcing them to shift focus or techniques.

A.1.15 Compromise Assessment (RFP 3.2 [15])

As part of the additional services, we will use ORION HUNT to respond to events in City networks exceeding the 80-hour requirement to evaluate the City for successful intrusion or exfiltration of data. Hunting internally exploits a former weakness for defenders, as internal networks are often conceded to adversaries. Additionally, R9B will utilize the proprietary ORKOS credential risk assessment tool to evaluate City networks for weak and re-used credentials. Credential abuse is a leading vector for adversaries to access and exploit networks, and the evaluation and remediation of this vector will greatly enhance the City’s cyber security posture.



CONCLUSION

Government and corporate infrastructure and data is under attack. The adversary is advanced and persistent; currently the vast majority of network defense dollars and energy goes to boundary defenses. This technology is no match for your adversary. The City requires a vendor to provide monitoring of technology security devices for attacks or malicious activity and protection of your critical information technology assets. Such services must include event correlation and log analysis, coupled with incident response and risk mitigation capability. R9B understands the City's needs and desires for advanced cybersecurity protection. We have an extensive client base of Fortune 500 customers, supporting similar concerns and battling similar adversaries. The City stands to benefit from our years of experience, quality of our personnel and advanced technologies. Not only have we been successful in reducing false positives, but we've prevented attacks before they were able to be successful.

R9B's core offering is an Intelligence-led MSS solution with the inclusion of an Incident Response Retainer. Immediately we begin engaging with City personnel, ensuring smooth transition from the incumbent contractor and onboarding, allowing for efficient and effective ongoing managed security services.

In support of the City's totality of needs, including both core and additional services, we offer our comprehensive MDR suite. The purchase of MDR allows us to address management, as well as analytics platform operations, email threat monitoring and analysis, cyber intelligence support, compromise assessment, and security system support as necessary. Paired with Threat Intelligence that actively scans the Dark Web and other forums for data leaks and the ability to be tipped and queued by MSS services, R9B provides a blanket of protection over City networks. Due to the integrative nature of these services, the City would realize economies of scale and a reduced cost when compared to procurement of services individually. R9B is confident that our team of experienced Operators and Analysts, together with the technologies and tools they utilize, meet and/or exceed the requirements of the RFP at a value that other vendors cannot offer. We look forward to supporting the City's security initiatives.

FORMS

The following forms are included in the subsequent pages:

- The “Addenda Receipt Confirmation” set forth in Section 6, Form 2
- The “Proposal Submission” set forth in Section 6, Form 3
- The “Pricing Worksheet” set forth in Section 6, Form 4
- The “MWSBE Utilization” form set forth in Section 6, Form 5
- The “Company’s Background Response” form set forth in Section 6, Form 6
- The “References” set forth in Section 6, Form 7
- The “Additional Company Questions” set forth in Section 6, Form 8
- The “Certification Regarding Debarment, Suspension and Other Responsibility Matters” set forth in Section 7, Form 9
- The “Byrd Anti-Lobbying Certification” set forth in Section 7, Form 10
- Exceptions to the Remainder of the RFP, including the Sample Contract in Section 7



REQUIRED FORM 2 – ADDENDA RECEIPT CONFIRMATION

RFP # 269-2019-109

Managed Security Services

Please acknowledge receipt of all addenda by including this form with your Proposal. All addenda will be posted to the NC IPS website at www.ips.state.nc.us and the City's Contract Opportunities Site at <http://charlottenc.gov/DoingBusiness/Pages/ContractOpportunities.aspx>.

ADDENDUM #:

1

**DATE ADDENDUM
DOWNLOADED FROM NC IPS:**

June 28, 2019

I certify that this proposal complies with the Specifications and conditions issued by the City except as clearly marked in the attached copy.

John Harbaugh

(Please Print Name)

07/11/19

Date

Authorized Signature

Chief Operating Officer

Title

root9B (R9B)

Company Name

REQUIRED FORM 3 – PROPOSAL SUBMISSION FORM

RFP # 269-2019-109

Managed Security Services

This Proposal is submitted by:

Company Name: root9B, LLC (R9B)

Representative (printed): John Harbaugh

Address: 90 S. Cascade Ave., Suite 800

City/State/Zip: Colorado Springs, CO 80133

Email address: john.harbaugh@root9b.com

Telephone: 719-368-3686
(Area Code) Telephone Number

Facsimile: N/A
(Area Code) Fax Number

The representative signing above hereby certifies and agrees that the following information is correct:

1. In preparing its Proposal, the Company has considered all proposals submitted from qualified, potential subcontractors and suppliers, and has not engaged in or condoned prohibited discrimination.
2. For purposes of this Section, discrimination means discrimination in the solicitation, selection, or treatment of any subcontractor, vendor or supplier on the basis of race, ethnicity, gender, age or disability or any otherwise unlawful form of discrimination. Without limiting the foregoing, discrimination also includes retaliating against any person or other entity for reporting any incident of discrimination.
3. Without limiting any other provision of the solicitation for proposals on this project, it is understood and agreed that, if this certification is false, such false certification will constitute grounds for the City to reject the Proposal submitted by the Company on this Project and to terminate any contract awarded based on such Proposal.
4. As a condition of contracting with the City, the Company agrees to maintain documentation sufficient to demonstrate that it has not discriminated in its solicitation or selection of subcontractors. The Company further agrees to promptly provide to the City all information and documentation that may be requested by the City from time to time regarding the solicitation and selection of subcontractors. Failure to maintain or failure to provide such information constitutes grounds for the City to reject the bid submitted by the Company or terminate any contract awarded on such proposal.
5. As part of its Proposal, the Company shall provide to the City a list of all instances within the past ten years where a complaint was filed or pending against the Company in a legal or administrative proceeding alleging that the Company discriminated against its subcontractors, vendors or suppliers, and a description of the status or resolution of that complaint, including any remedial action taken.



6. The information contained in this Proposal or any part thereof, including its Exhibits, Schedules, and other documents and instruments delivered or to be delivered to the City, is true, accurate, and complete. This Proposal includes all information necessary to ensure that the statements therein do not in whole or in part mislead the City as to any material facts.
7. None of Company's or its subcontractors' owners, employees, directors, or contractors will be in violation of the City's Conflict of Interest Policy for City, Secondary and Other Employment Relationships (HR 13) if a Contract is awarded to the Company.
8. It is understood by the Company that the City reserves the right to reject any and all Proposals, to make awards on all items or on any items according to the best interest of the City, to waive formalities, technicalities, to recover and resolicit this RFP.
9. This Proposal is valid for one hundred and eighty (180) calendar days from the Proposal due date.

I, the undersigned, hereby acknowledge that my company was given the opportunity to provide exceptions to the Sample Contract as included herein as Section 7. As such, I have elected to do the following:

Include exceptions to the Sample Contract in the following section of my Proposal: _____

Not include any exceptions to the Sample Contract.

I, the undersigned, hereby acknowledge that my company was given the opportunity to indicate any Trade Secret materials or Personally Identifiable Information ("PII") as detailed in Section 1.6.2. I understand that the City is legally obligated to provide my Proposal documents, excluding any appropriately marked Trade Secret information and PII, upon request by any member of the public. As such, my company has elected as follows:

The following section(s) of the of the Proposal are marked as Trade Secret or PII: _____

No portion of the Proposal is marked as Trade Secret or PII.

Representative (signed): _____

A handwritten signature in black ink, written over a horizontal line.



REQUIRED FORM 4 – PRICING WORKSHEET

RFP # 269-2019-109

Managed Security Services

Regardless of exceptions taken, Companies shall provide pricing based on the requirements and terms set forth in this RFP. Pricing must be all-inclusive and cover every aspect of the Project. Cost must be in United States dollars. **If there are additional costs associated with the Services, please add to this chart. Your Price Proposal must reflect all costs for which the City will be responsible.**

For purposes of this RFP, assume an initial term of three (3) years, with the City having an option to renew for two (2) additional consecutive one (1) year terms thereafter.

R9B's Pricing Worksheet can be found in Excel spreadsheet in Attachment A- Pricing Worksheet on the following pages and digitally.



REQUIRED FORM 5 – M/W/SBE UTILIZATION

RFP # 269-2019-109

Managed Security Services

The City maintains a strong commitment to the inclusion of MWSBEs in the City’s contracting and procurement process when there are viable subcontracting opportunities.

Companies must submit this form with their proposal outlining any supplies and/or services to be provided by each City certified Small Business Enterprise (SBE), and/or City registered Minority Business Enterprise (MBE) and Woman Business Enterprise (WBE) for the Contract. If the Company is a City-registered MWSBE, note that on this form.

The City recommends you exhaust all efforts when identifying potential MWSBEs to participate on this RFP.

Company Name:	root9B (R9B)
----------------------	--------------

Please indicate if **your company** is any of the following:

MBE WBE SBE None of the above

If your company has been certified with any of the agencies affiliated with the designations above, indicate which agency, the effective and expiration date of that certification below:

Agency Certifying: _____ Effective Date: _____ Expiration Date: _____

Identify outreach efforts that *were employed* by the firm to maximize inclusion of MWSBEs to be submitted with the firm’s proposal (attach additional sheets if needed):

R9B conducted an exhaustive search of small businesses (of any type) to identify potential partners offering equal or superior cybersecurity services or technologies to R9B. R9B was unable to identify candidate companies that meet our technical or operational capabilities.

Identify outreach efforts that *will be employed* by the firm to maximize inclusion during the contract period of the Project (attach additional sheets if needed):

R9B will continue to conduct exhaustive searches for small businesses that can provide equivalent cybersecurity services or technologies. We will continue to pursue small businesses who can provide specialized cyber services and technologies beyond the capacity of R9B. We will give preferential consideration for qualified MWSBE companies followed by companies located in and around the City of Charlotte.

[Form continues on next page]



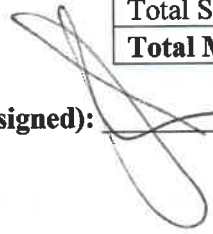


List below all **MWSBEs** that you intend to subcontract to while performing the Services:

Subcontractor Name	Description of work or materials	Indicate either "M", "S", and/or "W"	City Vendor #
N/A			

Total MBE Utilization	%
Total WBE Utilization	%
Total SBE Utilization	%
Total MWSBE Utilization	%

Representative (signed):



7/11/19
Date

John Harbaugh
Representative Name

N/A
Estimated Total Contract Value



REQUIRED FORM 6 – COMPANY’S BACKGROUND RESPONSE

RFP # 269-2019-109

Managed Security Services

Companies shall complete and submit the form below as part of their response to this RFP. Additional pages may be attached as needed to present the information requested.

Question	Response
Company’s legal name	root9B, LLC
Company Location (indicate corporate headquarters and location that will be providing the Services).	90 S. Cascade Ave, Ste. 800 Colorado Springs, CO 80903
How many years has your company been in business? How long has your company been providing the Services as described in Section 3?	root9B, LLC (R9B) was founded in 2011 as a cybersecurity training company. We have been providing Managed Security Services (MSS) since 2013.
How many public sector (cities or counties) clients does your company have? How many are using the Services? Identify by name some of the clients similar to City (e.g., similar in size, complexity, location, type of organization).	Due to the sensitive nature of the work performed the following references will remain redacted. R9B will provide references to City of Charlotte upon direct request and through a secure channel to protect client confidentiality.
List any projects or services terminated by a government entity. Please disclose the government entity that terminated and explain the reason for the termination.	We have never had a contract terminated by the government.
List any litigation that your company has been involved with during the past two (2) years for Services similar to those in this RFP.	We have never faced litigation for any service including the services listed by the RFP.
Provide an overview and history of your company.	<p>Since 2011, R9B has been a provider of advanced cybersecurity products, services, and training for commercial and public sector clients. Combining cutting-edge technology, tactics development, and deep mission experience, R9B personnel leverage their professional and intelligence backgrounds to execute vulnerability analysis, intelligence-led managed security services, incident response, and threat HUNTING (HUNT) worldwide.</p> <p>R9B is a team of pioneers and trailblazers. In 2013, we introduced the concept of threat HUNTING (HUNT) to commercial markets with the release of the ORION HUNT platform. Since then, ORION has been deployed to HUNT threats in public and private sector networks around the world. In 2018 ORION was named CSO Magazine’s Hottest Products at RSA and in 2019, ORION earned the prestigious Edison Award for applied technology, in recognition of its</p>



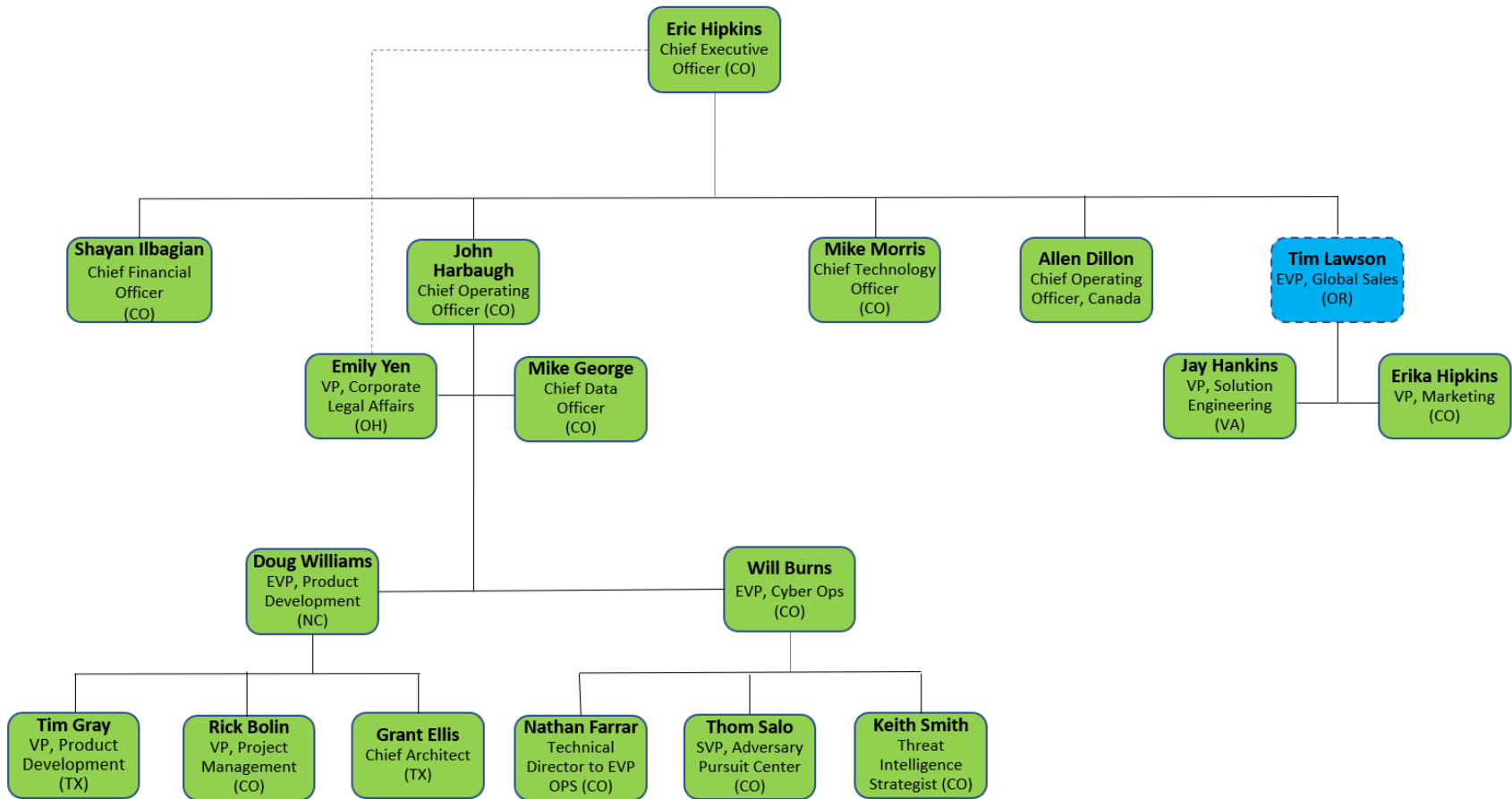
	<p>innovative approach to the challenges faced in cybersecurity. R9B’s product development and managed cybersecurity services are differentiated by integrating Threat Intelligence and client relevant business context into all aspects of our mission directed approach. We maintain dedicated Security Operations Centers in Colorado Springs, San Antonio, and Annapolis Junction where our cyber defense operators actively monitor and patrol global networks 24 hours a day, 7 days a week.</p> <p>We are tireless in our pursuit of improving network security and defending our clients’ enterprise from cyber adversaries. Many cyber companies promise “foolproof” software and technology solutions. While these solutions are necessary and can form the basis for action while providing valuable data to support situational awareness, and integrated cybersecurity operations, they are only tools which remain defeatable. Rather than layering on more technology, we augment our clients’ existing security technology investment to HUNT and eradicate the adversaries that defeat existing passive security technologies. Every product and service we offer takes into account the adversary’s tactics and techniques which we have learned through decades of experience and are strengthened by integrating expert Threat Intelligence. R9B takes a human-led, technology-accelerated approach to cybersecurity.</p>
<p>If your company is a subsidiary, identify the number of employees in your company or division and the revenues of proposing company or division.</p>	<p>N/A</p>
<p>Identify the percentage of revenue used for research and/or development by the proposing company or division.</p>	<p>N/A</p>
<p>Identify any certifications held by your company if you are implementing or reselling another company's products or services. Include how long the partnership or certification has been effect.</p>	<p>N/A</p>
<p>Describe your company’s complete corporate structure, including any parent companies, subsidiaries, affiliates and other related entities.</p>	<p>root9B, LLC is a wholly owned subsidiary of R9B, LLC. We have one subsidiary organization, root9B Canada, Inc.</p>



<p>Describe the ownership structure of your company, including any significant or controlling equity holders.</p>	<p>root9B, LLC is a Limited Liability Company. In September 2017 R9B was acquired by Tracker Capital Management, LLC ("Tracker Capital"), an early stage investor focused principally on emerging technologies and companies with the potential to advance U.S. national security interests. root9B operates as an independent, privately-held company.</p>
<p>Provide a management organization chart of your company's overall organization, including director and officer positions and names and the reporting structure.</p>	<p>Please see org chart at the end of this Form.</p>
<p>Describe the key individuals along with their qualifications, professional certifications and experience that would comprise your company's team for providing the Services.</p>	<p>R9B has over 90% Veterans on MSS teams. We provide continuous training, both external and R9B led from our course catalog and it's 100% U.S. based. We have decades of cybersecurity expertise battling real-world, nation-state adversaries and trans-national criminal organizations. We have Industry accepted certifications (SANS, CompTIA, ISC2,etc) and education considered in lieu of operational experience. Our experience spans Global, Law Enforcement, and Commercial Cyber Security Industry. We have SIEM Architects and Engineers Multiple Platforms – SPLUNK, LogRhythm, Elastic, qRadar. Our Security engineers hold the following certifications; Net+, Sec+, Linux+, Elastic Engineer, Splunk Power User, OSCP, Amazon Certified Cloud Practitioner (CCP). We are ready to recruit and train any additional resources that City of Charlotte may need on this effort.</p>
<p>If the Proposal will be from a team composed of more than one (1) company or if any subcontractor will provide more than fifteen percent (15%) of the Services, please describe the relationship, to include the form of partnership, each team member's role, and the experience each company will bring to the relationship that qualifies it to fulfill its role. Provide descriptions and references for the projects on which team members have previously collaborated.</p>	<p>N/A</p>
<p>Explain how your organization ensures that personnel performing the Services are qualified and proficient.</p>	<p>R9B is currently providing the required services to several organizations and has a collective experience of hundreds of hours of network monitoring, management and analyst experience. As such, our MSS staff are experienced and skilled in a wide array of network monitoring and management techniques and procedures gained through many years of experience and through a</p>



	<p>high volume of cases in both the public and private sectors. R9B has instituted a technical competency and apprenticeship program for all technical staff to evaluate related skills against industry standards and to provide guidance in skill/career advancement. All MSS staff are assigned work based on their demonstrated level of competency. All MSS staff have displayed practical knowledge in execution of the network monitoring and management and have achieved industry recognized certifications in various methodology.</p>
<p>Provide information regarding the level of staffing at your organization’s facilities that will be providing the Services, as well as the level of staffing at subcontractors’ facilities, if known or applicable.</p>	<p>R9B maintains two Adversary Pursuit Centers that are fully staffed for around-the-clock monitoring of client networks.</p>
<p>If your company has been the subject of a dispute or strike by organized labor within the last five (5) years, please describe the circumstances and the resolution of the dispute.</p>	<p>N/A.</p>
<p>Describe your security procedures to include physical plant, electronic data, hard copy information, and employee security. Explain your point of accountability for all components of the security process. Describe the results of any third party security audits in the last five (5) years.</p>	<p>R9B maintains comprehensive security policies and procedures to include all facets of security, from physical, to electronic data. Our security procedures are broken up into General Security, Physical Security, Information Systems Security, and Program Security. Each sect is facilitated by a specialized security manager. All security standards are laid out in our detailed Standard Security Policies and is available upon request.</p> <p>We don’t submit to 3rd Party Audits of our enterprise. Our suppliers subject to SOC compliance requirements do have audits and we have access to their statements (AWS, Data 102). We perform internal security assessments. As a Cyber Security provider, R9B regularly conducts self-delivered security assessments and exercises. These assessments include no-notice social engineering, internal and external penetration testing, credential risk assessment and wireless vulnerability testing. We utilize the same advanced cyber services and capabilities we provide to our clients to assess ourselves. Depending on the category, the assessments are either continuous no-notice or scheduled on a quarterly, annually or ad hoc.</p>



REQUIRED FORM 7 – REFERENCES

RFP # 269-2019-109

Managed Security Services

Companies shall complete the form below. The City’s preference is for references from organizations of similar size or where the Company is performing similar services to those described herein. If such references are not available, individuals or companies that can speak to the Company’s performance are adequate.

Due to the sensitive nature of the work performed the following references will remain redacted. R9B will provide references to City of Charlotte upon direct request and through a secure channel to protect client confidentiality.

REFERENCE 1:

Name of Client: _____ Main Phone: _____

Address: _____

Primary Contact: _____ Title: Director – Information Security

Contact Phone: _____ Contact E-mail: _____

Service Dates: February 2019 - Present

Summary & Scope of Project: Since February 2019 through 2022 we have been conducting full-spectrum network cyber defense operations that monitors, assesses, and actively defends [REDACTED] [REDACTED] worldwide infrastructure. The program objectives include identifying vulnerabilities, enumerating the attack surface, estimating adversary exploitation risk and impact, and providing remediation services for affected devices and information systems. The work includes [REDACTED] requested cyber defense and Managed Security Services (MSS) support as well as Active Adversarial Pursuit (HUNT) operations and supporting Managed Detection and Response (MDR).

We are responsible for monitoring ~450 routers, ~70 switches, ~600 Windows Servers, and over 7000 endpoints. SIEM support also included monitoring of [REDACTED]’s Intrusion Detection/Prevention Systems (IDS/IPS). We were able to leverage the clients LogRhythm SIEM/Management console to support all MSS/MDR functions to monitor, events and endpoints, capture information, and to provide remediation and advanced reporting functionality.

Contract Value: \$1,800,000 Number of Client Employees: ~19,000

REFERENCE 2:

Name of Client: _____ Main Phone: _____

Address: _____

Primary Contact: _____ Title: Sr. Director II, Incident Response and Cyber Hunt

Contact Phone: _____ Contact E-mail: _____

Service Dates: July 2018 - Present

Summary & Scope of Project: From July 2018 through Q4 2019 R9B is providing SME support to _____ . Our SME services integrate our HUNT capability into the client's existing security operations.

The primary objectives are to:

- Integrate and assist Walmart defense teams.
- Provide operational recommendations and guidance.
- Provide On-The-Job type training (OJT) using existing tools. OJT can include over the shoulder walk throughs, coaching, and mentoring within the normal working environment.
- Lead or provide input to HUNT operations data analysis.
- Collect and analyze a combination of endpoint and network generated artifacts to identify anomalous behavior.
- Collaborate with Walmart's security professionals to eradicate or mitigate any compromise
- Participate and support meetings and coordination events.

Combined, these services enable _____ enhanced detection and response capabilities through the guidance of our seasoned SME staff. Our HUNT platform is capable of performing real-time monitoring and detection of threats across all network aspects.

Contract Value: \$160,000 Number of Client Employees: ~2.2 million worldwide



REFERENCE 3:

Name of Client: _____ Main Phone: _____

Address: _____

Primary Contact: _____ Title: Sr. Director IT Security

Contact Phone: _____ Contact E-mail: _____

Service Dates: January 2017 - Present

Summary & Scope of Project: From January 2017 to present day R9B is providing _____ with a variety of cybersecurity services, including a cybersecurity architecture and vulnerability assessment, Digital Forensics Incident Response (DFIR) retainer, and ORKOS credential risk assessment. We performed a full system architecture assessment to determine the client's security architecture conformance to industry best standards, and applied recommendations/corrective actions to solve any deficiencies. Along with this we deployed penetration testing and vulnerability assessments on the Client's internal devices and information systems, wireless access points, web site applications, and conducted a social engineering campaign. Our professional operators possess the intimate knowledge and level of expertise to navigate and determine all weak points within the client's networks and generate reports for mitigation. This expertise translates strongly to network management responsibilities, as our staff whom conduct architecture review are capable to conduct MSS.

In addition, we provided the Client with DFIR and ORKOS services. Our DFIR retainer service provides the client with rapid/on-call response capability to any threats to their network sovereignty. This service will identify and eliminate these threats quickly and effectively before any consequences arrive. Our ORKOS assessment scanned over 2,000 systems to determine any credential risk within the Client's network.

Contract Value: \$238,132 Number of Client Employees: ~3,400



REFERENCE 4:

Name of Client: _____ Main Phone: _____

Address: _____

Primary Contact: _____ Title: Manager of Security Operations

Contact Phone: _____ Contact E-mail: _____

Service Dates: October 2014 – September 2017

Summary & Scope of Project: From October 2014 through September 2017 we have provided _____ with Network Defense Operations. We conduct full spectrum Defense Cyber Operations including our Active Adversary Pursuit (HUNT) operations to hunt, identify, stop, and remove intruders that existing passive security solutions are no match for. Our operators observed Client operations and provided recommendations to improve cybersecurity operations and insight into the actions of a 3rd party Service Operations Center (SOC). We ensured the Client was informed of potential events, the status of elevated tickets, and the circumstances of their closure. Revisions to the notification process now make _____ leadership a main player in the ticket status and decision closure process.

Additionally, R9B's operational support to _____ is focused on enterprise vulnerability identification and mitigation, active defense via our Adversary Pursuit (HUNT) operations, and Threat Intelligence. Our HUNT methodologies and tool sets allow cyber operators to pursue and identify active adversaries or artifacts of adversary movement within their network. HUNT operators analyze systems and networks containing critical and high-level vulnerabilities identified during Attack Surface Baseline (aka Penetration Testing) activities. HUNT operators preformed a broad collection approach throughout the _____ network to obtain solid baseline and better understanding for use in subsequent cybersecurity efforts.

Contract Value: \$1,844,496 Number of Client Employees: ~69,000

REFERENCE 5:

Name of Client: _____ Main Phone: _____

Address: _____

Primary Contact: _____ Title: Chief Information Security Officer

Contact Phone: _____ Contact E-mail: _____

Service Dates: January 2018 – February 2019

Summary & Scope of Project: R9B provided incident triage and DFIR services to the Client. The client experienced an incident and recruited our services to perform triage of said incident as well as a retainer service to prevent the occurrence of future incidents. Incident triage included reviewing all Indicators of Compromise (IoC) collected by Client staff, and aggregation, correlation, and analysis of log data. In addition, we performed log data analysis, along with malware and memory analysis. Following initial analysis, we preserved all collected evidence/artifacts and performed deep dive analysis of affected systems. Our DFIR retainer service provides the client with rapid/on-call response capability to any threats to their network sovereignty. This service will identify and eliminate these threats quickly and effectively before any consequences arrive.

Contract Value: \$100,000 Number of Client Employees: ~4,600



REQUIRED FORM 8 – ADDITIONAL COMPANY QUESTIONS

RFP # 269-2019-109

Managed Security Services

Companies shall include responses to the additional questions posed below. Responses may be provided on a separate sheet provided that such response clearly includes the question reference numbers.

General Questions:

1. What steps will your organization take to ensure that the transition of Services runs smoothly?

R9B utilizes a structured execution approach for all Managed Security Service transition projects. This approach provides a framework for communications, reporting, and project delivery. R9B will develop a client-specific transition plan and schedule in conjunction with City, the incumbent MSS provider, and the NOC provider. The R9B SDL will monitor and manage the transition plan and schedule. R9B will schedule weekly conference calls and provide weekly progress reports. The SDL will work with City to identify, review, and mitigate any risks.

2. Prepare and submit a Project Plan to describe all times, tasks and resources associated with the performance of Services.

R9B prepared a proposed client-specific transition plan which details roles and responsibilities of all parties involved and a proposed schedule of activities. Please reference MSS Transition Services Plan, **Appendix A**, and its attachment for complete details.

3. Describe the communications scheme that your organization will use to keep the City informed about the Services.

R9B will create a client-specific communication plan. The Communication Plan captures how R9B will manage communications throughout the project's life cycle. The plan describes scheduled and periodic communications occurring between the project stakeholders and the project team, as well as communications between the project team itself. The plan addresses the audience's needs for standardized communications to convey project awareness, status, and issues.

Within the Communications Plan is a Communications Matrix that will serve as the foundation of who, what, where, when, why, and how the project team will communicate with project stakeholders.

The objective of the Communication Plan is to provide support to the City's MSS project team by:

- Communicating to stakeholders the value and necessity of cooperating in City's MSS project initiatives.
- Establishing and maintaining momentum to keep City's MSS project efforts moving forward.

The Communication Plan identifies the procedures used to manage communication for the City's MSS project. The plan focuses on formal communication elements. Other communication channels exist on informal levels and enhance those discussed within the plan. The plan is not intended to limit, but to enhance communication practices. The plan will define Roles and Responsibilities, the project structure, stakeholder information requirements, internal communications, formal communications (status meetings, status reports, risk communication) and the escalation process.



4. Describe the risks associated with this Contract. What contingencies have been built in to mitigate those risks?

There are risks associated with every transition. To manage the risks, R9B takes a stringent, unwavering approach to transitions. Transitions are executed in a non-disruptive and responsive manner. R9B prepares in advance to manage any issues that might arise.

Through our risk management approach, we identify all risks and put in place mitigation plans. Risk analyses address all aspects of a project and include elements such as Financial impact, Schedule impact, and Quality impact. The following chart details initial risks identified by R9B for this proposal.

RISK	IMPACT	MITIGATION
Communication Challenges	Schedule	1. Centralized support through a single SDL representative. 2. Appointment of a backup SDL to ensure client contact with operators and management to communicate any issues.
Schedule Timelines	Schedule	1. Daily and/or weekly communication with City, IMP, and NOC to resolve schedule issues. 2. Commence planning upon award. 3. If necessary, additional resources added to meet timelines. 4. Minimal changes during on-boarding phase. 5. Break the project down to logical sub-projects to maintain control and manage risk.
Discovery of Unmonitored Devices by Incumbent MSS Provider	Quality	1. Develop Discovery Report with recommendations for additional monitoring. 2. Test integration points during onboarding.
Outage Impacting SIEM	Quality	Work with NOC to troubleshoot issue and correct.
Incumbent MSS Provider Fails to Conduct Handover	Quality	1. Carry out comprehensive testing prior to handover. 2. SDL will communicate status of transition issues.

5. Please fill out the Application Performance Monitoring and NOC Performance Monitoring worksheet in Attachment A- Pricing Worksheet and Specifications located on the following website: <https://charlottenc.gov/DoingBusiness/Pages/ContractOpportunities.aspx>.

R9B has provided its pricing inputs on Attachment A as requested.



City of Charlotte

MSS Transition Services Plan Appendix A to Required Form 8

Table of Contents

MSS Transition Services Plan..... 3
Transition Deliverables 3
Roles and Responsibilities..... 3
MSS Transition Schedule 6
 Attachment 1: Proposed MSS Transition Schedule..... 6

MSS Transition Services Plan

root9B (R9B) will transition the City of Charlotte’s (the City’s) Managed Security Services (MSS) functions, including the implementation and migration of services from the City’s existing MSS provider. The R9B transition plan includes an initial 90-day period from contract award to activities surrounding the transition of MSS services from the Current Service Provider (CSP) to final R9B go live. The transition plan includes R9B’s, the City’s, CSP’s, and Network Operations Center’s (NOC’s) tasks, timeline schedule of milestones, responsibilities, and estimated transition completion dates and deliverables.

Transition Deliverables

Table 1 provides a list of deliverables for the proposed transition and continuation of services. Report details are provided in the Communications Plan.

Deliverables	Classification (T) = Transition (S) = Continuation of Services
Weekly Progress Report	T
Discovery Phase Report	T
Client Specific Threat Report	T
Monthly Status Report	S
Annual Report	S

Table 1. Contract Deliverables

Roles and Responsibilities

R9B has combined roles and responsibilities in relation to the MSS transition of services into the chart below. The chart details primary and supporting roles and responsibilities for the R9B Service Delivery Lead (SDL), R9B Adversary Pursuit Center (SOC), the City, the CSP, and the NOC. For roles in which the City, the CSP, or the NOC has responsibilities, the last column indicates the level of support required in staff hours over a time span in hours, days, or weeks.

Table 2 delineates the MSS roles and responsibilities.

(P) = Primary role, (S) = Supporting role.

Roles and Responsibilities for Managed Security Services	SDL	SOC	City	CSP	NOC	Hours/Days/Weeks (Estimated)
Pre-Deployment						
Conduct kickoff meeting	P	S	S	S	S	2-3 hours
Develop communications management plan	P					5 days
In-Depth MSS onboarding survey sent to client	P					N/A
Schedule weekly recurring meeting	P	S	S	S	S	1 hour per week
Phase 1 - Security Provisioning						
Survey completed and returned			P	S	S	5 days
Account creation for SOC analyst(s) and engineers			P	S	S	2 days
VPN configured		P	S	S	S	
Appliance(s) built and ready for installation		P	S		S	5 days
Network requirements for appliance sent		P				
Phase 2 - Discovery						
Review of existing security posture		P	S	S	S	14 days
Appliance(s) installed		P	S		S	1 day
Access to configs: endpoints, network devices, appliances, tools (e.g., AV, SIEM)		P	S	S	S	10 days
Begin onboarding data (if applicable)		P			S	5 days
Begin alert creation process		P	S			5 days
Deliver draft discovery report	P	S				
Deliver client-specific threat report	P	S				

Phase 3 - Log Recognition and Normalization						
Begin normalization		P				
Modifications to existing data feeds and forwarders into client SIEM. (If needed)		P			S	5 days
Establishing new data feeds of critical systems identified during discovery (If needed)		P			S	5 days
Modifications to existing firewall rules (If needed)		P			S	10 days
Modifications to existing Group Policy Objects/Preferences (If needed)		P	S		S	10 days
Validate proper transport of logs from in-scope endpoints and network security appliances to client SIEM and ensure data is classified correctly		P				
Perform initial statistical analysis of aggregated logs and begin defining queries specific to client network. Evaluate audit-level settings of in-scope Operating Systems, applications, and services; recommend or make necessary changes		P				
Define and script new SIEM alerts for response to specific events and thresholds and define reporting criteria for each type of alert		P	S		S	10 days
Create and edit dashboards		P	S			5 days
Review and update tags associated with sets of fields and value pairs associated with data		P				
Manage and design data models and data summaries		P				
Map software errors and establish a client-specific baseline		P				

Working in concert with team, finalize the client-specific escalation matrix and alert classification scheme		S	P			1 day
Begin weekly reports for alerts		P				
Phase 4 – Service Framework Exercise						
Initiate and exercise limited monitoring, management, and analysis services (8 hours per day/5 days per week).		P				
Route alerts to R9B APC for further investigation		P			S	30 days
Exercise alert escalation based on agreed client process flow		P			S	30 days
Continue to tune baseline settings to maintain optimal system performance		P				
Sustainment Operations- Go Live						
Begin continuous monitoring		P				

Table 2. Roles and Responsibilities

MSS Transition Schedule

Attached to this Appendix as Attachment 1 is R9B’s complete proposed MSS Transition Schedule which provides detailed tasks with approximate dates of initiation/completion.

Attachment 1: Proposed MSS Transition Schedule

**REQUIRED FORM 9 – CERTIFICATION REGARDING
DEBARMENT, SUSPENSION AND OTHER RESPONSIBILITY
MATTERS**

RFP # 269-2019-109

Managed Security Services

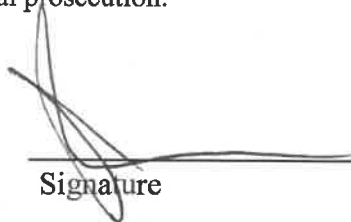
The bidder, contractor, or subcontractor, as appropriate, certifies to the best of its knowledge and belief that neither it nor any of its officers, directors, or managers who will be working under the Contract, or persons or entities holding a greater than 10% equity interest in it (collectively “Principals”):

1. Are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any or state department or agency in the United States;
2. Have within a three-year period preceding this proposal been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state or local) transaction or contract under a public transaction; violation of federal or state anti-trust or procurement statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
3. Are presently indicted for or otherwise criminally or civilly charged by a government entity, (federal, state or local) with commission of any of the offenses enumerated in paragraph 2 of this certification; and
4. Have within a three-year period preceding this application/proposal had one or more public transactions (federal, state or local) terminated for cause or default.

I understand that a false statement on this certification may be grounds for rejection of this proposal or termination of the award or in some instances, criminal prosecution.

I hereby certify as stated above:

John Harbaugh
(Print Name)



Signature

Chief Operating Officer
Title

07/11/19
Date

I am unable to certify to one or more the above statements. Attached is my explanation. [Check box if applicable]

(Print Name)

Signature

Title

Date

REQUIRED FORM 10 – BYRD ANTI-LOBBYING CERTIFICATION

RFP # 269-2019-109

Managed Security Services

The undersigned certifies, to the best of his or her knowledge and belief, that:

1. No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of and Federal contract, grant, loan, or cooperative agreement.
2. If any funds other than federal appropriated funds have been paid or will be paid to any person for making lobbying contacts to an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form—LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions [as amended by "Government wide Guidance for New Restrictions on Lobbying," 61 Fed. Reg. 1413 (1/19/96)].
3. The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including all subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction by 31 U.S.C. § 1352 (as amended by the Lobbying Disclosure Act of 1995). Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

root9B (R9B) (the "Company") certifies or affirms the truthfulness and accuracy of each statement of its certification and disclosure, if any. In addition, the Company understands and agrees that the provisions of 31 U.S.C. A 3801, et seq., apply to this certification and disclosure, if any.

John Harbaugh
(Print Name)

Authorized Signature

07/11/19
Date

root9B, LLC (R9B)
Company Name

90 S. Cascade, Suite 800
Address

Colorado Springs, CO 80903
City/State/Zip

SAMPLE CONTRACT

R9B takes no exceptions to the enclosed sample contract.

As used in this Section of the RFP, the term “Contract” shall refer to the agreement entered into between the City and the Company, and the term “Company” shall refer to the vendor that has been awarded a contract.

**STATE OF NORTH CAROLINA
COUNTY OF MECKLENBURG**

AGREEMENT TO PROVIDE MANAGED SECURITY SERVICES

THIS PROFESSIONAL SERVICES CONTRACT (the “Contract”) is made and entered into as of this _____ day of _____ 201_ (the “Effective Date”), by and between _____, a corporation doing business in North Carolina (the "Company"), and the City of Charlotte, a North Carolina municipal corporation (the "City").

RECITALS

WHEREAS, the City issued a Request For Proposals (RFP # 269-2019-109) for Managed Security Services dated JUNE 13, 2019. This Request for Proposals together with all attachments and addenda, is referred to herein as the “RFP”; and

WHEREAS, the City desires that the Company provide certain Managed Security Services (“Services”), and the Company desires to provide such Services; and

WHEREAS, the City and the Company have negotiated and agreed regarding the above-referenced Services and desire to reduce the terms and conditions of their agreement to this written form.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, and in further consideration of the covenants and representations contained herein, the parties agree as follows:

CONTRACT

1. EXHIBITS. The Exhibits below are hereby incorporated into and made a part of this Contract. With the exception of Exhibit C (Federal Contract Terms and Conditions), any conflict between language in an Exhibit or Appendix to this Contract and the main body of this Contract shall be resolved in favor of the main body of this Contract and any inconsistency between the Exhibits will be resolved in the order in which the Exhibits appear below. Notwithstanding anything contained in this Contract or any Exhibit to the contrary, in the event of a conflict between the language of Exhibit C and the main body of this Contract or any other Exhibit to this Contract, the language of Exhibit C shall prevail. Each reference to **COMPANY NAME** in the Exhibits and Appendices shall be deemed to mean the Company.

EXHIBIT A: PRICE SCHEDULE

EXHIBIT B: SCOPE OF WORK

EXHIBIT C: FEDERAL CONTRACT TERMS AND CONDITIONS

2. DEFINITIONS. This section may include, but not be limited to, terms defined in Section 1 of the RFP.

3. DESCRIPTION OF SERVICES.

3.1. The Company shall be responsible for providing the Services described in Exhibit B attached to this Contract and incorporated herein by reference. Without limiting the foregoing, the Company will perform the Services and meet the requirements as set forth in Exhibit B.

However, the Company shall not be responsible for tasks specifically assigned to the City in this Contract or in Exhibit B.

3.2. [REMOVE FOR PROJECTS WHERE THE COMPANY WILL BE PERFORMING THE WORK ON ITS PREMISES] The Company shall perform the Services on site at the City's facility in Charlotte, North Carolina, except as mutually agreed upon in writing in specific instances by the City. [IF DELETING THIS SUBSECTION, REMOVE THE 3.1 SUB-BULLET NUMBERING]

4. COMPENSATION.

4.1. TOTAL FEES AND CHARGES. [DELETE EITHER MILESTONE OR T&M LANGUAGE] [MILESTONE] The City agrees to pay the Company a fixed price (the "Purchase Price") as full and complete consideration for the satisfactory performance of all the requirements of this Contract. This amount constitutes the maximum total fees and charges payable to the Company under this Contract including Expenses and will not be increased except by a written instrument duly executed by both parties, which expressly states that it amends this Section of the Contract. [T&M] The City agrees to pay the Company on a time and materials basis. The City agrees to pay the Company for the Services at the hourly rates set forth in Exhibit A, which shall remain firm for the duration of the Contract, and shall not exceed a pre-determined amount (the "Payment Cap"). [OPTIONAL LANGUAGE] The Payment Cap constitutes the maximum total fees and charges payable to the Company under this Contract including Expenses and will not be increased except by a written instrument duly executed by both parties.

4.2. EXPENSES or NO EXPENSES CHARGEABLE. [CHOOSE ONE OR DELETE FOR MILESTONE PLAN] IF EXPENSES ALLOWED USE THIS LANGUAGE: As used in this Contract, the term "Expenses" shall mean the following expenses which are actually incurred by employees of the Company or its subcontractors who live outside of a one hundred (100) mile radius of Charlotte, North Carolina and who travel to Charlotte in the performance of the Services, when such travel would not otherwise have been necessary for the performance of this Contract:

- Lodging at a local hotel.
- A per diem meals reimbursement of \$40 per day.
- Long distance calls made by employees of Company while in Charlotte, if a given call is necessary for performance of the Services detailed in this Contract.
- Parking, tolls, or rental car.
- Travel costs to and from the City.

For the Company or subcontractors and employees who stay in Charlotte over extended time periods, the Company will rent an apartment in the City if doing so proves to be more economical on a monthly average. Otherwise, the Company will attempt to obtain accommodations at the same rates as those applicable for federal government employees. The Company will attempt to minimize travel costs by obtaining the lowest fares reasonably practicable under the circumstances.

Each invoice for Expenses shall itemize in detail and provide documentation for all Expenses for which the Company seeks reimbursement. The parties acknowledge that the Expenses apply only to the Services covered by this Contract, and that the Company shall not be permitted to charge the City for Expenses related to services not performed under this Contract. The City shall not be required to pay for Expenses that are not reasonable.

IF EXPENSES NOT ALLOWED USE THIS LANGUAGE: The Company shall not be entitled to charge the City for any travel, mileage, meals, materials or other costs or expenses associated with this Contract.

4.3. EMPLOYMENT TAXES AND EMPLOYEE BENEFITS. The Company represents and warrants that the employees provided by the Company to perform the Services are actual

employees of the Company, and that the Company shall be responsible for providing all salary and other applicable benefits to each Company employee. The Company further represents, warrants and covenants that it will pay all withholding tax, social security, Medicare, unemployment tax, worker's compensation and other payments and deductions that are required by law for each Company employee. The Company agrees that the Company employees are not employees of the City.

- 4.4. INVOICES. Each invoice sent by the Company shall detail all Services performed and delivered which are necessary to entitle the Company to the requested payment under the terms of this Contract. All invoices must include an invoice number and the City purchase order number for purchases made under this Contract. Purchase order numbers will be provided by the City. Invoices must be submitted with lines matching those on the City-provided purchase order.

The Company shall email all invoices to cocap@charlottenc.gov.

- 4.5. DUE DATE OF INVOICES. Payment of invoices shall be due within thirty (30) days after receipt of an accurate, undisputed properly submitted invoice by the City.
- 4.6. PRE-CONTRACT COSTS. The City shall not be charged for any Services or other work performed by the Company prior to the Effective Date of this Contract.
- 4.7. AUDIT. During the term of this Contract and for a period of one (1) year after termination of this Contract, the City shall have the right to audit, either itself or through an independent auditor, all books and records and facilities of the Company necessary to evaluate Company's compliance with the terms and conditions of this Contract or the City's payment obligations. The City shall pay its own expenses, relating to such audits, but shall not have to pay any expenses or additional costs of the Company. However, if non-compliance is found that would have cost the City in excess of \$10,000 but for the audit, then the Company shall be required to reimburse the City for the cost of the audit.

5. **RECORDS.** **[DELETE IF MILESTONE PLAN APPLIES – KEEP FOR T&M]** The Company shall be responsible for keeping a record that accurately states the type of Service performed **and the number of hours worked by the Company [REMOVE IF NOT APPLICABLE]**. The City shall have the right to audit the Company's invoices, expense reports and other documents relating to the Services performed under this Contract, and shall not be required to pay for Services which did not occur, or which occurred in breach of this Contract. The Company shall make such documents available for inspection and copying by the City in Charlotte, North Carolina between the hours of 9:00 a.m. and 5:00 p.m. Monday through Friday, whenever requested by the City.
6. **TIME IS OF THE ESSENCE.** Time is of the essence in having the Company perform all Services and deliver all Deliverables within the time frames provided by this Contract and Exhibit B, including all completion dates, response times and resolution times (the "Completion Dates"). Except as specifically stated in this Contract, there shall be no extensions of the Completion Dates. All references to days in this Contract (including the Exhibits) shall refer to calendar days rather than business days, unless this Contract provides otherwise for a specific situation.
7. **NON-APPROPRIATION OF FUNDS.** If the Charlotte City Council does not appropriate the funding needed by the City to make payments under this Contract for any given fiscal year, the City will not be obligated to pay amounts due beyond the end of the last fiscal year for which funds were appropriated. In such event, the City will promptly notify the Company of the non-appropriation and this Contract will be terminated at the end of the fiscal year for which the funds were appropriated. No act or omission by the City, which is attributable to non-appropriation of funds shall constitute a breach of or default under this Contract.
8. **COMPANY PROJECT MANAGER.** **[ADJUST AS APPLICABLE, especially if you do not have Milestones or defined deliverables – delete mentions of Project if there is no implementation/as appropriate]** The duties of the Company Project Manager include, but are not limited to:

- 8.1. Coordination of Project schedules and the Company's resource assignment based upon the City's requirements and schedule constraints;
 - 8.2. Management of the overall Project by monitoring and reporting on the status of the Project and actual versus projected progress, and by consulting with the City's Project Manager when deviations occur and by documenting all such deviations in accordance with agreed upon change control procedures;
 - 8.3. Provision of consultation and advice to the City on matters related to Project implementation strategies, key decisions and approaches, and Project operational concerns/issues and acting as a conduit to the Company's specialist resources that may be needed to supplement the Company's normal implementation staff;
 - 8.4. Acting as the Company's point of contact for all aspects of contract administration, including invoicing for Services, and status reporting;
 - 8.5. Facilitation of review meetings and conferences between the City and the Company's executives when scheduled or requested by the City;
 - 8.6. Communication among and between the City and the Company's staff;
 - 8.7. Promptly responding to the City Project Manager when consulted in writing or by E-mail with respect to Project deviations and necessary documentation;
 - 8.8. Identifying and providing the City with timely written notice of all issues that may threaten the Company's Services in the manner contemplated by the Contract (with "timely" meaning immediately after the Company becomes aware of them);
 - 8.9. Ensuring that adequate quality assurance procedures are in place throughout the Contract; and
 - 8.10. Meeting with other service providers working on City projects that relate to this effort as necessary to resolve problems and coordinate the Services.
- 9. CITY PROJECT MANAGER.** The duties of the City Project Manager are to (i) ensure that the Company delivers all requirements and specifications in the Contract; (ii) coordinate the City's resource assignment as required to fulfill the City's obligations pursuant to the Contract; (iii) promptly respond to the Company Project Manager when consulted in writing or by E-mail with respect to project issues; and (iv) act as the City's point of contact for all aspects of the Services including contract administration and coordination of communication with the City's staff. The City shall be allowed to change staffing for the City Project Manager position on one (1) business day's notice to the Company.
- 10. PROGRESS REPORTS.** **[REMOVE IF NO PROJECT PLAN OR IMPLEMENTATION]** The Company shall prepare and submit to the City **bi-weekly** (or at such other times as may be agreed in Exhibit B) written progress reports, which accomplish each of the following:
- 10.1. Update the project schedule set forth in Exhibit B, indicating progress for each task and Deliverable.
 - 10.2. Identify all information, personnel, equipment, facilities and resources of the City that will be required for the Company to perform the Services for the subsequent month.
 - 10.3. Identify and report the status of all tasks and Deliverables that have fallen behind schedule.
 - 10.4. Identify and summarize all risks and problems identified by the Company, which may affect the performance of the Services.
 - 10.5. For each risk and problem, identify the action and person(s) responsible for mitigating the risk and resolving the problem.
 - 10.6. For each risk and problem identified, state the impact on the project schedule.
- 11. DUTY OF COMPANY TO IDENTIFY AND REQUEST INFORMATION, PERSONNEL AND FACILITIES.** The Company shall identify and request in writing from the City in a timely manner:

(i) all information reasonably required by the Company to perform each task comprising the Services, (ii) the City's personnel whose presence or assistance reasonably may be required by the Company to perform each task comprising the Services, and (iii) any other equipment, facility or resource reasonably required by the Company to perform the Services. Notwithstanding the foregoing, the Company shall not be entitled to request that the City provide information, personnel or facilities other than those that Exhibit B specifically requires the City to provide, unless the City can do so at no significant cost. The Company shall not be relieved of any failure to perform under this Contract by virtue of the City's failure to provide any information, personnel, equipment, facilities or resources: (i) that the Company failed to identify and request in writing from the City pursuant to this Section; or (ii) that the City is not required to provide pursuant to this Contract. In the event the City fails to provide any information, personnel, facility or resource that it is required to provide under this Section, the Company shall notify the City in writing immediately in accordance with the notice provision of this Contract. Failure to do so shall constitute a waiver by Company of any claim or defense it may otherwise have based on the City's failure to provide such information, personnel, facility or resource.

12. COMPANY PERSONNEL REMOVAL, REPLACEMENT, PROMOTION, ETC.

The City will have the right to require the removal and replacement of any personnel of the Company or the Company's subcontractors who are assigned to provide Services to the City based on experience, qualifications, performance, conduct, compatibility, and violation of City policy or any other reasonable grounds. The addition or promotion of any personnel to key positions within the Project must be approved by the City in writing. The Company will replace any personnel that leave the Project, **including but not limited to Key Personnel**, with persons having at least equivalent qualifications who are approved by the City in writing. As used in this Contract, the "personnel" includes all staff provided by the Company or its subcontractors, **including but not limited to Key Personnel**.

13. BACKGROUND CHECKS.

Prior to starting work under this Contract, the Company is required to conduct a background check on each Company employee assigned to work under this Contract, and shall require its subcontractors (if any) to perform a background check on each of their employees assigned to work under this Contract (collectively, the "Background Checks"). Each Background Check must include: (i) the person's criminal conviction record from the states and counties where the person lives or has lived in the past seven (7) years; and (ii) a reference check.

After starting work under this Contract, the Company is required to perform a Background Check for each new Company employee assigned to work under this Contract during that year, and shall require its subcontractors (if any) to do the same for each of their employees. If the Company undertakes a new project under this Contract, then prior to commencing performance of the project the Company shall perform a Background Check for each Company employee assigned to work on the project, and shall require its subcontractors (if any) to do the same for each of their employees.

If a person's duties under this Contract fall within the categories described below, the Background Checks that the Company will be required to perform (and to have its subcontractors perform) shall also include the following additional investigation:

- **[ADJUST HERE AS NECESSARY] If the job duties require driving: A motor vehicle records check.**
- **If the job duties include responsibility for initiating or affecting financial transactions: A credit history check.**

The Company must follow all State and Federal laws when conducting Background Checks, including but not limited to the Fair Credit Reporting Act requirements, and shall require its subcontractors to do the same.

The Company shall notify the City of any information discovered in the Background Checks that may be of potential concern for any reason.

The City may conduct its own background checks on principals of the Company as the City deems appropriate. By operation of the public records law, background checks conducted by the City are subject to public review upon request.

- 14. ACCEPTANCE OF TASKS AND DELIVERABLES.** Within a reasonable time after a particular Deliverable has been completed (or such specific time as may be set forth in Exhibit B), the Company shall submit a written notice to the City's Project Manager stating the Deliverable(s) that have been met. This notice shall include a signature page for sign-off by the City Project Manager indicating acceptance of such Deliverable(s).

If the City Project Manager is not satisfied that the Deliverable(s) has been met, a notice of rejection (a "Rejection Notice") shall be submitted to the Company by the City Project Manager that specifies the nature and scope of the deficiencies that the City wants corrected. Upon receipt of a Rejection Notice, the Company shall: (i) act diligently and promptly to correct all deficiencies identified in the Rejection Notice, and (ii) immediately upon completing such corrections give the City a written, dated certification that all deficiencies have been corrected (the "Certification"). In the event the Company fails to correct all deficiencies identified in the Rejection Notice and provide a Certification within thirty (30) days after receipt of the Rejection Notice, the City shall be entitled to terminate this Contract for default without further obligation to the Company and without obligation to pay for the defective work.

Upon receipt of the corrected Deliverable(s), or a Certification, whichever is later, the above-described Acceptance procedure shall recommence. The City shall not be obligated to allow the Company to recommence curative action with respect to any deficiency previously identified in a Rejection Notice, or more than once for any given Deliverable (and shall be entitled to terminate this Contract for default if the Company does not meet this time frame).

- 15. NON-EXCLUSIVITY.** The Company acknowledges that it is one of several providers of Professional Services to the City and the City does not represent that it is obligated to contract with the Company for any particular project.

- 16. EACH PARTY TO BEAR ITS OWN NEGOTIATION COSTS.** Each party shall bear its own cost of negotiating this Contract and developing the exhibits. The City shall not be charged for any Services or other work performed by the Company prior to the Effective Date.

17. REPRESENTATIONS AND WARRANTIES OF COMPANY.

17.1. GENERAL WARRANTIES.

- 17.1.1. The Services shall satisfy all requirements set forth in this Contract, including but not limited to the attached Exhibits;
- 17.1.2. The Company has taken and will continue to take sufficient precautions to ensure that it will not be prevented from performing all or part of its obligations under this Contract by virtue of interruptions in the computer systems used by the Company;
- 17.1.3. All Services performed by the Company and/or its subcontractors pursuant to this Contract shall meet the highest industry standards and shall be performed in a professional and workmanlike manner by staff with the necessary skills, experience and knowledge;
- 17.1.4. Neither the Services nor any Deliverables provided by the Company under this Contract will infringe or misappropriate any patent, copyright, trademark or trade secret rights of any third party;
- 17.1.5. The Company and each Company employee provided by the Company to the City shall have the qualifications, skills and experience necessary to perform the Services described or referenced in Exhibit B;
- 17.1.6. All information provided by the Company about each Company employee is accurate; and

- 17.1.7. Each Company employee is an employee of the Company, and the Company shall make all payments and withholdings required for by law for the Company for such employees.
- 17.2. ADDITIONAL WARRANTIES. The Company further represents and warrants that:
- 17.2.1. It is a legal entity and if incorporated, duly incorporated, validly existing and in good standing under the laws of the state of its incorporation or licensing and is qualified to do business in North Carolina;
- 17.2.2. It has all the requisite corporate power and authority to execute, deliver and perform its obligations under this Contract;
- 17.2.3. The execution, delivery, and performance of this Contract have been duly authorized by the Company;
- 17.2.4. No approval, authorization or consent of any governmental or regulatory authority is required to be obtained or made by it in order for it to enter into and perform its obligations under this Contract;
- 17.2.5. In connection with its obligations under this Contract, it shall comply with all applicable federal, state and local laws and regulations and shall obtain all applicable permits and licenses; and
- 17.2.6. The performance of this Contract by the Company and each Company employee provided by the Company will not violate any contracts or agreements with third parties or any third party rights (including but not limited to non-compete agreements, non-disclosure agreements, patents, trademarks or intellectual property rights).

18. OTHER OBLIGATIONS OF THE COMPANY.

- 18.1. WORK ON CITY'S PREMISES. The Company and all its employees will, whenever on the City's premises, obey all instructions and City policies that are provided with respect to performing Services on the City's premises.
- 18.2. RESPECTFUL AND COURTEOUS BEHAVIOR. The Company shall assure that its employees interact with City employees and the public in a courteous, helpful and impartial manner. All employees of the Company in both field and office shall refrain from belligerent behavior and/or profanity. Correction of any such behavior and language shall be the responsibility of the Company.
- 18.3. REPAIR OR REPLACEMENT OF DAMAGED EQUIPMENT OR FACILITIES. In the event that the Company causes damage to the City's equipment or facilities, the Company shall, at its own expense, promptly repair or replace such damaged items to restore them to the same level of functionality that they possessed prior to the Company's action.
- 18.4. REGENERATION OF LOST OR DAMAGED DATA. With respect to any data that the Company or any Company employees have negligently lost or negligently damaged, the Company shall, at its own expense, promptly replace or regenerate such data from the City's machine-readable supporting material, or obtain, at the Company's own expense, a new machine-readable copy of lost or damaged data from the City's data sources.
- 18.5. NC E-VERIFY REQUIREMENT. The Company shall comply with the requirements of Article 2 of Chapter 64 of the North Carolina General Statutes, and shall require each of its subcontractors to do so as well.
- 18.6. NC PROHIBITION ON CONTRACTS WITH COMPANIES THAT INVEST IN IRAN OR BOYCOTT ISRAEL. Company certifies that: (i) it is not identified on the Final Divestment List or any other list of prohibited investments created by the NC State Treasurer pursuant to N.C.G.S. 147-86.58 (collectively, the "Treasurer's IDA List"); (ii) it has not been designated by the NC State Treasurer pursuant to N.C.G.S. 147-86.81 as a company engaged in the boycott

of Israel (such designation being referred to as the “Treasurer’s IB List”); and (iii) it will not take any action causing it to appear on the Treasurer’s IDA List or the Treasurer’s IB List during the term of this Contract. In signing this Contract Company further agrees, as an independent obligation, separate and apart from this Contract, to reimburse the City for any and all damages, costs and attorneys’ fees incurred by the City in connection with any claim that this Contract or any part thereof is void due to Company appearing on the Treasurer’s IDA List or the Treasurer’s IB List at any time before or during the term of this Contract.

19. REMEDIES.

- 19.1. **RIGHT TO COVER.** If the Company fails to meet any completion date or resolution time set forth in this Contract (including the Exhibits) or the Project Plan, the City may take any of the following actions with or without terminating this Contract, and in addition to and without limiting any other remedies it may have:
 - a. Employ such means as it may deem advisable and appropriate to perform itself or obtain the Services from a third party until the matter is resolved and the Company is again able to resume performance under this Contract; and
 - b. Deduct any and all expenses incurred by the City in obtaining or performing the Services from any money then due or to become due the Company and, should the City’s cost of obtaining or performing the services exceed the amount due the Company, collect the amount due from the Company.
- 19.2. **RIGHT TO WITHHOLD PAYMENT.** If the Company breaches any provision of this Contract, the City shall have a right to withhold all payments due to the Company until such breach has been fully cured.
- 19.3. **SPECIFIC PERFORMANCE AND INJUNCTIVE RELIEF.** The Company agrees that monetary damages are not an adequate remedy for the Company’s failure to provide the Services or Deliverables as required by this Contract, nor could monetary damages be the equivalent of the performance of such obligation. Accordingly, the Company hereby consents to an order granting specific performance of such obligations of the Company in a court of competent jurisdiction within the State of North Carolina. The Company further consents to the City obtaining injunctive relief (including a temporary restraining order) to assure performance in the event the Company breaches this Contract.
- 19.4. **SETOFF.** Each party shall be entitled to setoff and deduct from any amounts owed to the other party pursuant to this Contract all damages and expenses incurred or reasonably anticipated as a result of the other party’s breach of this Contract.
- 19.5. **OTHER REMEDIES.** Upon breach of this Contract, each party may seek all legal and equitable remedies to which it is entitled. The remedies set forth herein shall be deemed cumulative and not exclusive and may be exercised successively or concurrently, in addition to any other available remedy.

20. TERM AND TERMINATION OF CONTRACT.

- 20.1. **TERM.** This Contract shall commence on the Effective Date and shall continue in effect for Three (3) years with the City having the unilateral right to renew for Renewal Term (#) consecutive one (1) year terms.
- 20.2. **TERMINATION FOR CONVENIENCE.** The City may terminate this Contract at any time without cause by giving thirty (30) days prior written notice to the Company. As soon as practicable after receipt of a written notice of termination without cause, the Company shall submit a statement to the City showing in detail the Services performed under this Contract through the date of termination. The foregoing payment obligation is contingent upon: (i) the Company having fully complied with Section 20.8; and (ii) the Company having provided the City with written documentation reasonably adequate to verify the number of hours of Services rendered through the termination date and the percentage of completion of each task.

- 20.3. **TERMINATION FOR DEFAULT BY EITHER PARTY.** By giving written notice to the other party, either party may terminate this Contract upon the occurrence of one or more of the following events:
- a. The other party violates or fails to perform any covenant, provision, obligation, term or condition contained in this Contract, provided that, unless otherwise stated in this Contract, such failure or violation shall not be cause for termination if both of the following conditions are satisfied: (i) such default is reasonably susceptible to cure; and (ii) the other party cures such default within thirty (30) days of receipt of written notice of default from the non-defaulting party; or
 - b. The other party attempts to assign, terminate or cancel this Contract contrary to the terms hereof; or
 - c. The other party ceases to do business as a going concern, makes an assignment for the benefit of creditors, admits in writing its inability to pay debts as they become due, files a petition in bankruptcy or has an involuntary bankruptcy petition filed against it (except in connection with a reorganization under which the business of such party is continued and performance of all its obligations under the Contract shall continue), or if a receiver, trustee or liquidator is appointed for it or any substantial part of other party's assets or properties.

Any notice of default shall identify this Section of this Contract and shall state the party's intent to terminate this Contract if the default is not cured within the specified period.

Notwithstanding anything contained herein to the contrary, upon termination of this Contract by the Company for default, the Company shall continue to perform the Services required by this Contract for the lesser of: (i) six (6) months after the date the City receives the Company's written termination notice; or (ii) the date on which the City completes its transition to a new service provider.

- 20.4. **ADDITIONAL GROUNDS FOR DEFAULT TERMINATION BY THE CITY.** By giving written notice to the Company, the City may also terminate this Contract upon the occurrence of one or more of the following events (which shall each constitute separate grounds for termination without a cure period and without the occurrence of any of the other events of default previously listed):
- a. Failure of the Company to complete a particular task by the completion date set forth in this Contract;
 - b. The Company makes or allows to be made any material written misrepresentation or provides any materially misleading written information in connection with this Contract, the Company's Proposal, or any covenant, agreement, obligation, term or condition contained in this Contract; or
 - c. The Company takes or fails to take any action which constitutes grounds for immediate termination under the terms of this Contract, including but not limited to failure to obtain or maintain the insurance policies and endorsements as required by this Contract, or failure to provide the proof of insurance as required by this Contract.
- 20.5. **NO SUSPENSION.** In the event that the City disputes in good faith an allegation of default by the Company, notwithstanding anything to the contrary in this Contract, the Company agrees that it will not terminate this Contract or suspend or limit the Services or any warranties or repossess, disable or render unusable any software supplied by the Company, unless (i) the parties agree in writing, or (ii) an order of a court of competent jurisdiction determines otherwise.
- 20.6. **CANCELLATION OF ORDERS AND SUBCONTRACTS.** In the event this Contract is terminated by the City for any reason prior to the end of the term, the Company shall, upon termination, immediately discontinue all service in connection with this Contract and promptly

- cancel all existing orders and subcontracts, which are chargeable to this Contract. As soon as practicable after receipt of notice of termination, the Company shall submit a statement to the City showing in detail the Services performed under this Contract to the date of termination.
- 20.7. **AUTHORITY TO TERMINATE.** The following persons are authorized to terminate this Contract on behalf of the City: (i) the City Manager, any Assistant City Manager, or any designee of the City Manager; or (ii) the Department Director of the City Department responsible for administering this Contract.
- 20.8. **OBLIGATIONS UPON EXPIRATION OR TERMINATION.** Upon expiration or termination of this Contract, the Company shall promptly return to the City (i) all computer programs, files, documentation, media, related material and any other material and equipment that are owned by the City; (ii) all Deliverables that have been completed or that are in process as of the date of termination; and (iii) a written statement describing in detail all work performed with respect to Deliverables which are in process as of the date of termination. The expiration or termination of this Contract shall not relieve either party of its obligations regarding “Confidential Information,” as defined in this Contract.
- 20.9. **NO EFFECT ON TAXES, FEES, CHARGES OR REPORTS.** Any termination of this Contract shall not relieve the Company of the obligation to pay any fees, taxes or other charges then due to the City, nor relieve the Company of the obligation to file any daily, monthly, quarterly or annual reports covering the period to termination nor relieve the Company from any claim for damages previously accrued or then accruing against the Company.
- 20.10. **OTHER REMEDIES.** The remedies set forth in this Section and **Section 19** shall be deemed cumulative and not exclusive, and may be exercised successively or concurrently, in addition to any other remedies available under this Contract or at law or in equity.
- 21. TRANSITION SERVICES UPON TERMINATION.** Upon termination or expiration of this Contract, the Company shall cooperate with the City to assist with the orderly transfer of the Services provided by the Company to the City. Prior to termination or expiration of this Contract, the City may require the Company to perform and, if so required, the Company shall perform certain transition services necessary to shift the Services of the Company to another provider or to the City itself as described below (the “Transition Services”). Transition Services may include but shall not be limited to the following:
- Working with the City to jointly develop a mutually agreed upon Transition Services Plan to facilitate the termination of the Services;
 - Notifying all affected service providers and subcontractors of the Company;
 - Performing the Transition Services;
 - Answering questions regarding the Services on an as-needed basis; and
 - Providing such other reasonable services needed to effectuate an orderly transition to a new service provider.
- 22. CHANGES.** In the event changes to the Services (collectively “Changes”), become necessary or desirable to the parties, the parties shall follow the procedures set forth in this Section. A Change shall be effective only when documented by a written, dated agreement executed by both parties that expressly references and is attached to this Contract (a “Change Statement”). The Change Statement shall set forth in detail: (i) the Change requested, including all modifications of the duties of the parties; (ii) the reason for the proposed Change; and (iii) a detailed analysis of the impact of the Change on the results of the Services and time for completion of the Services, including the impact on all Milestones and delivery dates and any associated price.

In the event either party desires a Change, the Project Manager for such party shall submit to the other party’s Project Manager a proposed Change Statement. If the receiving party does not accept the

Change Statement in writing within ten (10) days, the receiving party shall be deemed to have rejected the Change Statement. If the parties cannot reach agreement on a proposed Change, the Company shall nevertheless continue to render performance under this Contract in accordance with its (unchanged) terms and conditions.

Changes that involve or increase in the amounts payable by the City may require execution by the City Manager or a designee depending on the amount. Some increases may also require approval by Charlotte City Council.

23. CITY OWNERSHIP OF WORK PRODUCT.

- 23.1. The parties agree that the City shall have exclusive ownership of all reports, documents, designs, ideas, materials, reports, concepts, plans, creative works, and other work product developed for or provided to the City in connection with this Contract, and all patent rights, copyrights, trade secret rights and other intellectual property rights relating thereto (collectively the “Intellectual Property”). The Company hereby assigns and transfers all rights in the Intellectual Property to the City. The Company further agrees to execute and deliver such assignments and other documents as the City may later require to perfect, maintain and enforce the City’s rights as sole owner of the Intellectual Property, including all rights under patent and copyright law. The Company hereby appoints the City as attorney in fact to execute all such assignments and instruments and agree that its appointment of the City as an attorney in fact is coupled with an interest and is irrevocable.
- 23.2. The City grants the Company a royalty-free, non-exclusive license to use and copy the Intellectual Property to the extent necessary to perform this Contract. The Company shall not be entitled to use the Intellectual Property for other purposes without the City’s prior written consent, and shall treat the Intellectual Property as “Confidential Information” pursuant to **Section 27** of the Contract.
- 23.3. The Company will treat as Confidential Information under the Confidentiality and Non-Disclosure Contract all data in connection with the Contract. City data processed by the Company shall remain the exclusive property of the City. The Company will not reproduce, copy, duplicate, disclose, or in any way treat the data supplied by the City in any manner except that contemplated by the Contract.

24. RELATIONSHIP OF THE PARTIES. The relationship of the parties established by this Contract is solely that of independent contractors, and nothing contained in this Contract shall be construed to (i) give any party the power to direct or control the day-to-day administrative activities of the other; or (ii) constitute such parties as partners, joint venturers, co-owners or otherwise as participants in a joint or common undertaking; or (iii) make either party an agent of the other, or any Company employee an agent or employee of the City, for any purpose whatsoever. Neither party nor its agents or employees is the representative of the other for any purpose, and neither has power or authority to act as agent or employee to represent, to act for, bind, or otherwise create or assume any obligation on behalf of the other.

25. INDEMNIFICATION. To the fullest extent permitted by law, the Company shall indemnify, defend and hold harmless each of the “Indemnitees” (as defined below) from and against any and all “Charges” (as defined below) paid or incurred as a result of any claims, demands, lawsuits, actions, or proceedings: (i) alleging violation, misappropriation or infringement of any copyright, trademark, patent, trade secret or other proprietary rights with respect to the Services or any products or deliverables provided to the City pursuant to this Contract (“Infringement Claims”); (ii) seeking payment for labor or materials purchased or supplied by the Company or its subcontractors in connection with this Contract; (iii) arising from the Company’s failure to perform its obligations under this Contract, or from any act of negligence or willful misconduct by the Company or any of its agents, employees or subcontractors relating to this Contract, including but not limited to any liability caused by an accident or other occurrence resulting in bodily injury, death, sickness or disease to any person(s) or damage or destruction to any property, real or personal, tangible or intangible; or (iv) arising from any claim that the Company or an employee or subcontractor of the Company is an employee of the City, including

but not limited to claims relating to worker's compensation, failure to withhold taxes and the like. For purposes of this Section: (i) the term "Indemnitees" means the City, any federal agency that funds all or part of this Contract, and each of the City's and such federal agency's officers, officials, employees, agents and independent contractors (excluding the Company); and (ii) the term "Charges" means any and all losses, damages, costs, expenses (including reasonable attorneys' fees), obligations, duties, fines, penalties, royalties, interest charges and other liabilities (including settlement amounts).

If an Infringement Claim occurs, the Company shall either: (i) procure for the City the right to continue using the affected product or service; or (ii) repair or replace the infringing product or service so that it becomes non-infringing, provided that the performance of the overall product(s) and service(s) provided to the City shall not be adversely affected by such replacement or modification. If the Company is unable to comply with the preceding sentence within thirty (30) days after the City is directed to cease use of a product or service, the Company shall promptly refund to the City all amounts paid under this Contract.

This **Section 25** shall remain in force despite termination of this Contract (whether by expiration of the term or otherwise).

26. SUBCONTRACTING. Should the Company choose to subcontract, the Company shall be the prime contractor and shall remain fully responsible for performance of all obligations that it is required to perform under the Contract. Any subcontract entered into by Company shall name the City as a third party beneficiary.

27. CONFIDENTIAL INFORMATION.

27.1. CONFIDENTIAL INFORMATION. Confidential Information includes any information, not generally known in the relevant trade or industry, obtained from the City or its vendors or licensors or which falls within any of the following general categories:

27.1.1. *Trade secrets.* For purposes of this Contract, trade secrets consist of *information* of the City or any of its suppliers, contractors or licensors: (a) that derives value from being secret; and (b) that the owner has taken reasonable steps to keep confidential. Examples of trade secrets include information relating to proprietary software, new technology, new products or services, flow charts or diagrams that show how things work, manuals that tell how things work and business processes and procedures.

27.1.2. *Information of the City or its suppliers, contractors or licensors marked "Confidential" or "Proprietary."*

27.1.3. *Information relating to criminal investigations conducted by the City, and records of criminal intelligence information compiled by the City.*

27.1.4. *Information contained in the City's personnel files, as defined by N.C. Gen. Stat. 160A-168.* This consists of all information gathered and/or maintained by the City about employees, except for that information which is a matter of public record under North Carolina law.

27.1.5. *Citizen or employee social security numbers collected by the City.*

27.1.6. *Computer security information of the City,* including all security features of electronic data processing, or information technology systems, telecommunications networks and electronic security systems. This encompasses but is not limited to passwords and security standards, procedures, processes, configurations, software and codes.

27.1.7. *Local tax records of the City that contains information about a taxpayer's income or receipts.*

27.1.8. *Any attorney / City privileged information disclosed by either party.*

27.1.9. *Any data collected from a person applying for financial or other types of assistance, including but not limited to their income, bank accounts, savings accounts, etc.*

- 27.1.10. *The name or address of individual homeowners who, based on their income, have received a rehabilitation grant to repair their home.*
- 27.1.11. *Building plans of city-owned buildings or structures, as well as any detailed security plans.*
- 27.1.12. *Billing information of customers compiled and maintained in connection with the City providing utility services.*
- 27.1.13. *Other information that is exempt from disclosure under the North Carolina public records laws.*

Categories stated in Sections 27.1.3 through 27.1.13 above constitute “Highly Restricted Information,” as well as Confidential Information. The Company acknowledges that certain Highly Restricted Information is subject to legal restrictions beyond those imposed by this Contract, and agrees that: (i) all provisions in this Contract applicable to Confidential Information shall apply to Highly Restricted Information; and (ii) the Company will also comply with any more restrictive instructions or written policies that may be provided by the City from time to time to protect the confidentiality of Highly Restricted Information.

The parties acknowledge that in addition to information disclosed or revealed after the date of this Contract, the Confidential Information shall include information disclosed or revealed within one (1) year prior to the date of this Contract.

27.2. **RESTRICTIONS.** The Company shall keep the Confidential Information in the strictest confidence, in the manner set forth below:

- 27.2.1. It shall not copy, modify, enhance, compile or assemble (or reverse compile or disassemble), or reverse engineer Confidential Information.
- 27.2.2. It shall not, directly or indirectly, disclose, divulge, reveal, report or transfer Confidential Information of the other to any third party or to any individual employed by the Company, other than an employee, agent, subcontractor or vendor of the City or Company who: (i) has a need to know such Confidential Information, and (ii) has executed a confidentiality agreement incorporating substantially the form of this Section of the Contract and containing all protections set forth herein.
- 27.2.3. It shall not use any Confidential Information of the City for its own benefit or for the benefit of a third party, except to the extent such use is authorized by this Contract or other written agreements between the parties hereto, or is for the purpose for which such Confidential Information is being disclosed.
- 27.2.4. It shall not remove any proprietary legends or notices, including copyright notices, appearing on or in the Confidential Information of the other.
- 27.2.5. The Company shall use its best efforts to enforce the proprietary rights of the City and the City’s vendors, licensors and suppliers (including but not limited to seeking injunctive relief where reasonably necessary) against any person who has possession of or discloses Confidential Information in a manner not permitted by this Contract.
- 27.2.6. In the event that any demand is made in litigation, arbitration or any other proceeding for disclosure of Confidential Information, the Company shall assert this Contract as a ground for refusing the demand and, if necessary, shall seek a protective order or other appropriate relief to prevent or restrict and protect any disclosure of Confidential Information.
- 27.2.7. All materials which constitute, reveal or derive from Confidential Information shall be kept confidential to the extent disclosure of such materials would reveal Confidential Information, and unless otherwise agreed, all such materials shall be returned to the City or destroyed upon satisfaction of the purpose of the disclosure of such information.

27.3. **EXCEPTIONS.** The parties agree that the Company shall have no obligation with respect to any Confidential Information which the Company can establish:

- 27.3.1. Was already known to the Company prior to being disclosed by the disclosing party;

- 27.3.2. Was or becomes publicly known through no wrongful act of the Company;
 - 27.3.3. Was rightfully obtained by the Company from a third party without similar restriction and without breach hereof;
 - 27.3.4. Was used or disclosed by the Company with the prior written authorization of the City;
 - 27.3.5. Was disclosed pursuant to the requirement or request of a governmental agency, which disclosure cannot be made in confidence, provided that, in such instance, the Company shall first give to the City notice of such requirement or request;
 - 27.3.6. Was disclosed pursuant to the order of a court of competent jurisdiction or a lawfully issued subpoena, provided that the Company shall take use its best efforts to obtain an agreement or protective order providing that, to the greatest possible extent possible, this Contract will be applicable to all disclosures under the court order or subpoena.
- 27.4. UNINTENTIONAL DISCLOSURE. Notwithstanding anything contained herein in to the contrary, in the event that the Company is unintentionally exposed to any Confidential Information of the City, the Company agrees that it shall not, directly or indirectly, disclose, divulge, reveal, report or transfer such Confidential Information to any person or entity or use such Confidential Information for any purpose whatsoever.
- 27.5. REMEDIES. The Company acknowledges that the unauthorized disclosure of the Confidential Information of the City will diminish the value of the proprietary interests therein. Accordingly, it is agreed that if the Company breaches its obligations hereunder, the City shall be entitled to equitable relief to protect its interests, including but not limited to injunctive relief, as well as monetary damages.

28. INSURANCE.

- 28.1. TYPES OF INSURANCE. The Company shall obtain and maintain during the life of this Contract, with an insurance company rated not less than "A" by A.M. Best, authorized to do business in the State of North Carolina, acceptable to the Charlotte-Mecklenburg, Risk Management Division the following insurance:
- 28.1.1. Automobile Liability - Bodily injury and property damage liability covering all owned, non-owned and hired automobiles for limits of not less than \$1,000,000 bodily injury each person, each accident and \$1,000,000 property damage, or \$1,000,000 combined single limit - bodily injury and property damage.
 - 28.1.2. Commercial General Liability - Bodily injury and property damage liability as shall protect the Company and any subcontractor performing Services under this Contract, from claims of bodily injury or property damage which arise from performance of this Contract, whether such operations are performed by the Company, any subcontractor, or anyone directly or indirectly employed by either. The amounts of such insurance shall not be less than \$1,000,000 bodily injury each occurrence/aggregate and \$1,000,000 property damage each occurrence/aggregate, or \$1,000,000 bodily injury and property damage combined single limits each occurrence/aggregate. This insurance shall include coverage for products, operations, personal and advertising injury, and contractual liability, assumed under the indemnity provision of this Contract.
 - 28.1.3. Workers' Compensation and Employers Liability - meeting the statutory requirements of the State of North Carolina, \$100,000 per accident limit, \$500,000 disease per policy limit, \$100,000 disease each employee limit.
 - 28.1.4. Technology Errors & Omissions - Insurance with a limit of not less than \$1,000,000 per claim, \$1,000,000 aggregate as shall protect the contractor and the contractor's employees for negligent acts, errors or omissions in performing the professional services under this contract.

The Company shall not commence any Services in connection with this Contract until it has obtained all of the foregoing types of insurance and such insurance has been approved by the City. The Company shall not allow any subcontractor to commence Services on its subcontract until all similar insurance required of the subcontractor has been obtained and approved.

28.2. OTHER INSURANCE REQUIREMENTS.

28.2.1. The City shall be exempt from, and in no way liable for any sums of money, which may represent a deductible in any insurance policy. The payment of such deductible shall be the sole responsibility of the Company and/or subcontractor providing such insurance.

28.2.2. The City of Charlotte shall be named as an additional insured for operations or services rendered under the general liability coverage. The Company's insurance shall be primary of any self-funding and/or insurance otherwise carried by the City for all loss or damages arising from the Company's operations under this agreement.

28.2.3. Certificates of such insurance will be furnished to the City and shall contain the provision that the City be given thirty (30) days' written notice of any intent to amend coverage reductions or material changes or terminate by either the insured or the insuring Company.

28.2.4. Should any or all of the required insurance coverage be self-funded/self-insured, a copy of the Certificate of Self-Insurance or other documentation from the North Carolina Department of Insurance shall be furnished to the City.

28.2.5. If any part of the Services under this Contract is sublet, the subcontractor shall be required to meet all insurance requirements as listed above. However, this will in no way relieve the Company from meeting all insurance requirements or otherwise being responsible for the subcontractor.

29. COMMERCIAL NON-DISCRIMINATION. As a condition of entering into this Contract, the Company represents and warrants that it will fully comply with the City's Commercial Non-Discrimination Policy, as described in Section 2, Article V of the Charlotte City Code, and consents to be bound by the award of any arbitration conducted thereunder. As part of such compliance, the Company shall not discriminate on the basis of race, gender, religion, national origin, ethnicity, age or disability in the solicitation, selection, hiring, or treatment of subcontractors, vendors or suppliers in connection with a City contract or contract solicitation process, nor shall the Company retaliate against any person or entity for reporting instances of such discrimination. The Company shall provide equal opportunity for subcontractors, vendors and suppliers to participate in all of its subcontracting and supply opportunities on City contracts, provided that nothing contained in this clause shall prohibit or limit otherwise lawful efforts to remedy the effects of marketplace discrimination that has occurred or is occurring in the marketplace. The Company understands and agrees that a violation of this clause shall be considered a material breach of this Contract and may result in termination of this Contract, disqualification of the Company from participating in City contracts or other sanctions.

As a condition of entering into this Contract, the Company agrees to: (i) promptly provide to the City in a format specified by the City all information and documentation that may be requested by the City from time to time regarding the solicitation, selection, treatment and payment of subcontractors in connection with this Contract; and (ii) if requested, provide to the City within sixty days after the request a truthful and complete list of the names of all subcontractors, vendors, and suppliers that the Company has used on City contracts in the past five years, including the total dollar amount paid by the Company on each subcontract or supply contract. The Company further agrees to fully cooperate in any investigation conducted by the City pursuant to the City's Non-Discrimination Policy, to provide any documents relevant to such investigation that are requested by the City, and to be bound by the award of any arbitration conducted under such Policy.

The Company agrees to provide to the City from time to time on the City's request, payment affidavits detailing the amounts paid by the Company to subcontractors and suppliers in connection with this

Contract within a certain period of time. Such affidavits shall be in the format specified by the City from time to time.

The Company understands and agrees that violation of this Commercial Non-Discrimination provision shall be considered a material breach of this Contract and may result in contract termination, disqualification of the Company from participating in City contracts and other sanctions.

- 23. NOTICES.** Any notice, consent or other communication required or contemplated by this Contract shall be in writing, and shall be delivered in person, by U.S. mail, by overnight courier, by electronic mail or by telefax to the intended recipient at the address set forth below. Notice shall be effective upon the date of receipt by the intended recipient; provided that any notice which is sent by telefax or electronic mail shall also be simultaneously sent by mail deposited with the U.S. Postal Service or by overnight courier. Each party may change its address for notification purposes by giving the other party written notice of the new address and the date upon which it shall become effective.

Communications that relate to any breach, default, termination, delay in performance, prevention of performance, modification, extension, amendment, or waiver of any provision of this Contract shall be sent to:

For the Company:	For the City:
	Kay Elmore
	City of Charlotte
	City Procurement
	600 East Fourth Street, 9 th Floor
	Charlotte, NC 28202
Phone:	Phone: 704-336-2524
Fax:	Fax: 704-632-8252
E-mail:	E-mail: kelmore@charlottenc.gov

With Copy To:	With Copy To:
	Adam Jones
	City of Charlotte
	City Attorney's Office
	600 East Fourth Street, 15 th Floor
	Charlotte, NC 28202
Phone:	Phone: 704-336-3012
E-mail:	E-mail: amiones@charlottenc.gov

All other notices shall be sent to the other party's Project Manager at the most recent address provided in writing by the other party.

31. MISCELLANEOUS.

- 31.1. **ENTIRE AGREEMENT.** This Contract is the entire agreement between the parties with respect to its subject matter, and there are no other representations, understandings, or agreements between the parties with respect to such subject matter. This Contract supersedes all prior agreements, negotiations, representations and proposals, written or oral.
- 31.2. **AMENDMENT.** No amendment or change to this Contract shall be valid unless in writing and signed by both parties to this Contract.
- 31.3. **GOVERNING LAW AND JURISDICTION.** The parties acknowledge that this Contract is made and entered into in Charlotte, North Carolina, and will be performed in Charlotte, North Carolina. The parties further acknowledge and agree that North Carolina law shall govern all the rights, obligations, duties and liabilities of the parties under this Contract, and that North Carolina law shall govern interpretation and enforcement of this Contract and any other matters

- relating to this Contract (all without regard to North Carolina conflicts of law principles). The parties further agree that any and all legal actions or proceedings relating to this Contract shall be brought in a state or federal court sitting in Mecklenburg County, North Carolina. By the execution of this Contract, the parties submit to the jurisdiction of said courts and hereby irrevocably waive any and all objections, which they may have with respect to venue in any court sitting in Mecklenburg County, North Carolina.
- 31.4. **BINDING NATURE AND ASSIGNMENT.** This Contract shall bind the parties and their successors and permitted assigns. Neither party may assign any of the rights and obligations thereunder without the prior written consent of the other. Any assignment attempted without the written consent of the other party shall be void.
- 31.5. **CITY NOT LIABLE FOR DELAYS.** It is agreed that the City shall not be liable to the Company, its agents or representatives or any subcontractor for or on account of any stoppages or delay in the performance of any obligations of the City or any other party hereunder caused by injunction or other legal or equitable proceedings or on account of any other delay for any cause beyond the City's reasonable control. The City shall not be liable under any circumstances for lost profits or any other consequential, special or indirect damages.
- 31.6. **FORCE MAJEURE.**
- 31.6.1. The Company shall be not liable for any failure or delay in the performance of its obligations pursuant to this Contract (and such failure or delay shall not be deemed a default of this Contract or grounds for termination hereunder if all of the following conditions are satisfied: (i) if such failure or delay: (a) could not have been prevented by reasonable precaution, and (b) cannot reasonably be circumvented by the non-performing party through the use of alternate sources, work-around plans, or other means; and (ii) if and to the extent such failure or delay is caused, directly or indirectly, by fire, flood, earthquake, hurricane, elements of nature or acts of God, acts of war, terrorism, riots, civil disorders, rebellions or revolutions, or court order.
- 31.6.2. Upon the occurrence of an event which satisfies all of the conditions set forth above (a "Force Majeure Event") the Company shall be excused from any further performance of those of its obligations pursuant to this Contract affected by the Force Majeure Event for as long as (i) such Force Majeure Event continues; and (ii) the Company continues to use commercially reasonable efforts to recommence performance whenever and to whatever extent possible without delay.
- 31.6.3. Upon the occurrence of a Force Majeure Event, the Company shall immediately notify the City by telephone (to be confirmed by written notice within two (2) days of the inception of the failure or delay) of the occurrence of a Force Majeure Event and shall describe in reasonable detail the nature of the Force Majeure Event. If any Force Majeure Event prevents the Company from performing its obligations for more than five (5) days, the City may terminate this Contract.
- 31.6.4. Strikes, slow-downs, walkouts, lockouts, and individual disputes are not excused under this provision.
- 31.7. **SEVERABILITY.** The invalidity of one or more of the phrases, sentences, clauses or sections contained in this Contract shall not affect the validity of the remaining portion of the Contract so long as the material purposes of the Contract can be determined and effectuated. If any provision of this Contract is held to be unenforceable, then both parties shall be relieved of all obligations arising under such provision, but only to the extent that such provision is unenforceable, and this Contract shall be deemed amended by modifying such provision to the extent necessary to make it enforceable while preserving its intent.
- 31.8. **NO PUBLICITY.** No advertising, sales promotion or other materials of the Company or its agents or representations may identify or reference this Contract or the City in any manner absent the written consent of the City.

- 31.9. APPROVALS. All approvals or consents required under this Contract must be in writing.
- 31.10. WAIVER. No delay or omission by either party to exercise any right or power it has under this Contract shall impair or be construed as a waiver of such right or power. A waiver by either party of any covenant or breach of this Contract shall not be constitute or operate as a waiver of any succeeding breach of that covenant or of any other covenant. No waiver of any provision of this Contract shall be effective unless in writing and signed by the party waiving the rights.
- 31.11. SURVIVAL OF PROVISIONS. The following sections of this Contract shall survive the termination hereof:
- Section 4.4 “Employment Taxes and Employee Benefits”
 - Section 17 “Representations and Warranties of Company”
 - Section 20 “Term and Termination of Contract”
 - Section 23 “City Ownership of Work Product”
 - Section 25 “Indemnification”
 - Section 27 “Confidential Information”
 - Section 28 “Insurance”
 - Section 30 “Notices and Principal Contacts”
 - Section 31 “Miscellaneous”
- 31.12. CHANGE IN CONTROL. In the event of a change in “Control” of the Company (as defined below), the City shall have the option of terminating this Contract by written notice to the Company. The Company shall notify the City within ten (10) days of the occurrence of a change in control. As used in this Contract, the term “Control” shall mean the possession, direct or indirect, of either (i) the ownership of or ability to direct the voting of, as the case may be fifty-one percent (51%) or more of the equity interests, value or voting power in the Company or (ii) the power to direct or cause the direction of the management and policies of the Company whether through the ownership of voting securities, by contract or otherwise.
- 31.13. DRAFTER’S PROTECTION. Each of the Parties has agreed to the use of the particular language of the provisions of this Contract and any questions of doubtful interpretation shall not be resolved by any rule or interpretation against the drafters, but rather in accordance with the fair meaning thereof, having due regard to the benefits and rights intended to be conferred upon the Parties hereto and the limitations and restrictions upon such rights and benefits intended to be provided.
- 31.14. FAMILIARITY AND COMPLIANCE WITH LAWS AND ORDINANCES. The Company agrees to make itself aware of and comply with all local, state and federal ordinances, statutes, laws, rules and regulations applicable to the Services. The Company further agrees that it will at all times during the term of this Contract be in compliance with all applicable federal, state and/or local laws regarding employment practices. Such laws will include, but shall not be limited to, workers' compensation, the Fair Labor Standards Act (FLSA), the Americans with Disabilities Act (ADA), the Family and Medical Leave Act (FMLA) and all OSHA regulations applicable to the Services.
- 31.15. CONFLICT OF INTEREST. The Company covenants that its officers, employees and shareholders have no interest and shall not acquire any interest, direct or indirect that would conflict in any manner or degree with the performance of Services required to be performed under the Contract.
- 31.16. NO BRIBERY. The Company certifies that neither it, any of its affiliates or subcontractors, nor any employees of any of the foregoing has bribed or attempted to bribe an officer or employee of the City in connection with the Contract.
- 31.17. HARASSMENT. The Company agrees to make itself aware of and comply with the City's Harassment Policy. The City will not tolerate or condone acts of harassment based upon race, sex, religion, national origin, color, age, or disability. Violators of this policy will be subject to

termination.

- 31.18. TRAVEL UPGRADES. The City has no obligation to reimburse the Company for any travel or other expenses incurred in connection with this Contract.
- 31.19. TAXES. Except as specifically stated elsewhere in this Contract, the Company shall collect all applicable federal, state and local taxes which may be chargeable against the performance of the Services, and remit such taxes to the relevant taxing authority. The Company consents to and authorizes the City to collect any and all delinquent taxes and related interest, fines, or penalties of the Company by reducing any payment, whether monthly, quarterly, semi-annually, annually, or otherwise, made by the City to the Company pursuant to this Contract for an amount equal to any and all taxes and related interest, fines, or penalties owed by the Company to the City. The Company hereby waives any requirements for notice under North Carolina law for each and every instance that the City collects delinquent taxes pursuant to this paragraph. This paragraph shall not be construed to prevent the Company from filing an appeal of the assessment of the delinquent tax if such appeal is within the time prescribed by law.
- 31.20. COUNTERPARTS. This Contract may be executed in any number of counterparts, all of which taken together shall constitute one single agreement between the parties.

[Signature Page Follows]



IN WITNESS WHEREOF, and in acknowledgement that the parties hereto have read and understood each and every provision hereof, the parties have caused this Contract to be executed as of the date first written above.

[INSERT COMPANY NAME]

BY: _____
(signature)

PRINT NAME: _____

TITLE: _____

DATE: _____

CITY OF CHARLOTTE:
[CITY MANAGER'S OFFICE/OFFICE/DEPARTMENT/DIVISION]

BY: _____
(signature)

PRINT NAME: _____

TITLE: _____

DATE: _____

[DELETE THE PRE-AUDIT SIGNATURE LINE IF CONTRACT IS NOT ENCUMBERED]

This instrument has been pre-audited in the manner required by Local Government Budget and Fiscal Control Act.

BY: _____
(signature)

DATE: _____



EXHIBIT A – PRICING SHEET

INTENTIONALLY LEFT BLANK FOR SAMPLE CONTRACT

> EXHIBIT B – SCOPE OF SERVICES

INTENTIONALLY LEFT BLANK FOR SAMPLE CONTRACT

EXHIBIT C – FEDERAL CONTRACT TERMS AND CONDITIONS

[NOTE: This exhibit *must be* included in all solicitations, including those where federal funds may be used to fund purchases of products, services, or construction solicited by this solicitation document. Contract drafters must inquire with the granting agency to determine if the agency has specific additional terms for agency contracts or if there are special terms for a specific grant. In the event that the agency requires terms different from or in addition to the general federal terms below, the agency's terms should be added to or substituted for the terms below.]

This Exhibit is attached and incorporated into the [EXACT CAPTION OF CONTRACT] (the "Contract") between the City of Charlotte and [COMPANY NAME] (the "Company"). Capitalized terms not defined in this Exhibit shall have the meanings assigned to such terms in the Contract. In the event of a conflict between this Exhibit and the terms of the main body of the Contract or any other exhibit or appendix, the terms of this Exhibit shall govern.

- 1. Debarment and Suspension.** The Company represents and warrants that, as of the Effective Date of the Contract, neither the Company nor any subcontractor or subconsultant performing work under this Contract (at any tier) is included on the federally debarred bidder's list listed on the government wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), "Debarment and Suspension." If at any point during the Contract term the Company or any subcontractor or subconsultant performing work at any tier is included on the federally debarred bidder's list, the Company shall notify the City immediately. The Company's completed Form XX – Vendor Debarment Certification is incorporated herein as Form [EXHIBIT LETTER].1 below.
- 2. Record Retention.** The Company certifies that it will comply with the record retention requirements detailed in 2 CFR § 200.333. The Company further certifies that it will retain all records as required by 2 CFR § 200.333 for a period of three (3) years after it receives City notice that the City has submitted final expenditure reports or quarterly or annual financial reports, as applicable, and all other pending matters are closed.
- 3. Procurement of Recovered Materials.** The Company represents and warrants that in its performance under the Contract, the Company shall comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds \$10,000 or the value of the quantity acquired during the preceding fiscal year exceeded \$10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.
- 4. Clean Air Act and Federal Water Pollution Control Act.** The Company agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).
- 5. Energy Efficiency.** The Company certifies that the Company will be in compliance with mandatory standards and policies relating to energy efficiency which are contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act (Pub. L. 94-163, 89 Stat. 871).
- 6. Byrd Anti-Lobbying Amendment (31 U.S.C. 1352).** The Company certifies that:

- 6.1. No federal appropriated funds have been paid or will be paid, by or on behalf of the Company, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal Loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of and Federal contract, grant, loan, or cooperative agreement.
 - 6.2. If any funds other than federal appropriated funds have been paid or will be paid to any person for making lobbying contacts to an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this federal contract, grant, loan, or cooperative agreement, the Company shall complete and submit Standard Form—LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions [as amended by "Government wide Guidance for New Restrictions on Lobbying," 61 Fed. Reg. 1413 (1/19/96)].
 - 6.3. The Company shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.
 - 6.4. The Company's completed Form **XX** –Byrd Anti-Lobbying Certification is incorporated herein as Form **[EXHIBIT LETTER].2** below.
 7. **Contract Work Hours and Safety Standards Act (40 U.S.C. 3701-3708).** If the Contract is in excess of \$100,000 and involves the employment of mechanics or laborers, the Company must comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, the Company is required to compute the wages of every mechanic and laborer on the basis of a standard work week of forty (40) hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of forty (40) hours in the work week. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or purchases of transportation or transmission of intelligence.
 8. **Right to Inventions.** If the federal award is a "funding agreement" under 37 CFR 401.2 and the City wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment of performance or experimental, developmental or research work thereunder, the City must comply with 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.
 9. **DHS Seal, Logo, and Flags.** The Company shall not use the Department of Homeland Security ("DHS") seal(s), logos, crests, or reproductions of flags or likenesses of DHS agency officials without specific FEMA pre-approval.
 10. The Federal Government is not a party to this Contract and is not subject to any obligations or liabilities to the City, Company, or any other party pertaining to any matter resulting from the Contract.
- [NOTE ON SECTIONS 11 THROUGH 13: The following three provisions are to be included only for construction contracts].**
11. **Davis-Bacon Act, as amended (40 U.S.C. 3141-3148).** In its performance under the Contract, the Company shall comply with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with

the statute, the Company is required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, the Company is required to pay wages not less than once a week.

12. **Copeland “Anti-Kickback” Act (40 U.S.C. 3145).** In its performance under the Contract, the Company shall comply with the Copeland “Anti-Kickback” Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, “Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States”). The Act provides that the Company is prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled.
13. **Equal Employment Opportunity.** In its performance under the Contract, the Company shall comply with the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, “Equal Employment Opportunity” (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, “Amending Executive Order 11246 Relating to Equal Employment Opportunity,” and implementing regulations at 41 CFR part 60, “Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor.”

Form 4- Pricing Worksheet

Regardless of exceptions taken, Companies shall provide pricing based on the requirements and terms set forth in this RFP. Pricing must be all-inclusive and cover every aspect of the Project. Cost must be in United States dollars. If there are additional costs associated with the Services, please add to this chart. Your Price Proposal must reflect all costs for which the City will be responsible.

For purposes of this RFP, assume an initial term of three (3) years, with the City having an option to renew for two (2) additional consecutive one (1) year terms thereafter.

This is a Three (3) Part RFP. You can propose on any combination of the parts (ie. only on one, both one and two, all three parts, ect). Please provide pricing for the parts of the RFP that you are proposing on. Pricing is based upon a lump sum of the contract services requested in Section 3 of the RFP. **If you are not proposing on a specific Part please place N/A in the pricing worksheet.**

For Part 1.0 Security Operation Services, this line should be the total of the lines below (1.1-1.8).

The City may require additional ad hoc services related to managed security services, Please provide an hourly labor rate below.

Part One- Security Operations Services

DESCRIPTION		Year 1- Monthly Cost	Year 2- Monthly Cost	Year 3- Monthly Cost	Optional renewal year 1 Monthly Cost	Optional Renewal Year 2- Monthly Cost
1.0	Security Operations Services	\$ 144,306.90	\$ 146,876.96	\$ 150,509.14	\$ 154,382.74	\$ 158,356.73
1.1	Core Security Operations Services	\$ 56,473.81	\$ 57,885.66	\$ 59,332.80	\$ 60,816.12	\$ 62,336.52
1.2	Analytics Platform Operations	Analytics Platform Operations is included in R9B's Core security Operations price, however, in the event the City purchases 1.2 only then the cost would be \$14,746.72	\$ 15,114.56	\$ 15,492.48	\$ 15,880.56	\$ 16,277.36
1.3	Email Threat Monitoring and Analysis	\$ 4,792.33	\$ 4,875.53	\$ 4,961.13	\$ 5,121.65	\$ 5,287.81
1.4	Cyber Intelligence Support	\$ 6,677.07	\$ 6,802.27	\$ 6,930.67	\$ 7,145.60	\$ 7,368.30
1.5	Security System Support	\$ 11,540.80	\$ 11,829.60	\$ 12,124.80	\$ 12,428.00	\$ 12,739.20
1.6	Onsite Services					
1.6.1	Onsite Tier 3 Infrastructure Security Engineer	\$ 21,854.53	\$ 21,905.60	\$ 22,454.40	\$ 23,014.40	\$ 23,590.40
1.6.2	Onsite Tier 3 Cyber Security Analyst	\$ 17,580.93	\$ 17,524.80	\$ 17,963.20	\$ 18,412.80	\$ 18,872.00
1.6.3	16 hours/month onsite information security engineering support	\$ 3,172.68	\$ 3,284.04	\$ 3,403.69	\$ 3,521.44	\$ 3,641.64
1.7	Threat Hunting	\$ 5,770.40	\$ 5,914.80	\$ 6,062.40	\$ 6,214.00	\$ 6,369.60

1.8	Compromise Assessment	\$ 1,697.63	\$ 1,740.10	\$ 1,783.57	\$ 1,828.17	\$ 1,873.90
-----	-----------------------	-------------	-------------	-------------	-------------	-------------

--	--	--	--	--	--	--

Part Two- Network Operations Center (NOC)

DESCRIPTION		Year 1- Monthly Cost	Year 2- Monthly Cost	Year 3- Monthly Cost	Optional renewal year 1 Monthly Cost	Optional Renewal Year 2- Monthly Cost
2.0	Network Operations Center (NOC)	N/A	N/A	N/A	N/A	N/A

--	--	--	--	--	--	--

Part Three- Application Monitoring

DESCRIPTION		Year 1- Monthly Cost	Year 2- Monthly Cost	Year 3- Monthly Cost	Optional renewal year 1 Monthly Cost	Optional Renewal Year 2- Monthly Cost
3.0	Applications Monitoring	N/A	N/A	N/A	N/A	N/A

Additional Hourly Labor Pricing
210.18

The Company Shall indicate in the box with an X if they can provide the following Application Monitoring Services or cannot provide the service.

Section	Key Requirements - Application Performance Monitoring	Critical	Can provide	Cannot Provide
1	Deployment Options			
1.1	Flexibility to monitor applications deployed both internally (incl. virtualized environments and /or private cloud) and externally (Amazon Cloud, Microsoft Azure etc.)	Critical		X
1.2	Vendor encrypts data transmissions end-to-end across the environment	Critical		X
2	Installation			
2.1	Ability to install Agent into application container	Important		X
2.2	Web based feature rich GUI without need for fat client (no installation, ongoing maintenance or management for web client)	Important		X
3	Configuration			
3.1	Automatically create a visualization of the entire application topology with all components.	Critical		X
3.2	Automatically discover business transactions	Critical		X
3.3	Automatically discover standard back end systems (database, web services, SAP etc.)	Critical		X
3.4	Agents will not consume more than 4% of cpu / ram / disk / network utilization.	Critical		X
3.5	Automatically baseline every component within the Business Transaction	Important		X
3.6	SSL Encrypted data transmission between EVERY monitoring component.	Critical		X
4	Better Application Visibility and Control			
4.1	Provide correlated views of distributed Business Transactions between tiers/services	Important		X
4.2	The ability to automatically baseline every component within the Business Transaction – so we understand not just that business transaction is slow but specifically which component is breaching the baseline.	Important		X
4.3	Provide code level diagnostics (class & method-level visibility) of poorly performing business transactions	Important		X
4.4	Monitor JVM health information (heap, GC, generational spaces, etc.)	Important		X
4.6	Report application errors & exceptions	Critical		X
5	Reduce Mean Time To Repair			
5.1	Identify slow and stalled Business transactions without manual intervention	Important		X
5.3	Identify error business transactions without manual intervention	Important		X
5.4	Identify slow SQL queries without manual intervention	Important		X
5.5	Identify slow backends systems or external services without manual intervention	Important		X
5.6	Automatically discover code deadlocks	Nice to Have		X
5.7	Provide quick cross launching into problem areas within the UI through hyper-linked alerts	Nice to Have		X
5.8	Automatically send email containing hyperlink to identified problem	Important		X
6	Using Business Transactions as Key Unit of Monitoring and Management			
6.1	Automatically discover business transactions (no need to configure the classes/methods for monitoring)	Nice to Have		X
6.2	Automatically learn and baseline performance of discovered business transactions	Important		X
6.3	Monitor performance and analyze customer experience through various network connections (on-site wired, on-site wireless, via VPN, via cellular)	Important		X

6.4	Discover complete transaction flow/architecture (support for synchronous, asynchronous and multi-threaded business transactions)	Important		X
7	Provide Real-Time Business Metrics			
7.1	Provide the facility to create custom dashboards for business metrics and related application behavior	Important		X
7.2	Provide pre-built performance reports on business transaction summary and business transaction trends	Important		X
7.3	Capture usage statistics for all urls, pages, web services, external calls, locations, servers.			X
7.4	Automatically correlate business transactions with environment monitoring (OS, JMX etc.)	Important		X
8	Usability			
8.1	Provide automatic & dynamic baselining of all metrics to reduce false alarms and elimination of static thresholds	Important		X
8.2	Solution offers ability to visualize multiple applications and the connectivity/dependencies between them.	Important		X
8.3	Ability to identify / collect / and provide for review transactions that relate to a given unique entity (session id, email address, login account, etc) showing the transactions in a chronological order.	Important		X
8.4	Ability to link business transaction directly back to log entries on the respective components involved in the transaction	Important		X
9	Historical Trending Capabilities			
9.1	Provide long term historical trending (metric persistence to enable historical observation (and comparison to baselines)	Critical		X
10	Support for Agile Development Processes			
10.1	Ability to provide dynamic instrumentation of applications. A newer release of an application should not break the monitoring. Agents should continue to monitor all components running while allowing for admin to properly identify the old vs the new application component.	Critical		X
10.2	Automatically baseline new components – no manual intervention required – no unnecessary alert storms or false negatives	Important		X
10.3	Allow regression analysis to compare and highlight application performance regressions/improvements	Nice to Have		X
11	Pre-Production Performance Tuning			
11.1	Identify application hotspots (quickly spot the longest running methods in poorly performing business transactions)	Nice to Have		X
11.2	Enable scalability analysis (determine impact and relationship between increased load and application average response times)	Nice to Have		X
11.3	Identify worst backend calls (Database, Web Services, other backends) automatically	Nice to Have		X
12	Workflow Orchestration and Alerting			
12.1	Ability for automated problem remediation through scripts, workflows, etc.	Critical		X
12.2	Ability for automated or manually execute processes, workflows to gather more troubleshooting details, remediate problems, or to dynamically scale resources.	Critical		X
12.3	Ability to create rules for actions and alerting: * Leverage multiple data inputs into analysis (app performance data, machine data and customer provided data) * Use Boolean logic to combine multiple conditions through AND / OR logic * Disable rule evaluation temporarily for predetermined maintenance windows * Trigger alerts or notifications when rules are violated (email, SMS or custom) * Use complex logic to combine different metrics into one trigger/alert	Critical		X
				X
				X
				X
				X
13	Memory Management			
13.1	Identify JVM memory leaks caused by leaky collections	Important		X
13.2	Enable tracking of object instantiations/destructions to troubleshoot JVM heap thrash	Important		X
14	Scalability and Infrastructure Efficiency			
14.1	Ability to support high availability APM infrastructure servers	Important		X

15	Integration with 3rd Party Tools			
15.1	Demonstrate how solution can integrate with 3rd parties (e.g. BMC, Splunk, Apica, SOASTA, Silkperformer, Jenkins etc.)	Important		X
15.2	Ease of integration via RESTful API	Important		X
0	Web Real User Monitoring			
16.1	Support for modern desktop browsers	Critical		X
16.2	Support for mobile browsers	Critical		X
16.3	Monitor all page requests	Critical		X
16.4	Monitor all AJAX requests	Critical		X
16.5	Monitor all iFrame requests	Nice to Have		X
16.6	Monitor all web platforms (Apache Tomcat, Jboss, Java, IIS)	Critical		X
16.7	Full support for monitoring single page applications properly	Critical		X
16.8	Automatically detect JavaScript errors	Critical		X
16.9	Correlate web transactions with server side transactions for drill down	Important		X
16.10	Provide detailed browser traces for poor performing end user requests	Important		X
16.11	Provide usage based analytics showing browser types and versions	Important		X
16.12	Provide usage based analytics showing device and OS types	Important		X
16.13	Provide cache metrics for each page request	Important		X
16.14	Show server side response time for all pages	Important		X
16.15	Provide tracking for various entities, such as sessions, ports, IPs, user logins.	Critical		X
17	Synthetic Visibility			
17.1	Real browser endpoints running scripts not simulated browsers	Important		X
17.2	Simulate mobile network speeds	Nice to Have		X
17.3	External website testing	Critical		X
17.4	Ability to script tests	Critical		X
17.5	Auto-retest after failed test	Critical		X
17.6	Flexible alerting system	Critical		X
17.7	Variable bandwidth testing	Nice to Have		X
17.8	Standards based scripting language (Selenium)	Important		X
17.9	Synthetic data analytics	Important		X
17.10	Synthetic session tracking	Important		X

The Company shall indicate in the box below by placing an X whether they can provide/cannot provide the following Services as it relates to the Network Operation Center performance monitoring.

Key Requirements	Impact Description	Can Provide	Cannot Provide
Incident Initiation Capabilities			
Compatibility with Cherwell	The ability to open send data to Cherwell so that tickets can be automatically opened and assigned based on an API or a properly formatted e-mail.		X
Monitoring Capabilities - Server			
Monitor Machine availability	The ability to monitor basic UP/DOWN of servers to ensure service.		X
Monitor CPU usage	The ability to watch CPU and gather statistics and tie consumption to specific processes.		X
Monitor Disk performance	The ability to monitor disk I/O IOPS metrics.		X
Monitor Volume usage	trending metrics.		X
Monitor Machine load	needs to go up or down.		X
Monitor Memory	consumers are with trending metrics.		X
Monitor SWAP	specific processes along with trending metrics.		X
Monitor Processes	for correlation along with trending metrics.		X
Monitor Network Adapter(s)	with the ability to monitor active/passive failover groups.		X
Dynamic Baselineing	baselines on system behavior for any available metric.		X
Synthetic page checker	performance checker within corporate firewalls.		X
Monitoring Capabilities - Network			
Monitor Machine availability	The ability to monitor basic UP/DOWN of network equipment to ensure service.		X
SNMP Traps on core / distribution / data center switches	The ability to watch and gather statistics and tie consumption to specific processes -CPU/Memory -Temperature -Power Supplies		X
Monitor Critical Interfaces on core / distribution / data center switches	The ability to monitor critical network interfaces.		X
Backup Switch Configurations	The ability to backup switch configurations		X
Netflow	Response time/latency -Bandwidth utilization on core/distribution/datacenter switches/firewalls -reporting		X
Monitoring Capabilities – Microsoft			
Microsoft Exchange	Must interface with MailScape		X
Microsoft Active Directory	Ability to monitor Active Directory Health		X
Monitoring Capabilities – Security Appliances			X