

Public Records Request #2783

The following materials have been gathered in response to public records request #2783. These materials include:

- RFP #269-2019-109 – Team Alphanumeric Response
- RFP #269-2019-109 – Team Alphanumeric Response – Pricing Worksheet
- RFP #269-2019-109 – root9B Response
- RFP #269-2019-109 – root9B Response – Pricing Worksheet
- RFP #269-2019-109 – root9B Response – Pricing Worksheet
- RFP #269-2019-109 – CenturyLink Response
- RFP #269-2019-109 – CenturyLink Response – Pricing Worksheet
- RFP #269-2019-109 Evaluation Workbook
- Contract #2020000428: Agreement to Provide Managed Security Services

This information was provided as a response to a public records request on 1/8/20 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

Note: There was no weighting or formal shortlisting, but three (3) companies were requested to provide Best and Final Offers (BAFO), so those three are included per the requestor's indication of wanting the top three vendors.

- Vendor Proposals (Note that CenturyLink DID indicate some confidential information, but the requestor is CenturyLink. Project file indicates they did not respond to requests to clarify so full copy has been provided – this should NOT go on the open portal)
- BAFO from Alphanumeric, Root9B, and CenturyLink
- Evaluation sheet with notes from those three vendors

Executed Root9B contract

City of Charlotte

Managed Security Services

Technical Proposal

12 July 2019

Submitted to:

Elizabeth Barnard
City of Charlotte - City Procurement
elizabeth.barnard@charlottenc.gov

Submitted by:

Rob Vanderberry
Team Alphanumeric
4515 Falls of Neuse Rd
Raleigh, North Carolina

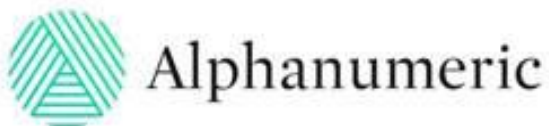


Table of Contents

| | |
|---|-----------|
| 1. COVER LETTER | 3 |
| 2. PROPOSED SOLUTION | 4 |
| 2.1 Security Operation Services | 4 |
| 2.1.1 Transition Support..... | 5 |
| 2.1.2 SOC Operations, Facilities, Personnel, and Communication..... | 5 |
| 2.1.3 System Access | 7 |
| 2.1.4 Reporting | 7 |
| 2.1.5 Security Event Management and Communication..... | 8 |
| 2.1.6 Security Event Analysis | 10 |
| 2.1.7 Security Incident Response..... | 12 |
| 2.1.8 Changes to Information Security Systems | 14 |
| 2.1.9 Additional Service Requirements..... | 14 |
| 2.2 Application Performance Monitoring | 17 |
| 2.3 Network Operations Center..... | 17 |
| 2.4 Reporting Requirements..... | 17 |
| 2.5 Training Plan..... | 17 |
| 2.6 Disaster Recovery | 17 |
| 2.7 City Hardware/Software Requirements | 17 |
| 3. SECTION 6, FORM 2, ADDENDA RECEIPT CONFIRMATION | 18 |
| 4. SECTION 6, FORM 3, PROPOSAL SUBMISSION..... | 19 |
| 5. SECTION 6, FORM 4, PRICING WORKSHEET | 21 |
| 6. SECTION 4, FORM 5, MWSBE UTILIZATION | 22 |
| 7. SECTION 6, FORM 6, COMPANY BACKGROUND AND EXPERIENCE | 24 |
| 8. SECTION 6, FORM 7, REFERENCES..... | 25 |
| 9. SECTION 6, FORM 8, ADDITIONAL COMPANY QUESTIONS..... | 32 |
| 10. SECTION 6, FORM 9, CERTIFICATION REGARDING DEBARMENT, SUSPENSION AND OTHER RESPONSIBILITY MATTERS..... | 35 |
| 11. SECTION 6, FORM 10, BYRD ANTI-LOBBYING CERTIFICATION..... | 36 |

1. Cover Letter

The Alphanumeric Team comprises resources from Alphanumeric Systems, Inc. and Delta Risk LLC, working in collaboration to leverage each company's specific expertise in Information Technology and Cybersecurity to provide a range of technical, assessment and advisory services to our clients in North Carolina.

Headquartered in Raleigh, Alphanumeric Systems, Inc., with over 40 years of experience serving North Carolina Universities, agencies and commercial clients, Alphanumeric has a unique insight into the State's culture and environments, as well as a keen understanding of the information technology landscape.

Our partner in delivering security assessments, Delta Risk, is a national and global leader in the cyber security community, delivering tailored and high-impact cyber security and risk management services to government and commercial clients worldwide. Established in 2007 by former Air Force cyber operators, Delta Risk provides a full complement of professional consulting and managed security services to include training, exercises, research, policy, governance, assessments, penetration testing, incident response, as well as the ActiveEye family of managed security services.

Delta Risk supports several US Government agencies to include the Department of Defense (DoD) and the Department of Homeland Security (DHS), as well as North Carolina State agencies. We also support a wide range of commercial and non-profit enterprises to include several Fortune 100 companies, Carnegie Mellon University's Software Engineering Institute, as well as other Universities. Delta Risk's Board of Directors is comprised of cyber and security leaders to include former DHS Secretary Michael Chertoff and former CIA Director Michael Hayden. Delta Risk was recently named a "Top 10 Managed Security Service Provider" by Enterprise Security Magazine and a "Top 25 Cyber Company" by CIO Applications. Delta Risk was recently added to the GSA IT-70 contract vehicle in May 2017 and that award included the Highly Adaptive Cybersecurity Service's for Penetration Testing, Incident Response, Cyber Hunt, and Risk and Vulnerability Assessments.

Team Alphanumeric is pleased to offer this proposal for the city of Charlotte. Our service is founded on our people; our U.S.-only based SOCs, located in San Antonio and Dulles, Virginia are staffed by a mix of veterans and commercially professionals who are experienced in security operations, analysis, and customer service. Our customer-focused platform provides complete visibility through our customized dashboard. Our dashboard is designed for ease of use and is the same dashboard that your personalized Team Alphanumeric account analyst uses.

Providing managed security services for our clients is an extension of the professional service business that Team Alphanumeric was founded on. We strive to be your partner for cybersecurity, providing the capability to for protecting your environment and detecting any suspicious or malicious activity in your environment. We go beyond just monitoring your network, providing research on any activity detected and working with your team to provide remediation recommendations and provide support until the problem is resolved.

2. Proposed Solution

Alphanumeric and Delta Risk have been working together since 2016, with broad experience between the teams that provides familiarity and understanding between our two companies and allows us to provide a seamless experience for our customers. Our solution focuses on the Security Operations Center sections of the RFP and does not include Application Performance Monitoring or Network Operations Center services.

2.1 Security Operation Services

Team Alphanumeric is pleased to offer its ActiveEye Managed Security Platform offered by Delta Risk. This platform is designed to support organizations requiring cybersecurity operations center support. Our solution offers a flexible platform that can be modified to fit each organization's need. As such, we offer custom implementations for each client, where understanding specific organization needs, environment, and capabilities are assessed and integrated into the final solution. Our ActiveEye solution is configurable based on customer requirements, and is powered by three core components:

Exceptional People: ActiveEye is staffed by Team Alphanumeric's team of highly trained and experienced security analysts and engineers, who provide expert analysis and actionable advice based on current threat intelligence.

Efficient Processes: ActiveEye employs proven processes for deployment, operations, maintenance, tuning, and more. The service can also integrate with existing information technology (IT), risk management, and security processes to provide high-impact information exchange. Team Alphanumeric constantly refines and improves processes in order to deliver ActiveEye capabilities at a much lower cost than a comparable in-house solution.

Multi-Layer Technology: ActiveEye offers advanced technology to secure customer systems and data, whether external to the customer network, at the perimeter of the customer network, or internal to the customer network. This is powered by the following advanced tools, enhanced and tailored to customer requirements.

In addition to traditional SOC services, Team Alphanumeric offers our ActiveEye Cloud services. ActiveEye Cloud combines configuration best practices with advanced analytics to gain visibility and control in platforms (AWS, Microsoft Azure, Google Cloud) and key enterprise applications (Office365, GoogleApps, Okta) driving the business.

ActiveEye Cloud provides three capabilities across the enterprise cloud environment:

1. **Discovery:** identify cloud resources as deployed and compare against approved workload types
2. **Configuration Assessment:** view current configuration and compare against best practice security approaches
3. **Activity Analytics:** monitor management and usage activity with advanced analytics and machine learning.

2.1.1 Transition Support

Upon award notification, Team Alphanumeric will begin transition activity, beginning with the stand-up of the managed transition team, led by the Alphanumeric Program Manager. The transition team will consist of the Charlotte Account SOC lead, a security engineer, and our Solutions Architect. This team will begin work with the City of Charlotte to schedule a kickoff meeting within two weeks of award.

The Alphanumeric Program Manager and the transition team will develop a Transition Management Plan that will detail activities to occur from Day 1 until SOC services are completely cutover to Team Alphanumeric. This plan will focus on setting up the monitoring services as required and develop procedures for cutting over monitoring services while maintaining coverage throughout the process. We will work with the incumbent provider to develop a plan that fits within the transition period. The plan will be developed in conjunction with City of Charlotte personnel for proper oversight.

During this transition, Team Alphanumeric will also work through on-boarding requirements, such as submitting paperwork and documentation and setting up required interviews for employees requiring elevated access. We will establish regular transition update meetings to keep the entire team aware of progress and then transition these meetings into the regular weekly and monthly update meetings as directed in the reporting requirements.

2.1.2 SOC Operations, Facilities, Personnel, and Communication

Our ActiveEye Service offering support our clients' integration of the NIST Cybersecurity Framework functions and provides a versatile platform that integrates the protect detect respond, and recover functions through a mixture of our experienced cybersecurity staff, processes and technology. Our ActiveEye solution provides:

Modern Security Management Platform

- **Simple to deploy SaaS solution** designed to co-manage security with customer
- Native security for Cloud & SaaS Apps

SOC-as-a-Service

- 24x7 **detection & response** with cyber experts trained in cloud security
- Assigned analysts and industry focused teams maintains continuity & awareness

Security Services

- Highly skilled experts deliver **incident response** & recovery on demand
- Proactive **threat hunting, penetration testing and cyber training** complete the solution

Our SOC services are 24x7, with the Delta Risk headquarters in San Antonio, Texas serving as our primary site, with a back-up location at our Dulles, Virginia office. All of our analysts and engineers are employees and none of our operations are offshored. You will be assigned a primary and secondary analyst that will focus on the City of Charlotte account. The primary analyst will spend 40%-60% of their time monitoring your deployed systems and associated data and captured events. The secondary analyst will back-up the primary analyst and range from 20%-50% depending on the availability of the primary analyst (i.e. days off and shift). Other analysts will be monitoring as needed and all major events/alerts

are broadcast to SOC staff for situational awareness and to ensure nothing is missed. The analysts are assigned during the onboarding of new customers as to best determine who is a best fit for the managed infrastructure and an appropriate balance of existing workloads. We also hire new analysts as needed to ensure proper time can be dedicated for each customer. Per the SOW requirements in Section 3.2.2.6, we will provide a Senior Security Engineer to provide specific security consulting advice on the City of Charlotte's cybersecurity needs. Team Alphanumeric has a deep bench of cybersecurity professionals who are experienced in providing cybersecurity engineering support and a variety of technical assessments to our clients, including the various North Carolina state agencies we support as part of the State of North Carolina's 918A Security Services contract.

Our SOC staffing is based on a three-tier system with the below qualifications standards:

Tier I

- Bachelor's Degree in Computer Science/Information Technology/Information Security or related experience
- 1-3 years hands-on technical security experience
- 1-3 years' experience in a DevSecOps, Security Operations, or similar role
- Certifications (A+, SEC+, Network+)

Tier II

- Bachelor's Degree in Computer Science/Information Technology/Information Security or related experience
- 3-5 years hands on technical security experience
- 3-5 years' experience in a DevSecOps, Security Operations, or similar role
- Previous experience in an incident response capacity
- Certifications (GSEC, SEC+, Network+, GCED, GCIA)

Tier III

- Bachelor's Degree in Computer Science/Information Technology/Information Security or related experience
- 7+ years hands-on technical security experience
- 7+ years' experience in a DevSecOps, Security Operations, or similar role
- Certifications (GSEC, CISSP, GCED, GCIA, OSCP)
- Experience with security architecture and design
- Experience in an offensive security role

We have reviewed the CJIS security policy and either are or can be in compliance with this policy. As a contractor to DoD and other Federal contracts, we maintain compliance with a variety of frameworks, such as NIST 800-171 *Protecting Unclassified Information in Nonfederal Information Systems and Organizations*, so we are familiar with implementing appropriate cybersecurity safeguards to protect our and our client's data. All Team Alphanumeric employees undergo a background check prior to hiring. Any employees who require security clearances undergo additional screening.

Notice will be made of any staffing changes made that affect the City of Charlotte. Notice will be made either at regularly scheduled weekly conference calls. In addition to personnel changes, our weekly conference calls, which will normally be led by the City of Charlotte's primary analyst, will review the current events that are being worked and any issues that require resolutions. More detailed analysis of

City data will be conducted at the monthly meetings detailed in Section 2.1.4 and in the monthly and annual reports.

2.1.3 System Access

Team Alphanumeric understands the principle of least privilege and will follow the City’s guidelines when any system access is granted. Any Team Alphanumeric personnel in a role that requires access will be submitted for approval to the city prior to being allowed any sensitive access to City of Charlotte systems.

2.1.4 Reporting

Our ActiveEye platform captures key metrics around workloads, ability to meet service levels, and response actions taken. Through the ActiveEye portal, the team produces a standard monthly report that highlights the previous month’s activities, pending tasks and technology health and profile of events. Monthly reports and key statistics required by the city and identified during the on-boarding process will be provided and delivered on the negotiated timeframes to meet City reporting deadlines. Our reporting is based around Service Level Agreements and our event adjudication is based on the negotiated timeline and tracked in real time. All events are available to the City of Charlotte in real time, but will be reviewed monthly to look at trends, analyst workloads, and any other required agenda times. An example of our Alerts Matrix is shown in Figure 1 where event response and closeout statistics are tracked in real time. Reports with graphical depictions of trends will be developed according to City of Charlotte requirements, as well as ad hoc reporting requirements with reports delivered within three business days. Our client portal does provide many reporting options that can either be requested or self-service and provides the same view that our SOC analysts see. Further information of the user portal can be found <https://deltarisk.com/activeeye-platform/>

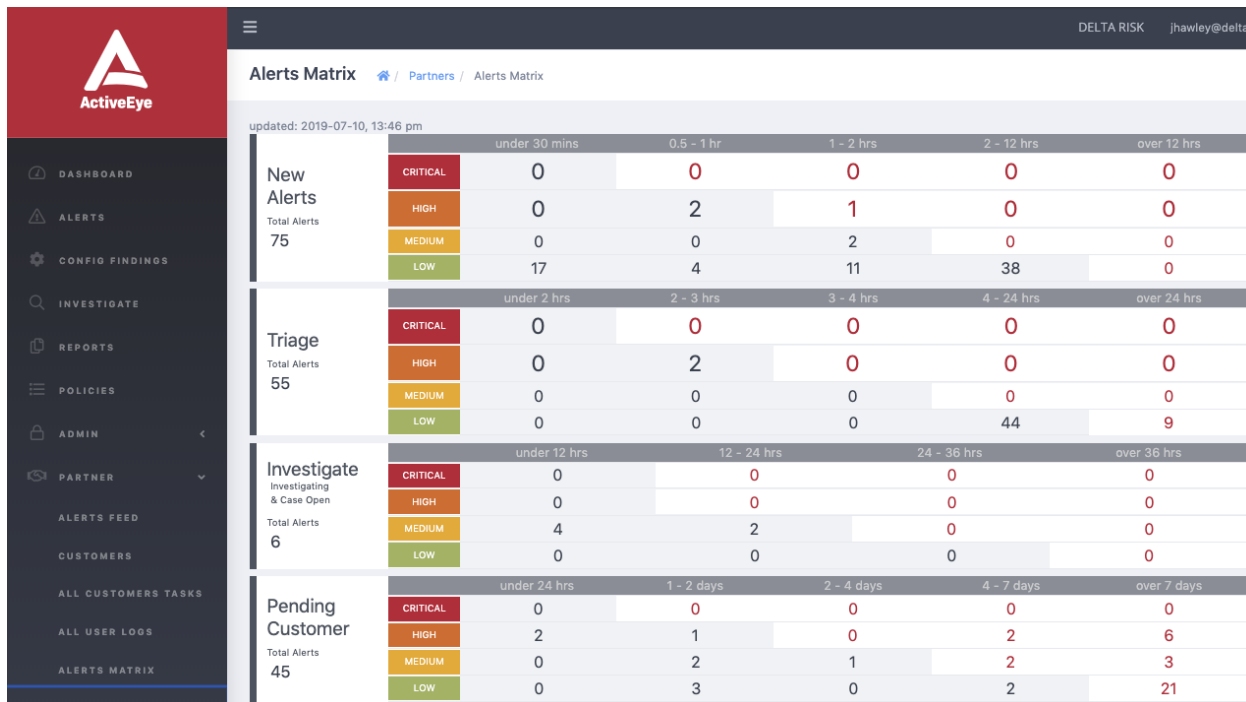


Figure 1: Alerts Matrix

2.1.5 Security Event Management and Communication

Team Alphanumeric can offer a competitive Security Incident and Event Management (SIEM)/Log Management system through implementation of our ActiveEye platform utilizing the Enhanced AlienVault Unified Security Management™ (“AlienVault”) Solution (Perimeter and Internal) system. AlienVault USMTM features fully integrated, onboard security controls such as robust network and host-based intrusion detection (NIDS and HIDS), asset inventory, archival log storage, threat intelligence and vulnerability scanning capabilities that are provided at no additional cost to the customer. In other words, customers may be able to eliminate or forego the costs of other “stand-alone” security technologies, as this provides perimeter and internal protection.

AlienVault USMTM also enables real-time massive log correlation utilizing both AlienVault and custom Team Alphanumeric correlation directives as well as highly skilled, recurring in-depth manual log review and security analysis (commonly referred to as “hunting”). Once Events of Interest (EOIs) have been detected and analyzed by Team Alphanumeric experts, actionable alerts are passed to the customer’s Incident Response process and followed until closed. Routine management and controls-based reporting is provided to support regulatory compliance as well to give the customer visibility and confidence in the security posture of the monitored environment.

All reporting and customer inputs are done through the ActiveEye portal. This portal serves as a common platform for both Team Alphanumeric and the City of Charlotte, with all the same functionality enabled to allow maximum visibility into the current security posture of the City, as well as allow City control to enter and track the status of tickets, track events, and request services offered as part of ActiveEye platform. The ActiveEye Portal is designed to adapt to screen sizes through responsive design and all communication is secured via https. It will work on any device with a standard browser and is most easily on larger form factor mobile devices. ActiveEye can send alert notifications via applications that work well on mobile devices like email, Teams, and Slack. Interaction with the SOC can be done via email that is configured securely with Team Alphanumeric. ActiveEye uses https for communications behind a web application firewall with rules specifically to limit risk and exposure to threats. Two factor authentication (2FA) is used using a one-time SMS code for login. User sessions are expired every 12 hours.

For data encryption, we can implement AES-256 encryption for all data collected when it is at-rest. For data in-transit, TLS 1.2 or greater is required. The following ciphers are supported on the ActiveEye platform:

ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
AES128-GCM-SHA256
AES128-SHA256
AES256-GCM-SHA384
AES256-SHA256

For incident reports, Team Alphanumeric can provide the following information as part of the reporting and tracking process, namely:

- Event Summary
- Severity
- Event data ad time in UTC
- SOC POC
- Current Status
- Attack vector
- Indicator of attack (raw log, hashes, file names, registry entry, etc)
- Other related incidents
- Actions taken by SOC
- Chain of custody if applicable
- Impact assessment
- Source hostname, IP, port, protocol
- Destination hostname, IP, port, protocol
- Endpoint protection software versions
- Impacted department
- Identification method
- References
- Resolution

Team Alphanumeric will analyze events created and/or aggregated by the service, assess their type, and notify the customer in accordance with established notification procedures for the City of Charlotte in line with the details from the RFP. As described in Table 1 below. Please note that our current operating model focuses on delivering analysis on the events that we see and working through established Team Alphanumeric alert lifecycle and our established SLA for triage and investigation. This allows our team to escalate security events that have been investigated, have sufficient detail, and provides the city clear steps and information for remediation or entry into the City’s Incident Response process. We can provide initial notification of events on the timelines noted, but they will not necessarily have full details associated with them. Our current tracked response timelines are denoted in Figure 1 above according to our standard service levels.

| Incident Risk Level | Notification to City Within | Required Notification Method(s) |
|----------------------------|------------------------------------|--|
| Critical | 5 minutes | Call first, then email |
| High | 30 minutes | Call first, then email |
| Medium | 60 minutes | Email |
| Low | 24 hours | Email |

Table 1: Notification times and methods.

2.1.6 Security Event Analysis

Team Alphanumeric can offer a competitive Security Incident and Event Management (SIEM) / Log Management system through implementation of our ActiveEye platform utilizing the Enhanced AlienVault Unified Security Management™ (“AlienVault”) Solution (Perimeter and Internal) system. ActiveEye employs an enhanced, proprietary implementation of AlienVault United Security Management™ (AlienVault USM™) technology deployed at both the Team Alphanumeric Security Operations Center (SOC) and within the customer’s environment. This technology is fully managed (e.g., configured, updated, performance-tuned, etc.) by Team Alphanumeric engineers on an ongoing basis.

AlienVault USM™ features fully integrated, onboard security controls such as robust network and host-based intrusion detection (NIDS and HIDS), asset inventory, archival log storage, threat intelligence and vulnerability scanning capabilities that are provided at no additional cost to the customer. In other words, customers may be able to eliminate or forego the costs of other “stand-alone” security technologies, as this provides perimeter and internal protection.

AlienVault USM™ also enables real-time massive log correlation utilizing both AlienVault and custom Team Alphanumeric correlation directives as well as highly skilled, recurring in-depth manual log review and security analysis (commonly referred to as “hunting”). Once Events of Interest (EOIs) have been detected and analyzed by Team Alphanumeric experts, actionable alerts are passed to the Customer Incident Response process and followed until closed. Routine management and controls-based reporting is provided to support regulatory compliance as well to give the Customer visibility and confidence in the security posture of the monitored environment.

For SIEM and log management, the AlienVault platform is a single platform that combines asset discovery, vulnerability assessment, intrusion detection, incident response, SIEM, and log management for your enterprise. Data logs are stored in the appliance at your site. If data logs are desired to be kept for a specific period of time (a year as described), the storage needs to be provisioned in the device system that our AlienVault client is installed or storage can be moved to a separate data store. As presented in this proposal, our SIEM and central log management are on the same device. The services can be separated onto their own devices, but this would add additional hardware and configuration costs. Team Alphanumeric can assist you in determining the best solutions for this. Log events are gathered primarily via syslog from managed devices and from port mirroring or SPAN ports. AlienVault USM immediately starts receiving events from the device through the port and starts analysis on them. Our USM platform solution does not perform an automatic NAT/PAT to Public IP lookup, however for clients who have assets that are NATed, we manually encode the mapping to assist in attack correlation and target identification and could do this for uncomplicated environments. For most of our implementations, we have not had issues with correlations arising from NAT schemas. AlienVault USM can receive events from the device through the port and begin analysis. When an incident happens, you need immediate 360° visibility of the actors, targeted assets, exploitable vulnerabilities on those assets, methods of attack, and more. AlienVault USM delivers all this data in a unified console with rich security analytics to give you rich context to make fast, effective decisions.

The Team Alphanumeric service provides:

- Log aggregation, correlation, monitoring, and notifications for in-scope assets and services, including:
 - OS logs

- Application logs
- Infrastructure logs
- Security device logs
- Create custom plugins to ingest logs from non-standard sources, as required
 - Up to three custom plugins are included at no additional cost
 - Subsequent custom plugins can be created and paid for through a change order
- Monitoring Server and Service availability
- Crowd-sourced Threat Intelligence

In our solution, all relevant security data is available at your fingertips with intuitive search and filter capabilities, making incident investigation a fast and efficient process. In the USM platform, you can easily:

- Search events to identify activity and trends
- Apply filters to find more granular data
- Sort by event name, IP address, and more
- Create, save, and export custom data views
- Examine raw log data related to alarm activity
- Access OTX pulses and “in the wild” security information

Unified Security Visibility of Assets, Events, and Vulnerabilities

For every alarm raised in AlienVault USM, analysts (and you as the customer) can drill down to see the related assets, vulnerabilities, events, and much more from a single consolidated view. All-in-one unified security management means that you can:

- See all alarms and events per asset
- Know if your vulnerabilities affect high-priority or business-critical assets
- Correlate vulnerabilities with malicious activities
- Drill down in an alarm to see the individual events that triggered the alarm
- View forensics data about what triggered events

Our analysts use a combination of network-based signatures, host-based intrusion detection system (HIDS), existing security appliance event logs, event correlations, behavioral analysis, log volumes are methods that the Team Alphanumeric SOC uses to detect threats. The SIEM is the main component to exposing these and enabling the advanced detection and analysis capabilities.

Tuning

Team Alphanumeric will assess certain events to be environmental noise, potentially addressable configuration items, or false positives. Team Alphanumeric may recommend these be addressed by the Customer to preserve system and network resources.

Tuning Period

The first thirty (30) days of the SOW Term are considered the Tuning Period. During the Tuning Period, Team Alphanumeric may make recommendations to the Customer to adjust the configurations of their installed software so that Services can be efficiently and effectively delivered over the course of the SOW Term. This optimization may include the tuning of Intrusion Detection, establishing a baseline of network traffic, or other activities designed to improve the quality of the Services. Best efforts will be made to

provide services during this period. However, SLAs will not be applicable during the Tuning Period. Additional tuning recommendations will continue, if necessary, after this initial 30-day period, with no impact to SLAs.

Analysis

As anomalous traffic is detected and alerted on, each event will be assigned to an analyst for further investigation according to the alert priority. All events trigger a trouble ticket and will result in a detailed analysis with a written synopsis of the event with recommended courses of action and any research that was done on the specific incident that will help educate the City of Charlotte on the specific threat vector. All analysts are available to discuss the event further if needed. Any event that is determined to be a malicious actor and/or could pose a threat to the City of Charlotte's information or infrastructure will then be moved to the incident response process as described in the following section.

2.1.7 Security Incident Response

Our incident response service specifically deals with a bona-fide incident response at the level of a major incident that requires additional specialist support and is described in the following paragraphs. As detailed by the City of Charlotte, our normal process for alerts covers the requirements as detailed in this RFP. Our analysts don't just report an issue and leave you to deal with the remediation and recovery efforts – we provide recommendations on remediation and recovery, as well as work with your team to support the process. If a major incident occurs, we can provide additional support that is described below, but on-site additional support requires additional funds to implement.

Team Alphanumeric is in a unique position to offer Incident Response capabilities for our clients in conjunction with our managed security service. Our team includes military veterans who have served in cyber defense units who have extensive cyber incident response and cyber hunt skills. Unless requested otherwise, the Team Alphanumeric SOC will organize incident response efforts as described in NIST 800-61 Rev. 2, *Computer Security Incident Handling Guide*. This national standard describes best practices throughout the incident response lifecycle, namely: Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and Post-Incident Activities.

Team Alphanumeric's Incident Response process is flexible and will adjust to match an incident's circumstances. Preparing for, detecting, and formally declaring an incident is the responsibility of the customer unless we come to a different agreement during the on-boarding process.

Once an incident is declared, Team Alphanumeric will provide the following support to investigate, contain, eradicate, and recover from the incident:

- Appropriately trained and certified incident response personnel
- Technical tools required to collect incident response data on a variety of system types.
- Analysis of data to help determine the incident's impact, cause, extent, and discernable details.
- Incident response advice to inform Customer's choices regarding containment, eradication, and recovery
- Procedural advice and expertise.
- Assistance communicating with outside vendors and other entities.
- Assistance in meeting incident response requirements levied through policy, procedure, law, or regulation.

Our AlienVault platform provides 24x7 analysis, aggregation, and alerting of network and host activity, allowing our analysts to screen all anomalous activity. Carbon Black Response allows us to detect, record, and stop malicious activity on your enterprise. Infocyte HUNT allows our analysts to remotely and actively scan systems for indicators of compromise, giving us a snapshot of the possible threats on systems. In the event of discovering anomalous activity, our team of analysts perform manual host-level forensics using a variety of tools, including the SIFT workstation, FTK imager, and encase. We also use Splunk to do big-data and statistical analysis of relevant logs. Finally, we perform manual and automated reverse engineering and analysis of malware using tool such as Joe Sandbox.

In the event of a suspected incident, Team Alphanumeric works remotely with the customer to validate the incident and provide analytical support immediately. We provide you with the tools needed to acquire and send the forensics artifacts and logs needed to answer immediate questions and concerns. Team Alphanumeric helps remediate the incident by making sure the customer understands the full scope of the incident, how it occurred, and what needs to be fixed or contained. Our support, while initially remote, can change to include on-site support depending on the circumstances and level of engagement required. We follow the NIST SP 800-61r2 process for incident containment, eradication, and recovery. This includes defining the incident's scope and finding malicious indicators that inform containment and remediation actions. We then work with the customer to evaluate how the capabilities they already have on-site can be used for containment, as well as any new controls that may need to be introduced. When necessary, Team Alphanumeric will introduce Carbon Black Response to endpoints to help prevent the spread of an incident. Once the circumstances that allowed the incident to occur are understood, Team Alphanumeric provides post-incident recovery recommendations to improve the organization's security posture. Throughout the event, regular meetings are held until the event is mitigated.

All phases are fully coordinated with Customer's Project Sponsor, to minimize any adverse impacts that may occur as a result of Team Alphanumeric services. While it is solely the Project Sponsor's decision and responsibility to inform other individuals, components, divisions and management, Team Alphanumeric strongly recommends full disclosure of any technical need / possible security incident to all individuals responsible for the network, application and / or related services and devices. Should the assignment be of a technical nature, Team Alphanumeric takes precautions to minimize negative impact on Customer systems. However, due to the inherent risk of such a service, Team Alphanumeric does not guarantee against service interruptions. Team Alphanumeric encourages open communications and the establishment of response procedures in the event of any adverse impact or disruption of network services and will work with your team to provide a resilient response to maintain service where possible and provide recommended courses of action throughout the response activities.

Team Alphanumeric typically does not perform configuration changes as part of its service offering but will work with the City of Charlotte to identify tasks that may be conducted to improve efficiency towards are more effective response. This topic is discussed more fully in section 2.1.9.8.

Lesson learned are a key step in the incident response process. Team Alphanumeric is a firm believer in learning from incidents to document and improve processes used, as well as identify any gaps in training or tools that should be addressed to be better prepared for future events. Team Alphanumeric will support the City's efforts post-incident and provide specific feedback and recommendations to improve the processes, as well as support the assessment to determine root cause of the incident.

2.1.8 Changes to Information Security Systems

Team Alphanumeric will follow the City of Charlotte's change management process, both for routine and emergency changes to support the proper documentation of the network environment in line with industry best practices. If Team Alphanumeric were to make changes, our analysts are available 24x7 to make these changes. Changes to systems are further discussed in Section 2.1.9.8.

2.1.9 Additional Service Requirements

Team Alphanumeric is prepared to support the additional service requirements that the City of Charlotte has and has provided responses for the nine additional categories below.

2.1.9.1 Analytics Platform Operations

As described in Section 2.1.6, the AlienVault SIEM has an analytics platform that can both store and conduct analysis on logs. Our storage solution can be on the City premises or hosted on Amazon Web Services, depending on the options desired by the City. Logs can be searchable for up to 90 days, with cold storage for 365 days available. Our platform is able to meet the log requirements of 7,000 events per second and 200 GB daily log data as detailed in section 3.17 of the RFP. All alerts can be securely accessed through the ActiveEye Portal using secure http with multi-factor authentication or through local storage, depending on the option taken. Log sources can be added by opening a request ticket and parsing and indexing for new devices can be set up within 30 days. We can set up alerts in the AlienVault SIEM to alert on non-responsive device when they reach the time threshold and will notify the City based on the source's threshold being reached. We currently provide daily status checks on monitored devices. We believe we can reconfigure alerts for the 2-hour requirement and will work towards this if awarded. We can create automated alerts on identified triggers to allow the City of Charlotte a more redundant monitoring and alerting capability for critical systems. The ActiveEye Portal is the same view that our analysts have, so City of Charlotte employees can create custom notifications in the portal (or open a request ticket to have a notification created). We will provide training for at least 14 personnel on the ActiveEye platform for City employee to be familiar and able to effectively utilize the ActiveEye Platform. User access to the ActiveEye Portal can be added to the City of Charlotte's Active Directory user store to provide secure, single sign-on. Delta Risk provides on-going support thru the incident ticketing system, email or phone to our SOC. Team Alphanumeric has over five years of experience with implementing these types of solutions.

2.1.9.2 Email Threat Monitoring and Analysis

Team Alphanumeric support the analysis of suspicious email through our SOC analysts. Our team has the ability to sandbox suspicious emails and conduct analysis of the links and any payloads associated with the email to determine if any malicious code or links to questionable sites are included. We can associate indicators discovered to known threat actors through our experience with our other customers and our threat intelligence sources to help identify specific countermeasures that can be implemented and to track specific threat actors against the city to track any trends that may be discovered through data analysis of City of Charlotte data, as well as through our other ActiveEye Managed Security Service customers. Any malicious emails that pose a threat to the City of Charlotte's information systems will enter the Incident Response process. Our bid is based on a workload of 300 emails/month. If the expected workload is significantly different from this assumption, we can modify our quote accordingly.

2.1.9.3 Cyber Intelligence Support

Team Alphanumeric partners with multiple technology and service providers to stay current with the latest alerts and notifications. Team Alphanumeric's ActiveEye solution integrates with the leading threat, endpoint and SIEM vendors like AlienVault and Carbon Black, and recently achieved Amazon Web Services Advanced Partner Status. Team Alphanumeric also interacts with and contributes to threat intelligence feeds like the AlienVault Open Threat Exchange (OTX) to be aware of potential threats. OTX provides open access to a global community of threat researchers and security professionals. It now has more than 100,000 participants in 140

countries, who contribute over 19 million threat indicators daily. In addition, other threat intelligence feed and tools, such as Maxmind, VirusTool, and IBM X-Force are often utilized during investigations. Carbon Black also leverages its Predictive Security Cloud's aggregated threat intelligence which is applied to look for flagged behavior patterns. Team Alphanumeric analysts use pre-defined playbooks to consistently address security threats and to train new analysts around common scenarios. These playbooks are regularly updated into the ActiveEye Platform to automate common response actions for low and medium threat events, enabling analysts to spend more time on alerts that benefit from deeper, human review.

Threat reports are generated as needed to support developments related to our clients and keep them informed. We communicate threats and current security issues during our account reviews and other conference call to keep our clients aware of any changes to the threat landscape. Any actionable intelligence gathered from research will be monitored and evaluated. Necessary actions will be incorporated into services provided to our clients, to include developing new signatures and other similar countermeasures to deal with emerging threats. Team Alphanumeric will develop threat reports as requested by the City and return these reports within 12 hours as reasonable.

2.1.9.4 Security System Support

Team Alphanumeric does not preform maintenance on equipment as part of its service offering. While we can definitely provide support for the monitoring aspect, performing changes on the systems themselves is not a capability that we have developed. In light of the scope of this contract, we could develop this specific capability, however as it stands now, we would not be able to provide this support at the beginning of service unless it were to fall to the personnel identified in 2.1.9.5 Onsite services described in the next section.

2.1.9.5 Onsite Services

Team Alphanumeric is prepared to provide two on-site personnel in the functions of a Tier 3 Infrastructure Security Engineer and a Tier 3 Cyber Security Analyst as listed in the RFP. Upon award of a contract, resumes of potential candidates will be provided when asked for the addition of these employees in support of the City. Team Alphanumeric will support the 16 hours monthly if information security engineering support in addition to the two positions described above.

2.1.9.6 Threat Hunting

Team Alphanumeric's threat hunting capability aim to find evidence of threats and intrusions on a customer's network that bypassed defender's detection efforts. Our team of Cyber Hunt specialists includes military veterans who conducted cyber defense and hunt activities as part of their service. Specifically, for Cyber Hunt capabilities, we are looking for specific indicators of compromise that pertain to Advanced Persistent Threats (APTs) that have eluded detection. APT detection, while are subject to the same indicators of compromise that we monitor for, depends on meaningful data to analyze and monitor for those modified signatures or for longstanding access in the system. Our team can develop specific Tactics, Techniques and Procedures (TTPs) specific to the City to identify likely threats gathered from our threat intelligence reporting to actively search City systems and flush out any anomalous behavior that is "low and slow" and likely to evade normal monitoring protocols.

2.1.9.7 Compromise Assessment

Team Alphanumeric's Compromise Assessment aims to find evidence of threats and intrusions on a network that bypassed defender's detection efforts. We use both manual and automated techniques, with our primary tool being Carbon Black Response. The Carbon Black solution allows us to monitor and record the activities occurring within the network by installing small sensors on a customer's endpoints, allowing Team Alphanumeric to:

- Automate data collection with continuous recording, centralization and retention of endpoint activity
- Create a system of record that dynamically models the complete kill chain
- Map attacks across the enterprise to scope the incident and determine root cause.
- Have the capability to isolate, terminate, remediate and ban endpoint threats

Our primary purpose is to collect key system data-points and analyze the results for indicators of compromise. Data

collected from endpoints includes processes, libraries, drivers, network connections, and memory artifacts. This information is then sent to high quality threat intelligence feeds, such as MITRE ATT&CK, AlienVault's Open Threat Exchange, and Carbon Black's Advanced Threat Feed for initial triage. These results are then analyzed and validated, to include having the raw data examined using big data analytical techniques.

Our manual examination includes, but is not limited to, a review of commonly misused tools (e.g. cmd.exe, powershell.exe, and net.exe), unwanted registry modifications, persistently installed software, and atypical parent-process relationships. The in-depth analysis and insight we provide through our Compromise Assessments goes beyond what most organizations can do themselves. We continually seek to improve our threat hunting capabilities and techniques as the industry evolves in order to detect the attackers that go undetected through routine cybersecurity tools and tactics.

Team Alphanumeric's compromise assessment approach involves the following stages:

1. Pre-Assessment Planning – Based on network architecture, needs, and other information provided by the County, Team Alphanumeric will determine the best methods to conduct the assessment and agree on Rules of Engagement to be followed.
2. Preparation of the Environment – The County will provide required access and install any required software.
3. Map the Network – Enumeration of network assets within assessment scope.
4. Assessment – Active survey of network assets for malware and intrusion indicators.
5. Analysis – Analysis of collected data and customer-provided data such as log files. During analysis phase, Team Alphanumeric may deploy deep inspection surveys to suspicious hosts on a targeted basis.
6. Report – Produce and deliver report and recommendations that include best practices that Orange County can use to improve their cybersecurity posture.

Team Alphanumeric will search for host and network indicators of compromise from all major operating systems (Windows, Mac OSX, and Linux). We will also assess artifacts from the deployed Carbon Black Enterprise Response and other available network devices, to form a comprehensive assessment. Team Alphanumeric will then analyze the collected digital artifacts for evidence of abnormal and suspicious activity. This methodology is able to discover malicious activity that avoided detection by traditional signature-based and host-based intrusion detection methods (e.g., antivirus).

All efforts to minimize impact to the network operations are made. During our assessment, some intense scan-types may have a noticeable performance impact on a system that could last up to 10 minutes and are only used on suspect systems identified with the wide-scope non-intrusive scans. Team Alphanumeric's Compromise Assessment looks for anomalous artifacts in the following locations:

- Host system memory
- Host file system
- Host network connections
- User accounts
- Security and infrastructure device logs

Our final report and outbrief will provide details on any findings, results of any scanning, any critical or high vulnerabilities that were discovered, and our observations related to observed practices on the network and/or systems. Remediation recommendations will be provided for any found threat actors.

2.1.9.8 Current Environment

Team Alphanumeric typically does not perform configuration changes as part of its service offering but will work with the City of Charlotte to identify tasks that may be conducted to improve efficiency towards are more effective response. The specific systems and tasks listed on the table in RFP section 3.16 are not overly difficult and could be

accomplished after specific platform training is completed and members are qualified to make changes. This is something that can be discussed, or our on-site personnel could get qualified to perform these activities and other team members added going forward. This is a capability we could add to our offering, but it would not be available at the start of the contract if awarded.

2.1.9.9 Total Log Volume

Log volume data is noted and has been used to price out storage requirements necessary to meet City log retention and access needs.

3. Section 6, Form 2, Addenda Receipt Confirmation

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 #:

**DATE ADDENDUM
DOWNLOADED FROM NC IPS:**

 Addendum #1

 6/28/2019

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

 Linda Herndon
(Please Print Name)

 7/11/2019
Date

 Linda Herndon
Authorized Signature

 Sr. VP Global Sales & Solutions
Title

 Alphanumeric Systems, Inc.
Company Name

4. Section 6, Form 3, Proposal Submission

This Proposal is submitted by:

Company Name: Alphanumeric Systems, Inc.

Representative (printed): Linda Herndon

Address: 4515 Falls of Neuse Rd. #250

City/State/Zip: Raleigh, NC 27609

Email address: lherndon@alphanumeric.com

Telephone: 919-781-7575

Facsimile: 919-872-1440

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.

Linda Herndon

Representative (signed): _____

5. Section 6, Form 4, Pricing Worksheet

| City of Charlotte | | | | | | |
|------------------------------------|--|-----------------------|-----------------------|-----------------------|------------------------------------|--|
| Security Operations Services | | | | | | |
| Team Alphanumeric Pricing | | | | | | |
| Description | | Year 1 - Monthly Cost | Year 2 - Monthly Cost | Year 3 - Monthly Cost | Option renewal year 1 Monthly Cost | Optional Renewal Year 2 - Monthly Cost |
| Implementation Fee One-Time Charge | | \$ 65,883.42 | N/A | N/A | N/A | N/A |
| 1.0 | Security Operations Services* | \$ 145,620.89 | \$ 148,223.48 | \$ 150,872.92 | \$ 153,570.04 | \$ 156,315.71 |
| 1.1 | Core Security Operations Security | \$ 50,209.13 | \$ 51,094.31 | \$ 51,995.42 | \$ 52,912.75 | \$ 53,846.59 |
| 1.2 | Analytics Platform Operations | \$ 5,082.35 | \$ 5,173.84 | \$ 5,266.96 | \$ 5,361.77 | \$ 5,458.28 |
| 1.3 | Email Threat Monitoring Program | \$ 15,882.35 | \$ 16,168.24 | \$ 16,459.26 | \$ 16,755.53 | \$ 17,057.13 |
| 1.4 | Cyber Intelligence Support | \$ 8,470.59 | \$ 8,623.06 | \$ 8,778.27 | \$ 8,936.28 | \$ 9,097.14 |
| 1.5 | Security System Support** | \$ - | \$ - | \$ - | \$ - | \$ - |
| 1.6 | Onsite Services | \$ 56,094.12 | \$ 57,103.81 | \$ 58,131.68 | \$ 59,178.05 | \$ 60,243.26 |
| 1.6.1 | Onsite Tier 3 Infrastructure Security Engineer | \$ 25,411.76 | \$ 25,869.18 | \$ 26,334.82 | \$ 26,808.85 | \$ 27,291.41 |
| 1.6.2 | Onsite Tier 3 Cyber Security Analyst | \$ 27,294.12 | \$ 27,785.41 | \$ 28,285.55 | \$ 28,794.69 | \$ 29,312.99 |
| 1.6.3 | 16 hours/month onsite information security engineering support | \$ 3,388.24 | \$ 3,449.22 | \$ 3,511.31 | \$ 3,574.51 | \$ 3,638.85 |
| 1.7 | Threat Hunting | \$ 8,470.59 | \$ 8,623.06 | \$ 8,778.27 | \$ 8,936.28 | \$ 9,097.14 |
| 1.8 | Compromise Assessment | \$ 1,411.76 | \$ 1,437.18 | \$ 1,463.05 | \$ 1,489.38 | \$ 1,516.19 |

**Security Operations Services is the total pricing for all SKU's that Team Alphanumeric will provide the City of Charlotte. A breakdown of each service and their associate cost can be found in the rate table above.*

***Team Alphanumeric does not make changes to client infrastructure but can consider making a change to this policy depending on discussions with the City of Charlotte as detailed in the response.*

6. Section 4, Form 5, MWSBE Utilization

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: | Alphanumeric Systems, Inc. |
|----------------------|----------------------------|

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):

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):

[Form continues on next page]

7. Section 6, Form 6, Company Background and Experience

| Question | Response |
|--|---|
| Company's legal name | Alphanumeric Systems, Inc. & Delta Risk LLC |
| Company Location (indicate corporate headquarters and location that will be providing the Services). | <p>Headquarters: 4515 Falls of Neuse Rd #250, Raleigh, NC 27609</p> <p>Managed Security Services Operations Center: 106 S. St. Mary's Street, Suite 601 San Antonio, TX 78205</p> <p>Secondary Security Operations at: 21355 Ridgetop Circle, Suite 350 Sterling, VA 20166</p> |
| How many years has your company been in business? How long has your company been providing the Services as described in Section 3? | <p>Alphanumeric has been in business serving the NC public sector for 40 years, since 1979. Delta Risk has been in business for 12 years, since 2007. We started off as a cybersecurity professional services company but added Managed Security Services in 2016 (3 years).</p> |
| 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). | <p>Alphanumeric has 160 active clients within the NC public sector. For managed security services, our primary customers have been in the commercial sector because we have not marketed extensively to the public sector. Starting in 2018, we began to market Managed Security Services to the public sector.</p> <p>Delta Risk provides service to over 70 ActiveEye Managed Security Service clients, with approximately 10 of them being public sector. Our public sector clients include the Tarrant River Water District, and we have recently added a contract with Manhattan and Associates that is of similar size and scope to the City of Charlotte. Delta Risk also supports the DoD CIO, the DoD Principal Cyber Advisor Office, the Defense Cyber Crime Center, and the Department of Homeland Security for a variety of professional services to include Risk and Vulnerability Assessment, Security Architecture Reviews, Threat Intelligence, Phishing Exercises, Strategy and Governance Consulting, and Continuous Monitoring Policy and Strategy Implementation.</p> |
| List any projects or services terminated by a government entity. Please disclose the government entity that terminated and explain the reason for the termination. | Alphanumeric nor Delta Risk have not had any services terminated by a government or any other public or private organization. |

| | |
|--|--|
| List any litigation that your company has been involved with during the past two (2) years for Services similar to those in this RFP. | None |
| Provide an overview and history of your company. | <p>Since 1979 Alphanumeric has helped our clients realize their vision by removing the friction from customer and employee experience. We provide global contact centers powered by talent and artificial intelligence, fully managed technology modernization, security, and support, and learning for onboarding, compliance, and transformation.</p> <p>Delta Risk was founded in 2007 by two retired Air Force officers and a former Chicago Board of Exchange trader to provide high end cybersecurity services to the Department of Defense and counter Advanced Persistent Threat consulting to commercial clients. Headquartered in San Antonio, TX.</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. | Alphanumeric is not a subsidiary. Delta Risk is a partner to Alphanumeric, but they are not a subsidiary. |
| Identify the percentage of revenue used for research and/or development by the proposing company or division. | Team Alphanumeric's research and development expenditures are ~14% of revenue is used toward Research and Development of the ActiveEye Platform and associated technologies. |
| 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. | Alphanumeric & Delta Risk have been partnered together since 2016 and have completed 10 cybersecurity engagements for the NC public sector within that time. |
| Describe your company's complete corporate structure, including any parent companies, subsidiaries, affiliates and other related entities. | Alphanumeric is the parent company for 9 other entities. |
| Describe the ownership structure of your company, including any significant or controlling equity holders. | Alphanumeric is owned by 5 individuals and 1 Trust. The majority owner has a 70% ownership interest. |
| Provide a management organization chart of your company's overall organization, including director and officer positions and names and the reporting structure. | <p>Alphanumeric: CEO – Randy Trice CIO – Jay Baucom Controller – Michelle McNally Sr. VP Global Solutions – Linda Herndon</p> <p>Delta Risk: CEO – Scott Kaine CFO and Managed Services VP – Jim Garner VP and General Manager of Operations – Fred Wainwright John Hawley – Vice President, Product Strategy</p> |

| | |
|--|---|
| | <p>Joseph Acosta – Director, Security Operation Center</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>Joseph Acosta Director, Security Operations Years of Experience: 13+ years Type of Experience: Experience with a wide range of security domains including governance, risk, compliance, physical, environmental, network, incident response, intrusion prevention, architecture and design. Experience in technical roles as well as leadership roles. Skill Set: Risk management, security consultation, design, supply chain, DLP, vulnerability management, web proxy.</p> <p>Shawn Ellerthorpe Director, Product Management Years of Experience: 20+ years Summary: Shawn Ellerthorpe is a Director with Delta Risk LLC. He is an information security leader with business and technical expertise in developing, enhancing and implementing Managed Security Services and providing reliable ongoing support to clients. He applies a unique combination of more than 20 years of experience in security leadership, security operations architecture, operational processes development and business experience to provide clients with effective and practical information security services.</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>Alphanumeric and Delta Risk have been working together since 2016, with broad experience between the teams that provides familiarity and understanding between our two companies and allows us to provide a seamless experience for our customers. As of today Alphanumeric and Delta Risk have completed 10 successful cybersecurity engagements with the NC public sector.</p> |
| <p>Explain how your organization ensures that personnel performing the Services are qualified and proficient.</p> | <p>Resumes of each subcontractor candidate are sent to Alphanumeric prior to contract execution for vetting and ensuring that the resources assigned have the necessary skillsets and certifications.</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>Alphanumeric has approximately 600 employees with our headquarters located in Raleigh, NC.</p> <p>Delta Risk has approximately 75 employees with about 40 employees at the primary SOC location in San Antonio, TX.</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>Team Alphanumeric uses Datawatch badges to secure all of its external entrances and has a separate badging lock for access to the SOC floor. Team Alpha umeric maintains its data in its Office365 cloud environment, with the majority of files being stored on either SharePoint or OneDrive. All data at rest is encrypted, to include use of Bitlocker on all company computers. We use a comply to connect system to ensure all systems connecting to Alphanumeric resources are up to date on patches and have the appropriate minimum level of security controls in order to connect. Hard copy information is limited, however all hard copies of sensitive data are maintained in locked cabinets inside Alphanumeric facilities. Electronic data is further protected from misuse and insider threats through our implementation of Controlled, Unclassified Information Security controls that we have in place. These controls include identifying PII, HIPAA and other restricted information on electronic files and limit the access to need to know. Access to files are also further restricted by group policies. We have download limits applied to all data stored in or environment that alerts when a user exceeds normal download size in a given time period. Team Alphanumeric employees use the ActiveEye platform to protect its network, as well as ActiveEye Cloud for our Office365 and AWS environments and associated SaaS applications used by the company. Team Alphanumeric recently underwent A SOC2 Certification overseen by BDO and was granted in July 2019</p> |

8. Section 6, Form 7, References

Reference #1

Name of Client: Manhattan Associates

Main Phone Number: 770-955-7070

Address: 300 Windy Ridge Parkway, Atlanta, GA 30339

Primary Contract: George Garza

Title: Director Security & Risk Cloud Operations

Contact Phone: (678) 597-6307

Contact Email: ggarza@manh.com

Service Dates: 4/30/18-Present

Summary & Scope of Project:

Team Alphanumeric provides ActiveEyeSM Managed Cybersecurity Services which combines people, process, and technologies to support the detection of threats within the Manhattan Associates's digital footprint by leveraging Team Alphanumeric's ActiveEye Infrastructure SecurityTM. With ActiveEyeSM, Manhattan Associates is able to transfer responsibility for the complex, time-consuming, and costly task of security event aggregation, monitoring, and analysis to a Team Alphanumeric as a security partner.

Team Alphanumeric also provides SOC-as-a-Service for Manhattan Associates. Team Alphanumeric's Security Operations Center (SOC) offers 24/7/365 monitoring by a U.S. based team of highly trained and experienced security analysts and engineers, who provide processes for deployment, operations, maintenance, tuning, monitoring and alerting.

Contract Value: \$556,000 **Number of Client Employees:** 3,000

Reference #2

Name of Client: Tarrant Water Regional Water District

Main Phone Number: 817-335-2491

Address: 800 E. Northside Drive, Fort Worth, TX 76102

Primary Contract: Todd Hatcher

Title: Cybersecurity Operations Manager

Contact Phone: 817-988-6830

Contact Email: Todd.hatcher@trwd.com

Service Dates: October 2017 - Present

Summary & Scope of Project:

Team Alphanumeric is currently providing the Tarrant River Water District (TRWD) Managed Security Detection, Prevention, and Incident Response Services in support of their cybersecurity support requirements. Team Alphanumeric is providing 24x7 support in via our ActiveEye Threat Monitoring platform. We are providing continuous security monitoring of the TRWD environment for perimeter and internal threats. Our solution is protecting their environment and monitoring and logging network devices, endpoints, and servers that are part of the critical network. On these monitored assets, Team Alphanumeric provides real time log aggregation, security analysis of traffic and logs, with monthly statistical reporting, and vulnerability scanning of the TRWD environment with support coming from our Security Operations Center in San Antonio, Texas.

Number of Client Employees: 1000

Reference #3

Name of Client: Texas Farm Bureau Insurance

Main Phone Number: 1-800-772-6535

Address: 7420 Fish Pond Road, Waco, TX 76710

Primary Contract: Shane Jensen

Contact Phone: 254-399-5091

Contact Email: sjensen@txfb-ins.com

Service Dates: December 2017 - Present

Summary & Scope of Project:

Team Alphanumeric provides 24x7 SOC monitoring for Texas Farm Bureau Insurance's network and assist them with detecting and responding to threats. Team Alphanumeric also manages, tunes, and updates the SIEM.

Number of Client Employees: 2,400

Reference #4

The below reference is for professional services, but directly related to the work that we would be doing under the project and demonstrates our knowledge of federal processes, finding vulnerabilities and recommending fix actions and securing information systems.

Name of Client: The Software Engineering Institute (SEI) - Please note SEI is an FFRDC and as such may only confirm that we do this work, but cannot comment any further.

Primary Contract: Debbie Spear

Contact Phone: 412-268-7742

Contact Email: daspear@sei.cmu.edu

Service Dates: September 2015 - Present

Summary & Scope of Project:

The Team Alphanumeric team has provided world class technical leads, penetration testers, and project managers in support of the SEI's contribution to the DHS RVA program. From 2017 - 2019, Team Alphanumeric has participated in RVAs supporting 80+ unique customers, to help determine operational and technical risk to their networks. Furthermore, Team Alphanumeric has provided technical leadership in the role of a "tech lead" to 19 of those risk assessments, with duties to include scoping, logistics, and technical accuracy and "safety" while on assessments, sometimes overseeing other contractor or government personnel.

Using Team Alphanumeric's expert skills in penetration testing, vulnerability assessments, and security consultant services, Team Alphanumeric provides thorough and extensive technical engagements and creates deliverables that are management oriented and tailored to the needs of the customer. RVAs serve not only as holistic assessments of network defense technologies in place but also as educational experiences which allows organizations to understand the current posture of their security infrastructure against modern day attacks and methodologies generated in a controlled manner some of the world's finest cyber security professionals. The results of RVAs are a full scope of awareness into any potential vulnerabilities in the client environment (based on testing type), a detailed metric by which to begin any required remediation or mitigation processes of vulnerabilities found, and a true understanding of the capabilities of security practices and mechanisms present in client enterprise environments.

Team Alphanumeric's RVA methodology exhibits real world tactics and procedures to provide federal and commercial entities a well-rounded and through cyber security assessment experience. Team Alphanumeric begins engagement by determining the approved platform for engagement execution and stays in touch with designated authorities and upper management. Next, housekeeping activities are conducted to determine how data will be stored, IP assignments, and review all Rules of Engagement (ROE) stipulations and clauses to assert full understanding of the task at hand. Scanning operations then ensure and are introduced against the target environment using a multitude of approved tools to discover points for potential network and service exploitation, entry, and vulnerability analysis. Social Engineering, if authorized, is the next step in RVA operations to test the "human" aspect of an enterprise's security awareness

program as well as aid in the determination as to how receptive users are to phishing campaigns. Subsequent to these events, exploitation measures are taken against vulnerable effects and if entries points have been successfully exploited, team members conduct post-exploitation measures such as dumping password hashes, browsing file systems of affected workstations and servers, and escalate privileges to display the breath of residual events that could occur as a result of the discovered vulnerabilities. After the assessment is complete, operators conduct an out-brief meeting to detail to the customer the results of the engagement. The final stage of our methodology, and often the most important, is reporting. In this phase, all data is encrypted and archived, and a report passed containing findings that are documented in a clear and understandable manner is sent to Contract Authority for review.

Team Alphanumeric follows the Department of Homeland Security's Rules of Engagement (ROE) with each RVA undertaken. No formal "penetration testing" methodology is followed, and no open source or published standard is met throughout the execution of the RVA. Each ROE is custom to each client and contains information such as scope, working hours, and "off limits" systems, each tester is chartered to stay within the bounds of the ROE, and any violations of the ROE could potentially be met with de-certification of the penetration tester.

Team Alphanumeric's Risk and Vulnerability Assessments (RVA) Team conducts assessments of enterprises across a broad client base exposing them to a vast array of technologies and enterprise devices. The RVA Team's primary task is to conduct assessments in search of threats and vulnerabilities that may be present in target environments, determine the level of risk any found vulnerabilities pose to these environments, and provide mitigation strategies and countermeasures to help reduce or eliminate discovered threats. The RVA Team offers a variety of services (including, but not limited to): Network Mapping, Vulnerability Scanning, Phishing Assessments, Wireless Assessments, Web Application Assessments, Operating System Security (OSSA) Assessments, and Database Assessments. Operators within this team are experts in the Offensive Security discipline and are proficient in executing complex and high caliber assessments with skills from a variety of past performances and experience. Operators of this team understand traffic analysis and protocols, system and application threats, understand Public Key Infrastructure (PKI) and network access, identity and management systems, network architectures and topology analysis, and maintain Confidentiality, Integrity and Availability throughout proposed engagements. Finally, the RVA Team ensures protection of data received during engagements and provides clients with robust reports that give network defenders a comprehensive look into how a malicious adversary could exploit discovered vulnerabilities to cause harm to the client organization. As the RVA Team assesses a multitude of both federal, commercial and private entities, operators always remain current with attack methodologies, vulnerability analysis techniques, social engineering techniques, and Computer Network Defense audit and compliance policies.

Contract Value: \$1,600,000

9. Section 6, Form 8, Additional Company Questions

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

Upon award notification, Team Alphanumeric will begin transition activity, beginning with the stand-up of the managed transition team, led by the Alphanumeric Program Manager. The transition team will consist the Charlotte Account SOC lead, a security engineer, and our Solutions Architect. This team will begin work with the City of Charlotte to schedule a kickoff meeting within two weeks of award.

The Alphanumeric Program Manager and the transition team will develop a Transition Management Plan that will detail activities to occur from Day 1 until SOC services are completely cutover to Team Alphanumeric. This plan will focus on setting up the monitoring services as required and develop procedures for cutting over monitoring services while maintaining coverage throughout the process. We will work with the incumbent provider to develop a plan that fits within the transition period. The plan will be developed in conjunction with City of Charlotte personnel for proper oversight.

During this transition, Team Alphanumeric will also work through on-boarding requirements, such as submitting paperwork and documentation and setting up required interviews for employees requiring elevated access. We will establish regular transition update meetings to keep the entire team aware of progress and then transition these meetings into the regular weekly and monthly update meetings as directed in the reporting requirements.

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

This is a high-level project plan that details our normal process integrated in with the transition of services from the City's incumbent Managed Security Provider. Our Deployment process is also detailed below to describe the steps we take

Phase 1: Information Exchange

Team Alphanumeric Deliverables: Team Alphanumeric will schedule a service kick-off meeting with customer representative(s) and provide information-gathering documents to the customer within one week of contract signature. The kick-off meeting will be conducted at the earliest mutually available opportunity.

Phase 2: Infrastructure Readiness and Process Development

Team Alphanumeric Deliverables: Team Alphanumeric will provide detailed requirements regarding customer infrastructure preparation actions and work with established POCs to identify target devices to monitor and validate infrastructure requirement and architecture for monitoring. Our analysts will begin tailoring checklists and procedures to the customer's requirements, processes and architecture.

Phase 3: System Build and Deployment

Team Alphanumeric Deliverables: Team Alphanumeric will provision tools in accordance with requirements of the SOW, and consistent with information gathered in phases 1 and 2. Team Alphanumeric will also provide detailed requirements regarding customer deployment actions.

Phase 4: Monitoring Turn Up

Team Alphanumeric Deliverables: Team Alphanumeric will monitor the service for all in scope assets which are generating events. Team Alphanumeric will begin monitoring any properly connected in-scope sources after the initial tuning period.

Phase 5: Tuning/Report Setup

Team Alphanumeric Deliverables: Team Alphanumeric will conduct initial tuning of the events and alarms in the service, as well as set up initial reports, within two weeks of events flowing into the service.

| City of Charlotte Managed Service Support Transition | Month 1 | | | | Month 2 | | | | Month 3 | | | |
|--|---------|---|---|---|---------|---|---|---|---------|---|---|---|
| | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| Kick off Meeting City of Charlotte and Team Alphanumeric Leadership & Key Personnel | █ | | | | | | | | | | | |
| Information Gathering Matt McTigue; Solutions Architect Sean Ellerbe; Engineer City of Charlotte Primary Account Analyst Macie Thompspon; Incident Response Lead | █ | █ | █ | | | | | | | | | |
| Infrastructure Readiness Matt McTigue; Solutions Architect Sean Ellerbe; Engineer | | █ | █ | | | | | | | | | |
| System Build Matt McTigue; Solutions Architect Sean Ellerbe; Engineer | | █ | █ | █ | | | | | | | | |
| Process Development City of Charlotte Primary Account Analyst City of Charlotte Alternate Account Analyst Macie Thompspon; Incident Response Lead | | █ | █ | █ | █ | █ | █ | | | | | |
| System Deployment Matt McTigue; Solutions Architect Sean Ellerbe; Engineer | | | █ | █ | █ | | | | | | | |
| Monitoring Turn Up Matt McTigue; Solutions Architect Sean Ellerbe; Engineer | | | | █ | █ | █ | | | | | | |
| Monitoring Cut Over | | | | | | █ | | | | | | |
| Event/Alarm Tuning and Report Setup Matt McTigue; Solutions Architect Sean Ellerbe; Engineer | | | | | █ | █ | █ | █ | █ | █ | █ | █ |

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

Team Alphanumeric will maintain an open line of communication with the City of Charlotte and will maintain oversight with our teaming partners. Our project manager and SOC team lead(s) will supervise all personnel to ensure delivery of required work products and serve as the conduit for all communications between city officials and the Team Alphanumeric team. Our team can use a variety of platform to keep in communication. Email is the primary communication method to use for normal operations, however we also utilize a number of messaging platforms that can facilitate information exchange, to include Microsoft Teams and Slack. Our ActiveEye Portal also provides a central hub for all information related to the City of Charlotte Environment, with a dashboard providing current metrics and access to open tickets. Phone calls are also effective to

convey deeper information or critical information. We understand that simply firing a text or an email does not equate to positive contact. Actually getting a response from our client means that our message was received, and we want to make sure that for critical communications that our message was not just received, but also understood. This is critical to establishing trust with our clients and enables us to provide service our customers deserve.

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

The primary risk in this project is ensuring there is not loss or degradation in service during the cutover of monitoring services. The main way to mitigate this risk is through careful monitoring of the transition period with communication channels with the City and with the incumbent set up to facilitate easy and open discussions as needed to resolve issues and to have a simple cutover service that is effective and minimizes overlapping service. This risk is addressed in our transition plan, with effective communication with the city and the incumbent being critical to mitigating this risk.

The variability in services required is also a risk for this contract, looking specifically at the number of events, emails or other issues that may need to be addressed simultaneously. Our Managed Security service scales to address surges in client requirements so that we can meet all our client needs. Additionally, we have the ability to rapidly staff up if required through use of our internal professional services cadre to meet contingency requirements for client facing a significant incident to provide more in-depth service while maintaining support for our other customers.

10. Section 6, Form 9, Certification Regarding Debarment, Suspension and Other Responsibility Matters

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:

| | |
|--|---|
| <p>Linda Herndon _____ (Print Name)</p> <p>Sr. VP Global Sales & Solutions _____ Title</p> | <p><i>Linda Herndon</i> _____ Signature</p> <p>7/11/2019 _____ Date</p> |
|--|---|

11. Section 6, Form 10, Byrd Anti-Lobbying Certification

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.

Alphanumeric Systems, Inc. (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.

Linda Herndon
(Print Name)

Linda Herndon
Authorized Signature

7/11/2019
Date

Alphanumeric Systems, Inc.
Company Name

4515 Falls of Neuse Rd. #250
Address

Raleigh, NC 27609
City/State/Zip

5. Section 6, Form 4, Pricing Worksheet

| City of Charlotte | | | | | | |
|--|--|-----------------------|-----------------------|-----------------------|------------------------------------|--|
| Security Operations Services | | | | | | |
| Team Alphanumeric Pricing – BAFO submitted 8/28/2019 | | | | | | |
| Description | | Year 1 - Monthly Cost | Year 2 - Monthly Cost | Year 3 - Monthly Cost | Option renewal year 1 Monthly Cost | Optional Renewal Year 2 - Monthly Cost |
| Implementation Fee One-Time Charge | | \$65,500.00 | N/A | N/A | N/A | N/A |
| 1.0 | Security Operations Services* | \$137,885.88 | \$140,367.83 | \$142,894.45 | \$145,466.55 | \$148,084.95 |
| 1.1 | Core Security Operations Security | \$46,717.65 | \$47,558.56 | \$48,414.62 | \$49,286.08 | \$50,173.23 |
| 1.2 | Analytics Platform Operations | \$4,828.24 | \$4,915.14 | \$5,003.62 | \$5,093.68 | \$5,185.37 |
| 1.3 | Email Threat Monitoring Program | \$15,088.24 | \$15,359.82 | \$15,636.30 | \$15,917.75 | \$16,204.27 |
| 1.4 | Cyber Intelligence Support | \$8,047.06 | \$8,191.91 | \$8,339.36 | \$8,489.47 | \$8,642.28 |
| 1.5 | Security System Support** | 0** | 0** | 0** | 0** | 0** |
| 1.6 | Onsite Services | \$53,816.47 | \$54,785.17 | \$55,771.30 | \$56,775.18 | \$57,797.14 |
| 1.6.1 | Onsite Tier 3 Infrastructure Security Engineer | \$24,395.29 | \$24,834.41 | \$25,281.43 | \$25,736.49 | \$26,199.75 |
| 1.6.2 | Onsite Tier 3 Cyber Security Analyst | \$26,202.35 | \$26,674.00 | \$27,154.13 | \$27,642.90 | \$28,140.47 |
| 1.6.3 | 16 hours/month onsite information security engineering support | \$3,218.82 | \$3,276.76 | \$3,335.74 | \$3,395.79 | \$3,456.91 |
| 1.7 | Threat Hunting | \$8,047.06 | \$8,191.91 | \$8,339.36 | \$8,489.47 | \$8,642.28 |
| 1.8 | Compromise Assessment | \$1,341.18 | \$1,365.32 | \$1,389.89 | \$1,414.91 | \$1,440.38 |

***Security Operations Services is the total pricing for all SKU's that Team Alphanumeric will provide the City of Charlotte. A breakdown of each service and its associated cost can be found in the rate table above.**

****Not included in solution at this time, but can be proposed separately (or during NOC re-bid?)**



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.

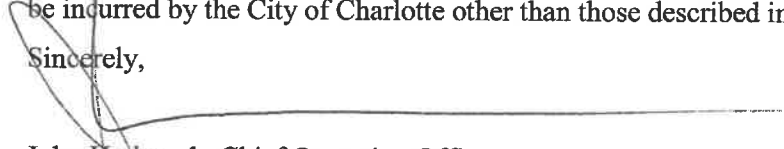
As a comprehensive solution, fulfilling both the core and additional service requirements, R9B offers our Threat Intelligence-led Managed Detection and Response (MDR) service. The key differentiator to other providers is the inclusion of Threat Intelligence as an integral component of the service and 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]



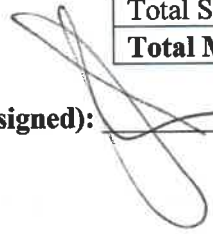


List below all **MWSBEs** that you intend to subcontract to while performing the Services:

| 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> |



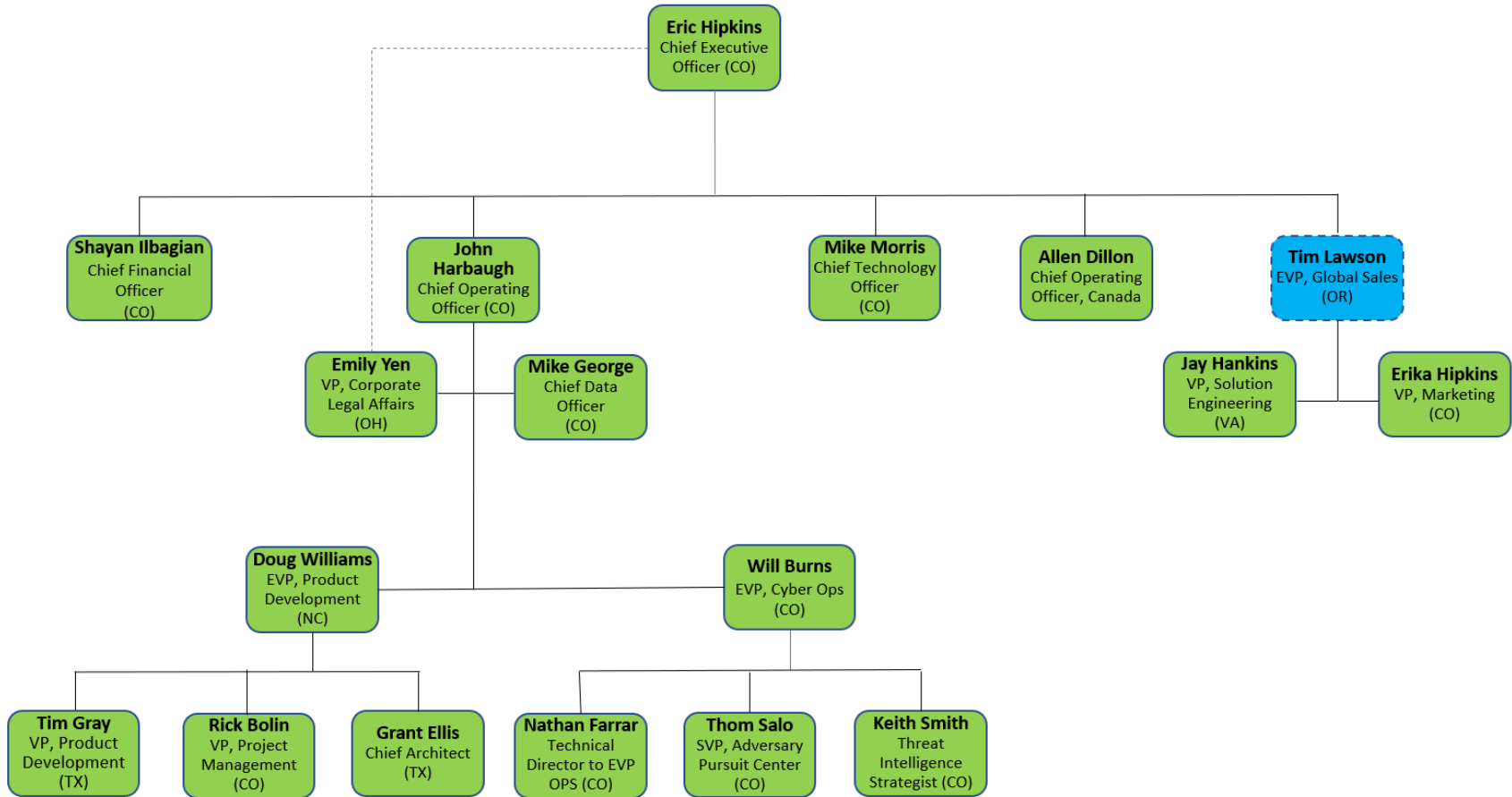
| | |
|---|--|
| | <p>innovative approach to the challenges faced in cybersecurity. R9B’s product development and managed cybersecurity services are differentiated by integrating Threat Intelligence and client relevant business context into all aspects of our mission directed approach. We maintain dedicated 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

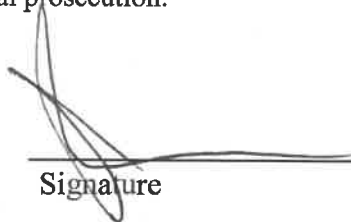
The bidder, contractor, or subcontractor, as appropriate, certifies to the best of its knowledge and belief that neither it nor any of its officers, directors, or managers who will be working under the Contract, or persons or entities holding a greater than 10% equity interest in it (collectively “Principals”):

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)

[Signature]
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 |

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

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 | \$ 108,230.18 | \$ 110,157.72 | \$ 112,881.86 | \$ 115,787.06 | \$ 118,767.55 |
| 1.1 | Core Security Operations Services | \$ 42,355.36 | \$ 43,414.25 | \$ 44,499.60 | \$ 45,612.09 | \$ 46,752.39 |
| 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 \$11,060.04 | \$ 11,335.92 | \$ 11,619.36 | \$ 11,910.42 | \$ 12,208.02 |
| 1.3 | Email Threat Monitoring and Analysis | \$ 3,594.25 | \$ 3,656.65 | \$ 3,720.85 | \$ 3,841.24 | \$ 3,965.86 |
| 1.4 | Cyber Intelligence Support | \$ 5,007.80 | \$ 5,101.70 | \$ 5,198.00 | \$ 5,359.20 | \$ 5,526.23 |
| 1.5 | Security System Support | \$ 8,655.60 | \$ 8,872.20 | \$ 9,093.60 | \$ 9,321.00 | \$ 9,554.40 |
| 1.6 | Onsite Services | | | | | |
| 1.6.1 | Onsite Tier 3 Infrastructure Security Engineer | \$ 16,390.90 | \$ 16,429.20 | \$ 16,840.80 | \$ 17,260.80 | \$ 17,692.80 |
| 1.6.2 | Onsite Tier 3 Cyber Security Analyst | \$ 13,185.70 | \$ 13,143.60 | \$ 13,472.40 | \$ 13,809.60 | \$ 14,154.00 |
| 1.6.3 | 16 hours/month onsite information security engineering support | \$ 2,379.51 | \$ 2,463.03 | \$ 2,552.77 | \$ 2,641.08 | \$ 2,731.23 |
| 1.7 | Threat Hunting | \$ 4,327.80 | \$ 4,436.10 | \$ 4,546.80 | \$ 4,660.50 | \$ 4,777.20 |
| 1.8 | Compromise Assessment | \$ 1,273.22 | \$ 1,305.08 | \$ 1,337.68 | \$ 1,371.13 | \$ 1,405.43 |

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 |



CenturyLink Response to

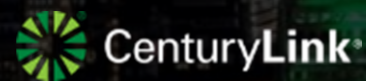
City of Charlotte

Request for Proposal for

Managed Security Services

RFP # 269-2019-109

July 15, 2019



COPY

Legal Statement

CenturyLink is excited to discuss this opportunity with the City and how CenturyLink may provide products and services that help strengthen your businesses and connect you to the power of the digital world. CenturyLink is committed to delivering product and service offerings that meet the personal and business communications needs of our customers. CenturyLink thanks the City for the opportunity to respond and to propose services to the City.

Informational Purposes Only

CenturyLink has endeavored to provide responses as requested by the RFP, but as contemplated by RFP Section 1.6.1, our response is not intended to create a binding contractual commitment between the parties without further discussions as to the final solution and information exchanged during discussions between the parties. In accordance with Sections 1.6.12 and 4.1.4 of the RFP, CenturyLink has documented its proposed exceptions to the RFP as specifically set forth in this response. Therefore, regardless of any condition contained within the RFP, including but not limited to CenturyLink's signature to its submission, the responses are informational only and are provided for the City's evaluation. If the City awards this bid to CenturyLink, the City is deemed to have acknowledged CenturyLink's responses and agrees to negotiate in good faith a mutually acceptable agreement.

Contract and Service Terms

In accordance with Sections 1.6.12 and 4.1.4 of the RFP, CenturyLink respectfully takes exception to the City's Sample Contract at this time and offers the services subject to its standard agreement, service attachments, service exhibits, and SLAs attached to this bid response (the "CenturyLink Contract"). As required, CenturyLink has provided specific exceptions to the RFP terms and conditions and the City's Sample Agreement identified herein. CenturyLink understands the City may require the inclusion of certain terms and conditions from the RFP and use of the Sample Contract in the resultant Agreement and agrees to negotiate in good faith a mutually beneficial agreement adequately addressing both parties' needs. CenturyLink is confident we will reach a mutually beneficial agreement, but if for any reason the parties are unable to reach an agreement, CenturyLink respectfully reserves the right to decline the award without penalty.

The terms and conditions for the Enhanced Cybersecurity Service (ECS) must be negotiated separately and outside of the terms of this RFP. ECS is a service that requires specific terms due to its relationship with the Dept of Homeland Security.

Affiliated Companies

CenturyLink services are provided through affiliated companies. The CenturyLink Contract and/or the applicable Service Exhibits attached thereto will identify the legal CenturyLink affiliate providing the services.

Critical 9-1-1 Circuits

The parties acknowledge that the Federal Communications Commission's reliability rules mandate the identification and tagging of any circuits or equivalent data paths ("Transport Services") to public safety answering points that are used to transport 9-1-1 calls and information ("9-1-1 Data"). Customer agrees to cooperate with CenturyLink regarding compliance with these rules and will notify CenturyLink of all Transport Services used for 9-1-1 Data that Customer purchases under this Agreement.

Insurance

CenturyLink purchases sufficient insurance limits to protect the company from risks and liabilities associated with providing its commercial services and products. CenturyLink's standard coverage is in accordance with generally accepted industry standards for the type services and/or work proposed. CenturyLink's Memorandum of Insurance is available at www.centurylink.com/moi.

Confidentiality

CenturyLink's proposal may contain CenturyLink trademarks, trade secrets, and other proprietary information and may not be disclosed to a third party without the prior written consent of CenturyLink. CenturyLink acknowledges that the proposal may be subject to disclosure in whole or in part under applicable freedom of information, open records, or sunshine laws and regulations (collectively, "FOI"). CenturyLink requests that customer provide CenturyLink with prompt notice of any intended disclosures, including copies of copies of applicable FOI for review, and an appropriate opportunity to seek protection of CenturyLink confidential and proprietary information consistent with all applicable laws and regulations.

Table of Contents

| | |
|---|----|
| Legal Statement | i |
| B. Proposed Solution | 1 |
| C. Addenda Receipt Confirmation | 45 |
| D. Proposal Submission..... | 47 |
| E. Pricing Worksheet | 50 |
| F. MWSBE Utilization..... | 52 |
| G. Company’s Background Response | 55 |
| H. References | 67 |
| I. Additional Company Questions..... | 71 |
| J. Certification Regarding Debarment, Suspension and Other Responsibility Matters | 75 |
| K. Byrd Anti-Lobbying Certification | 77 |
| L. Exceptions to the Remainder of the RFP, including Sample Contract in Section 7 | 79 |

CenturyLink Attachments

| | |
|--------------|--|
| Attachment A | R041265 City of Charlotte MSA 7.10.19 |
| Attachment B | Form 8 Supplement Sample Security Log Monitoring Project |
| Attachment C | Form 8 Supplement Sample Monitoring and Management Project |



July 12, 2019

City of Charlotte
600 East Fourth St.
Charlotte, NC 28202

Greetings:

Based on a thorough assessment of your Request for Proposal # 269-2019-109 for Managed Security Services, CenturyLink is proud to submit the following response for your evaluation. CenturyLink has made every effort to respond with accurate and relevant information to your request.

Based on your RFP you are seeking Managed Security Services in the following areas:

- Security Operations Services
- Application Performance Monitoring
- Network Operations Center

The CenturyLink solution proposal consists of primarily of remotely delivered services for security log monitoring, application performance monitoring, and network operations. The solution is strengthened by staffing key positions onsite and we support the Charlotte Business INClusion program with MWSBE subcontracting. Aside from small exceptions, CenturyLink has fully complied with the requirements of the RFP.

You have our commitment to ensure that the highest attention to accuracy, quality, and performance are provided on an ongoing basis. CenturyLink is committed to focusing on every aspect of our business relationship with you and to ensure that we are here to support you with innovative technology solutions for your business operations, both now and in the future.

We hope that you find that this response provides all the necessary information you need to accurately evaluate our solutions, but feel free to reach out to me should you have any questions. We look forward to working with you to provide the highest standard of service and security needed for your business requirements.

Best Regards,

A handwritten signature in blue ink, appearing to read "Rob Robinson".

Rob Robinson

NC SLED Account Manager, on behalf of Dennis Fisher, Director, Pricing and Offer Management

CenturyLink
State, Local, Educations Division
11006 Rushmore Dr, Suite 200
Charlotte, NC 28227
704-213-4113

Rob.Robinson@CenturyLink.com
www.centurylink.com

B. Proposed Solution

Given the purpose of this Project and the City's goals as stated in this RFP, provide a creative solution to meet such goals. For each component of the Project described in Section 3, state whether and how your Proposed Solution complies as well as any additional information requested. If you wish to add supplemental information, it shall be labeled "Supplemental Information."

3. SCOPE OF MANAGED SECURITY SERVICES.

3.1. General Scope.

This scope is broken into the following three parts: 1) Security Operations Services; 2) Application Performance Monitoring; and 3) Network Operation Center ("NOC"). Service Providers may choose to propose on any or all of the parts.

While the City is flexible with respect to certain elements of the Managed Security Services, the City has specific requirements and preferences for the Service delivery method.

CenturyLink Proposed Solution

CenturyLink is pleased to offer the solution described in the following pages in response to the City's RFP for Managed Security Services.

We understand the complexity and magnitude of the security challenges and risks that face organizations, such as the City of Charlotte. CenturyLink is an experienced security services provider that utilizes advanced information security solutions to deliver outstanding protection of your environment. The CenturyLink solution will improve your network cyber security, strengthen governance, and support regulatory compliance.

In these few pages that follow, we will describe the solution for the three parts of scope: 1) Security Operations Services; 2) Application Performance Monitoring; and 3) Network Operation Center .

CenturyLink will deploy a highly experienced team that will draw upon a deep base of intellectual capital, including proven processes, and a rich tool set to satisfy the City's objectives.

CenturyLink – Who We Are

CenturyLink (NYSE: CTL) is a U.S.-based company with headquarters in Monroe, Louisiana. CenturyLink is a global communications and IT services company focused on connecting its customers to the power of the digital world. Our offerings include network and data systems management, big data analytics, managed security services, hosting, cloud, and IT consulting services in support of clients ranging from large-scale commercial and governmental organizations to mid-market firms and smaller government entities. CenturyLink provides services across the U.S., Europe, and Asia.

- Annual revenue of approximately \$23.5 billion
- Approximately 45,000 employees
- Number 132 of the 2019 Fortune 500
- Serves 98% of the Fortune 500 and 500 state and local government customers
- 33,000 business and government clients
- One of the two largest telecommunication companies in the U.S.

- Proprietary networks that carry 20% of the world's Internet traffic
- Own and operate 450,000 U.S. fiber route miles

Awards and Accolades

- CenturyLink is listed on Forbes Magazine's Best Places to Work for New Graduates – 2018
- Named one of Barron's Top 100 Sustainable Companies for 2018
- CenturyLink is an AWS Managed Service Provider Partner
- CenturyLink is a Microsoft Azure Expert Managed Service Provider (MSP)
- Named an authorized commercial ISP by The Quilt, a national coalition of non-profit U.S. regional research and education networks
- Repeat winner of Several Metro Ethernet Forum (MEF) Awards 2017/18
- Winner of HPE 2019 Global Service Provider of the Year Award
- Winner of two Business Connectivity Service Provider Excellence awards from ATLANTIC-ACM for delivering high-quality customer service and value 2017/18
- Winner of the Frost & Sullivan 2018 Product Leadership Award for innovative Cloud Application Manager hybrid cloud management platform

For more information: <http://news.centurylink.com/international-awards>.

Localized, Dedicated Account Team Support

CenturyLink has a dedicated local account team with a commitment to build and maintain a long and mutually beneficial relationship with the City of Charlotte. Our core account team has extensive experience in the industry and a track record of successfully assisting clients in obtaining their objectives.

The CenturyLink City of Charlotte account team is led by Rob Robinson, a Charlotte-born North Carolinian. Rob is a State & Local Government Account Manager, with three-plus decades of technology experience, including with 911 services in North Carolina. Keefe Leiter provides Sales Engineering support and has extensive experience in enterprise and government. Our team prides itself in being customer-focused, responsive, and a trusted partner to every customer served. Our customer service commitment is embraced by our executive team and every person in our company.

CenturyLink is confident the solution set forth in this proposal offers high value to the City of Charlotte's leadership team, IT organization, other stakeholders, and especially the citizens and voters of the Queen City by satisfying your managed security requirements at a competitive price.

Part 1 – Security Operations Services

"We see more, so we can stop more." Monitoring over 114 billion NetFlow sessions each day, CenturyLink securely connects, proactively monitors and effectively defends against constantly evolving security threats.

You take care of business. We'll keep it secure. CenturyLink's Black Lotus Labs analyzes traffic on CenturyLink's global enterprise network, delivering deep intelligence, and insights to help secure your data and business through CenturyLink's portfolio of security services.

Measurements of CenturyLink's success include:

- 400K+ cyber-attacks halted each month
- \$1B+ on pace to prevent \$1B in cybercrime this year
- 1.3B+ security events monitored daily

See the whole story here: <https://www.centurylink.com/asset/business/enterprise/report/2018-threat-research-report.pdf>

CenturyLink is helping spearhead the fight against cyber intrusions into the IT systems of government agencies and enterprise organizations. CenturyLink's extensive work in the cyber security space has led it to form a valuable relationship with a powerful ally in the nation's struggle against cybercrime. Improving the City's security posture will mitigate risk to the citizens of the City of Charlotte, and the various stakeholders within the City government including the various departments. The City will enhance its information security posture by contracting with CenturyLink.

With over 20 years of experience in cyber security, CenturyLink has recognized by industry analysts, including Gartner Group and Forrester Research, as an innovator and leader. CenturyLink's corporate security leaders participate on several private and public boards focused on IT cyber security.

CenturyLink is an original Commercial Service Provider (CSP) participating in the Department of Homeland Security's Enhanced Cybersecurity Services (ECS) program providing protections to US-based public and private entities.

CenturyLink Security Operation Centers, SOCs, currently support over 1,500 customers and have industry-leading experience supporting and managing complex environments. We have over 400 certified security team members.

Security Operations Centers and Security Log Monitoring

CenturyLink has two U.S.-based Security Operations Centers that would be used to support the City:

- Santa Clara, CA
- St Louis, MO

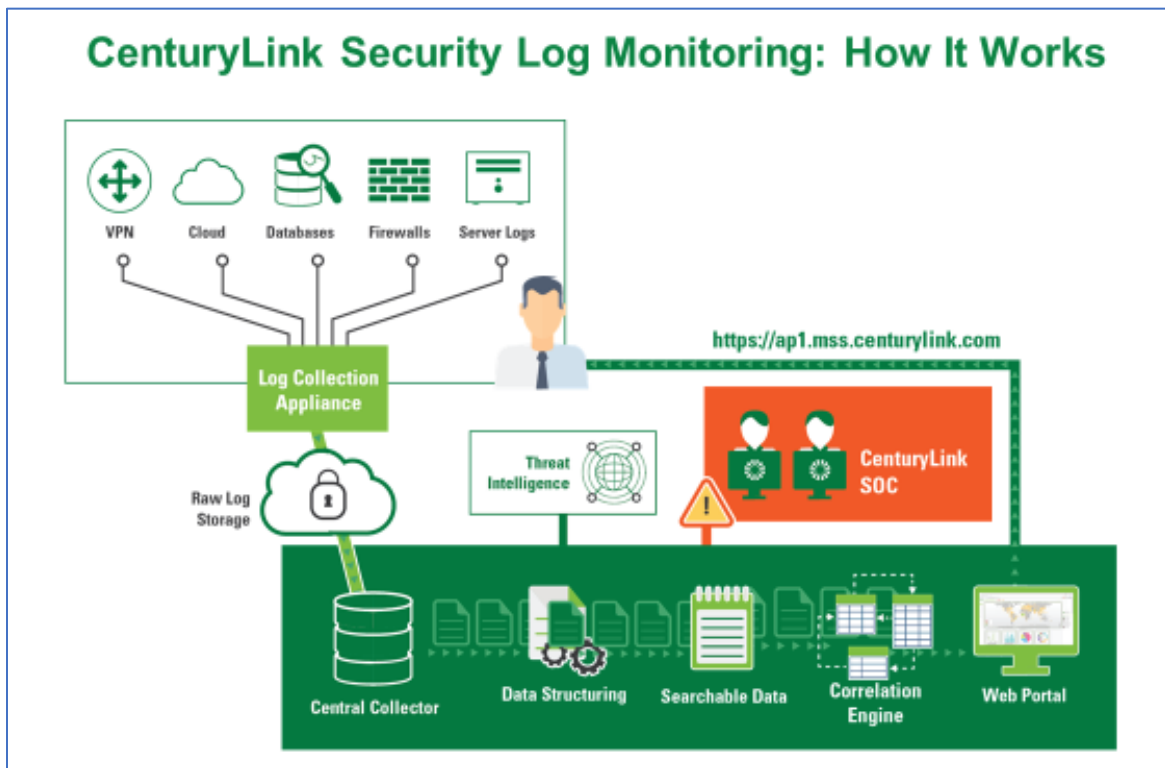
CenturyLink's Security Log Monitoring is a 24/7/365, customizable service that enables rapid detection and response to security threats. The CenturyLink Security Log Monitoring platform identifies indicators of compromise within your logs or security events and adds deeper context, generating leads by

correlating with proprietary and third-party threat intelligence to form cases for either the SOC staff or City team to investigate and escalate as warranted.

CenturyLink's Security Log Monitoring is a cloud-based offering of a network of Security Operation Centers and teams of security engineers and analysts. It uses an on-premise Log Collector Appliance to collect your system and application logs, and then encrypt and transmit the data.

We offer this service so that our customers can focus on their core business functions and keep the expense of security and compliance within a predictable budget.

Approximately 45 Security Engineers support three shifts 24/7/365 at each U.S.-based SOC. 100% of SOC staff have security certifications. Most prevalent are CISSP, CISA, SANS GCIA/GMON/GPPA, CCNA Security, CCDA, and CCSK. CISSP is typically the initial achievement.



The ratio of monitored and managed security devices to technical SOC staff varies according to the specific requirements of the customer and the complexity of devices supported. Additionally, the amount of automation embedded in the processes and software, of which CenturyLink has a significant amount, enables the CenturyLink SOC staff to provide a higher quality, more responsive service than service providers with a primarily labor-based solution.

The CenturyLink network of SOCs is configured to enable failover in the event of the loss of an individual SOC. This enables high availability and disaster recovery.

Log data will be collected by the CenturyLink Log Collector Appliance, which will reside with the City's network, and data will be continuously transmitted to the CenturyLink cloud-based Security Log

Monitoring (SLM) solution for analysis and action. The service is priced by average daily rate of log data ingested, i.e., per GB. We have used the number provided in the RFP as the basis of pricing. Logs will be stored for 90 days. Storage beyond 90 days is available as an option.

The CenturyLink Security Log Monitoring platform begins by establishing rules that generate what experience tells us to be meaningful. We identify indicators of compromise and other items of interest from your logs and add context from proprietary and third-party threat intelligence sources to add fidelity to the information, forming clues into leads. Algorithms prioritize leads for further investigation and determine which events require human investigation. Our Tier 2 and Tier 3 SOC analysts will follow your escalation procedures to share investigations with the City.

CenturyLink uses proprietary (custom developed) software that is integrated with the open-source Elasticsearch, Syslog-NG, and Kibana and other commercial tools. CenturyLink provides multiple methods of analysis that reflect industry best practices while maintaining flexibility and adaptability.

CenturyLink offers Cloud Security Monitoring as an additional feature of SLM. This would enable the City to extend SLM protection to AWS, Azure, and other private clouds.

Threat Intelligence

The primary threat intelligence source that will be used to support the City is CenturyLink's Black Lotus Labs. CenturyLink's Black Lotus Labs collects threat intelligence information by monitoring traffic on the CenturyLink network, which supports a large percentage of the world's internet traffic. Black Lotus Labs performs NetFlow and DNS analysis; correlates traffic via deep data mining against malicious actors, C2's, public threat repositories (Homeland Security, FBI); curates to minimize duplicates and stale information; and generates real-time alerts for high risk events.

Threat research is performed by CenturyLink's Black Lotus Labs. The mission of Black Lotus Labs is to leverage CenturyLink's network visibility to help protect customers and keep the internet clean. Among the ways Black Lotus Labs does this is by tracking and disrupting Command and Control servers (C2's or malicious hosts). Black Lotus Labs keeps track of 5000 C2's daily: "No ifs, ands, or bots!"

Data regarding C2's is part of the threat intelligence feed CenturyLink will use in the correlation process to identify malicious hosts.

Portal

A portal ("MSS Portal") is a standard feature of the proposed SLM offering. The MSS Portal provides a full set of standard reports, which in most cases prove fully adequate. Customized reports can be created using the MSS Portal's ad hoc reporting capability.

The MSS Portal is available to the City using role-based access control. This is the same portal that the CenturyLink SOC analysts use. A sample screenshot is included in the "Additional Information" area. The MSS Portal is also available as a mobile application.

The MSS portal dashboard may be customized for users based on role-based access. Raw log data may be viewed.

Incident Response

As part of implementation, the CenturyLink SOC team will work with the City to define severity levels according to the nature of the threat and create tailored response plans.

CenturyLink's primary offering for immediate mitigation capability to identified threats is our Incident Management and Response Service. On a contingent basis a team of veteran experts will be positioned to assist the City when the need arises.

Implementation

The estimate for implementation is 30-60 days assuming adequate support from the City. Deployment of CenturyLink's SLM has four phases, the first three of which are considered implementation.

- 1) Onboarding - installation of the Log Collector Appliance; performed in as little one day.
- 2) Log Source Configuration - configure log sources to appliance; typically, 1-2 weeks.
- 3) Tuning/Parsing/Rule Deployment - regular calls to review logs, rules, ingestion rates and structure; performed over a few weeks.
- 4) Ongoing SOC support.

Staffing

CenturyLink will also provide a dedicated Security Account Manager (SAM) to the City. He or she will be your subject matter expert and interface into the CenturyLink security organization.

CenturyLink will utilize MWSBE subcontractors with the requisite experience and skill to provide onsite services.

Compliance with Specific Requirements

Later in this response we indicate our compliance (or exception) to the individual requirements. CenturyLink proposes one exception: Incident Risk Level of Critical with Notification to Within 5 minutes. In our experience, 5 minutes is an inadequate amount of time to detect, route to an analyst, quickly evaluate, and react to a suspected event without generating an excessive number of false positives. Industry standard for this target is 15 minutes and that is what CenturyLink proposes. CenturyLink proposes the same exception elsewhere in this solution.

Part 2 – Application Performance Monitoring

CenturyLink recommends Dynatrace as the solution to meet the City of Charlotte’s Application Performance Monitoring (APM) needs. CenturyLink and Dynatrace have a longstanding relationship and have worked together to solve many customer application monitoring challenges.

Dynatrace is a software intelligence company providing APM, artificial intelligence for operations (AIOps), cloud infrastructure monitoring, and digital experience management (DEM), with products for the information technology departments and digital business owners of medium and large organizations. The company’s services include performance management software for programs running on-premises and in the cloud. This software manages the availability and performance of software applications and the impact on user experience in the form of deep transaction tracing, synthetic monitoring, real user monitoring, and network monitoring.

The Dynatrace team is immensely proud to once again been positioned as a Leader in the Gartner 2019 Magic Quadrant for Application Performance Monitoring. Not only was Dynatrace named a Leader, but Dynatrace has been recognized as highest in ability to execute and furthest for completeness of vision in APM.

This recognition is a testament to Dynatrace’s drive to constantly innovate and be the best in all that they do.



Source: Gartner (March 2019)

For the ten applications identified in the RFP, CenturyLink and Dynatrace propose the following approach to monitoring.

| Application | Dynatrace Monitoring Class |
|------------------------|----------------------------|
| Tyler Munis Financials | DEM |
| PeopleSoft HRMS | Infrastructure |
| Microsoft SharePoint | Dynatrace APM |
| Hansen Banner | DEM |

| Application | Dynatrace Monitoring Class |
|------------------------|----------------------------|
| Azteca CityWorks | DEM |
| Emerald | Infrastructure |
| Emerald Web | Infrastructure |
| ESRI Infrastructure | DEM |
| Tableau Infrastructure | Infrastructure |
| Mobile Apps | DEM |

Digital Experience Monitoring (DEM): Real User Monitoring (RUM) is one of the two fundamental constituents of DEM, the other one being Synthetic monitoring. DEM is defined by Gartner as an availability and performance monitoring discipline that supports the optimization of the operational experience and behavior of a digital agent, human or machine, as it interacts with enterprise applications and services.

Dynatrace RUM gives you the power to know your end users by providing performance analysis in real time. This includes all user actions taken and how the various actions impact performance. You can also easily identify problems or errors that occurred as well as user experience ratings, geolocation breakdowns and much more. You can also gain insight into the behavior of your users. With Dynatrace RUM, you have the context over time and immediate analysis to the complete picture of your end user experience.

Dynatrace offers three types of synthetic monitoring: single-URL browser monitors, browser clickpaths, and HTTP monitors.

1. A single-URL browser monitor is the equivalent of a simulated user visiting your application using a modern, updated web browser. Browser monitors can be configured to run from any of our global locations at frequencies of up to every 5 minutes. Browser monitors alert you when your application becomes inaccessible or when baseline performance degrades significantly.
2. Browser clickpaths are simulated user visits that monitor your application's business critical workflows. You can use the Dynatrace recorder to record an exact sequence of clicks and user input that you are interested in monitoring for availability and performance. Once you've captured the mouse clicks and additional user actions that you want your browser clickpath to include, you can set your browser clickpath to run automatically at regular intervals to test your site's availability and functionality.
3. An HTTP monitor is a simple HTTP request. You can use it to check if your website or API endpoint is available. As with browser monitors, HTTP monitors run automatically at regular intervals. HTTP monitors are executed by an ActiveGate and require a special ActiveGate configuration. With this configuration, you can also use HTTP monitors to check the availability of your internal resources that are inaccessible from outside your network.

Infrastructure Monitoring

Full-stack Monitoring – it provides insight into infrastructure, network, into your services for code level visibility and even all the way out to users on your front-end website and mobile applications. In short, it's a single agent that gets deployed at the host/OS level (Windows/Linux/AIX/Solaris) that automatically detects all the processes, services, and applications running inside (real-time), auto-instruments them and then auto-baselines performance across those tiers. Then when there's an anomaly across the environment that's impacting user or operational performance, Dynatrace's A.I. engine automatically detects this issue, along with the impact to users, the application impacted, and ultimately the root cause. No more are the days of alert spam, no more are the days of "war rooms", and no more are the days of having multiple tools across your full stack (infrastructure all the way down to the method call).

Infrastructure Monitoring – analyzes key infrastructure health metrics in real-time. Automatically correlate performance problems with system changes.

CenturyLink estimated the sizing of APM infrastructure for the 10 application areas using the following planning assumptions.

- 25% of the 1,483 servers (360) are application and/or database servers.
- 8GB of RAM per host.
- Full stack monitoring applies to application servers and infrastructure monitoring for database servers.
- DEM – Digital Experience Monitoring – will support third-party SaaS applications and mobile applications.

Dynatrace will be configured to forward alerts to the Adaptive Service Desk.

Compliance with Specific Requirements

Please refer to "*Attachment A – Pricing Worksheet and Specifications.xlsx*", Application Performance Monitoring, which shows compliance (or exception) to the individual requirements. CenturyLink proposes one exception: Incident Risk Level of Critical with Notification to Within 5 minutes. In our experience, 5 minutes is an inadequate amount of time to detect, route to an analyst, quickly evaluate, and react to a suspected event without generating an excessive number of false positives. Industry standard for this target is 15 minutes and that is what CenturyLink proposes. CenturyLink proposes the same exception elsewhere in this solution.

Part 3 – Network Operation Center using CenturyLink Adaptive Service Desk

CenturyLink's Network Operation Center, known as the Adaptive Service Desk, will perform the following remote monitoring functions for the City from a U.S. location.

1. Application performance monitoring
2. Network and server event monitoring
3. Reporting

The CenturyLink Adaptive Service Desk is designed to support the highest possible uptime for key business applications and its enabling infrastructure by rapidly responding to events.

Adaptive Service Desk Monitoring for Applications

Applications will be monitoring for performance using Dynatrace DEM and infrastructure monitoring. Alerts generated by Dynatrace will be forwarded to the Adaptive Service Desk as set forth in the preceding section and handled in a similar fashion to Event Notifications generated by network devices or servers, which will be described below.

Adaptive Service Desk Monitoring for Network and Servers

The CenturyLink Adaptive Service Desk will monitor the in-scope applications and devices 24x7x365. Tools used will include an advanced monitoring platform, polling, and data collectors (historical data). The Adaptive Service Desk uses a variety of tools; the primary tool is SolarWinds.

Steady State Adaptive Service Desk Event Monitoring

As part of the monitoring, if required, CenturyLink will install a secure path for in-scope device monitoring via a VPN connection between the Customer's environment and the CenturyLink Adaptive Service Desk. The VPN connection is used solely to permit the CenturyLink Adaptive Service Desk to monitor the device.

Devices are configured to send "Event" (as defined in the Operating Guide) notifications (traps) to the CenturyLink Adaptive Service Desk. These notifications are automatically correlated and indexed in order to be categorized into the appropriate severity group. The notification is then forwarded to the City for response. The City shall notify CenturyLink in advance of any maintenance which may result in a failure notification. The City shall also notify the CenturyLink Adaptive Service Desk of any device outages caused by the City and when such outages are resolved.

When Event Monitoring identifies an Event, the CenturyLink Adaptive Service Desk will work with the City to identify the City's resolver groups for routing notifications. A City notification for each Event is logged in CenturyLink's ticketing system then forwarded to the Customer based on the incident classification outlined in the RFP requirements and agreed to in the CenturyLink Operating Guide.

When an Event is resolved, the City will close the ticket in their ticketing system. As the proposed solution includes integration of Cherwell with CenturyLink's ticketing system, the ticket will register as closed in our system. This process will be agreed to and outlined in the Operating Guide.

Implementation of Adaptive Desk Monitoring

CenturyLink will incorporate into the project a transition plan to operational steady state. This will include the development of the Operating Guide for the Adaptive Service Desk that will be supporting the City.

The implementation of Adaptive Service Desk monitoring will be performed by CenturyLink in the following sequence:

- Assigning a Customer Success Manager (CSM) and a Technical Account Manager (TAM) to coordinate the activities between CenturyLink and the City's key technical leads.
- Gathering the specific monitoring requirements for the network devices and servers
- Working with the City to develop a migration plan for onboarding the in-scope devices, which includes:
 - Approximately 1,500 Servers: 1,343 Windows servers and 140 Linux servers;
 - Approximately 1,700 network devices in 2 data centers running on Cisco Nexus 9000, 7000, 5000, and 2000;
 - An assortment of Cisco route / switch platforms, including but not limited to Cisco 6500, 3700, 3500, 2900, and 2600;
 - Approximately 550 Cisco LWAPP access points; and
 - Two controllers for LWAPP infrastructure.
- Confirming that each in-scope network device and server is monitorable.
- Implementing monitoring, alerting, and reporting to the CenturyLink Adaptive Desk.
- Tweaking monitoring to filter out "noise."
- Documenting a change process for updating monitoring.
- Defining device onboarding processes to bring new devices into monitoring.
- Work with the City to identify and document monitoring procedures in an Operating Guide.

Compliance with Specific Requirements

Please refer to Attachment A – Pricing Worksheet and Specifications.xlsx, NOC Performance Monitoring, which shows compliance (or exception) to the individual requirements. CenturyLink proposes one exception: Incident Risk Level of Critical with Notification to Within 5 minutes. In our experience, 5 minutes is an inadequate amount of time to detect, route to an analyst, quickly evaluate, and react to a suspected event without generating an excessive number of false positives. Industry standard for this target is 15 minutes and that is what CenturyLink proposes. CenturyLink proposes the same exception elsewhere in this solution.

3.2. Part 1 – Security Operations Services

Response:

Please see the Proposed Solution at the beginning of Section B (beginning on p. 1) for a holistic overview of the CenturyLink proposal that includes Security Operations Services.

Primary Objectives

The City of Charlotte is seeking to procure Security Operations services. We have identified below what we have determined to be the most important services and business requirements to meet our needs.

Core required services include Security Operations Center (“SOC”) operations, security event management, security event analysis, security incident response (“IR”) and management. We are sure to require these core services to be awarded and under contract.

We also have additional service requirements in the areas of analytics platform operations, email threat monitoring and analysis, cyber intelligence support, compromise assessment, and security system support. These additional services are preferred but may not be awarded depending on cost and funding availability.

Core Service Requirements

The following sections detail requirements for core services requested for Security Operations.

1. Transition Support

- 1.1. *Provide support for transition planning and transition plan execution associated with meeting agreed upon timeline for transition of Security Operations services from the incumbent contractor.*
- 1.2. *Actively participate in the transition of Security Operations services from the incumbent contractor and develop a Security Operations Incoming Transition Plan that ensure that there is not degradation of Security Operations services during the transition.*
- 1.3. *Develop and submit an Outgoing Transition Plan for transitioning work to a successor contractor or the City.*

Response:

CenturyLink fully complies.

2. SOC Operations, Facilities, Personnel, and Communication

- 2.1. *The objectives of the SOC are to protect, detect, respond, and recover from cyber security threats to the City's enterprise and associated information systems.*
- 2.2. *Provide a SOC, along with one or more secondary or backup SOCs in case of emergency, located within the continental United States. A tour of SOC facilities shall be provided upon request by the City.*
- 2.3. *SOC services must be available 24 hours a day, seven days a week.*
- 2.4. *The SOC must be staffed with personnel who have the required educational background and experience to meet the requirements of this SOW.*
- 2.5. *Provide a Senior Security Engineer who will be available to consult on security matters and direct SOC actions based on the City's cyber security needs.*
- 2.6. *Ability to comply with the current and future requirements of the Criminal Justice Information Services (“CJIS”) Security Policy including but not limited to mandatory background checks and training.*
- 2.7. *Notify the City of onboarding and offboarding personnel to the City's account.*

- 2.8. *A weekly conference call will be hosted by the Company to review the current state of Security Operations services. This call must include sufficient technical representation from the Company to discuss the details of security issues being worked, as well as sufficient management representation to execute corrective actions when necessary.*

Response:

CenturyLink fully complies.

3. Systems Access

- 3.1. *Access to City information systems will be provided on a least-privilege basis. The Company will document and propose a tiered, role-based access management procedure for Security Operations personnel which takes into account the education, certification, and experience of the individual and provides the City an opportunity to review and approve/reject applications for access.*
- 3.2. *The City reserves the right to interview personnel prior to granting elevated access to City information systems. If personnel are determined to be unqualified for elevated access, such access will be denied.*

Response:

CenturyLink fully complies.

4. Reporting

- 4.1. *On a monthly, annual, and ad hoc basis, provide reporting on key performance indicators (“KPI”) and other metrics related to the City’s information security posture. The requirements for these reports will vary, but monthly and annual reports are required.*
- 4.2. *These reports must also provide graphs comparing current metrics against previous months to identify trends in the direction of the City’s information security landscape.*
- 4.3. *Ad hoc reporting on indicators of attack such as Internet Protocol (“IP”) addresses, hashes, etc., from information security system logs/events will be required to comply with federal and regulatory reporting requirements. Ad hoc reports must be provided within three business days of request.*

Response:

CenturyLink fully complies.

5. Security Event Management and Communication

- 5.1. *A centralized, secure method to track and communicate information and data related to security events must be provided to allow authorized City personnel to view information relating to ongoing and resolved security events. This may take the form of an incident management platform, a ticketing system, or some other system for tracking these events.*
- 5.2. *This system must be secure, encrypted, authenticated, and allow for access by authorized City employees from their mobile devices.*
- 5.3. *Encryption must be in place both at rest and in transit and must use the latest standards required by the City. The City’s current standards are AES-256 at rest and TLS 1.2 in transit.*
- 5.4. *The system must protect the City’s data from access by unauthorized individuals, especially via segmentation from other customer data.*

5.5. The system must record, at a minimum, the following information below about each event in separate fields for reporting and trend analysis.

- Event summary
- Severity
- Event date and time, including time zone (in UTC)
- SOC point of contact
- Current status
- Attack vector
- Indicators of attack (raw logs, hashes, file names, registry entries, etc.)
- 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
- Operating System, including version
- Endpoint protection software versions
- Impacted department
- Identification method
- References
- Resolution

5.6. Messaging communications regarding security events between the SOC and the City must take place over secure, encrypted methods. Such communication methods must be approved by the City prior to implementation or use.

5.7. The SOC must notify the City of suspected security incidents in accordance with the requirements in the following table. This constitutes the service level agreement “(SLA)” for SOC notifications to the City.

| Incident Risk Level | Notification to City Within | Required notification method(s) |
|---------------------|-----------------------------|---------------------------------|
| Critical | 5 minutes | Call first, then email |
| High | 30 minutes | Call first, then email |
| Medium | 60 minutes | Email |
| Low | 24 hours | Email |

Response:

CenturyLink complies except for Incident Risk Level Critical of Notification to the City Within 5 minutes. In our experience, 5 minutes is an inadequate amount of time to detect, route to an analyst, quickly evaluate, and react to a suspected event without generating an excessive number of false positives. Industry standard for this target is 15 minutes and that is what CenturyLink proposes.

6. Security Event Analysis

- 6.1. *Review all security device data feeds, analytical systems, sensor platforms, output from other information security systems. This may be performed via an analytics platform.*
- 6.2. *If the analytics platform is not capable of properly ingesting, parsing, and indexing the output of a given security system, that system must be reviewed directly.*
- 6.3. *Analyze and investigate any events that would pose a threat to the City's information systems.*
- 6.4. *The analysis process will differ by event type, so procedures or playbooks should be developed by the SOC and approved by the City for each type of event.*
- 6.5. *In addition to reviewing other events and logs from City information systems, analysis processes should include thorough searches of both open source and closed source intelligence sources, monitoring of possible attacker communication channels, sandboxing, manual malware analysis and any other tasks useful to enriching the context of the event.*
- 6.6. *As events are analyzed and determined to be false positives, propose security system configuration changes to the City to tune out those events. Tuning of the analytics platform may also be performed on confirmed false positives.*
- 6.7. *Any security event which, during analysis and investigation, is determined to be malicious and may pose a threat to the security of the City's information systems would enter the security IR process.*

Response:

CenturyLink fully complies.

7. Security IR

Once a security event is identified as a threat to the City's information systems, that event must be tracked, managed, communicated about, and responded to by the SOC through all phases of the IR process. The City's incident response process consists of the following phases.

- 7.1. *Preparation*
 - 7.1.1. *The SOC will be responsible for supporting and assisting the City in the development and maintenance of the City's overall IR capability. The SOC will also assist the City in ensuring that systems, networks, and applications are sufficiently secure.*
- 7.2. *Identification*
 - 7.2.1. *This phase will be the primary focus of the SOC during typical daily operations. This will include the Security and Event Analysis, Email Threat Monitoring and Analysis, Threat Hunting, Cyber Intelligence Support as well as additional operations to enrich and further investigate events to provide clarity regarding the nature of a given event and its possible or actual impact on the City's information systems.*
 - 7.2.2. *Identification and validation of a possible threat should include investigation into the configuration of affected systems. This may include performing vulnerability assessments of affected systems such as port scanning, service and software identification, and configuration review. Port/vulnerability scanning will only be performed with the explicit approval of the City.*
- 7.3. *Containment*
 - 7.3.1. *The SOC will make containment strategy recommendations to the City based on the knowledge gathered during the Identification phase. Recommendations should consider the potential damage to and theft of resources, need for evidence collection/preservation, potential impact to service availability, time and resources required to implement, effectiveness, and duration.*
 - 7.3.2. *In addition to making containment strategy recommendations, once a strategy is approved, the SOC may be responsible for executing all or part of the strategy by making configuration changes to City information security systems.*

7.4. *Eradication*

7.4.1. *The SOC will make eradication strategy recommendations to the City based on the knowledge gathered during the Identification and Containment phases.*

7.4.2. *In addition to making eradication strategy recommendations, once a strategy is approved, the SOC may be responsible for executing all or part of the strategy by making configuration changes to City information security systems.*

7.5. *Recovery*

7.5.1. *The SOC will monitor recovery from information security incidents and provide status updates as the City brings affected systems back online.*

7.6. *Lessons Learned*

7.6.1. *The SOC will recommend changes to City policy, process, or technology to prevent or more quickly detect similar incidents in the future. Depending on the scope of the incident, the SOC may need to participate in a root cause or lessons learned meeting to provide information about the incident from their perspective.*

Response:

CenturyLink fully complies.

8. Changes to Information Security Systems

8.1. *Any changes to City information security systems must be approved by the City prior to the change taking place. Depending on the nature of the change, and at the City's discretion, the SOC may need to use the City's Change Management process to make the change.*

8.2. *Information security systems in which the SOC may be required to make configuration changes to secure the City's information systems are in the Current Environment section.*

8.3. *Capacity to make security-related changes (blacklist hash, block IP, tune Intrusion Detection Prevention Systems, etc.) to these systems must be available 24 hours a day, seven days a week.*

Response:

CenturyLink fully complies.

9. Additional Service Requirements

The following sections detail requirements for additional services which may be needed for Security Operations.

9.1. *Analytics Platform Operations*

9.1.1. *Provide a hosted or cloud-based security analytics platform (or security information and event management ["SIEM"]) system to ingest, parse, index, categorize, correlate, visualize, and alert on security logs.*

9.1.2. *This analytics platform must be hosted within the continental United States only.*

9.1.3. *The analytics platform must parse and index logs from all City information security systems and make those logs hot searchable for no less than 15 days.*

9.1.4. *All logs ingested by the analytics platform must be retained in their raw log format for a minimum of 365 days.*

9.1.5. *Current log volume is provided in the Current Environment section below. The analytics platform should have the ability to scale up as the City's volume increases.*

9.1.6. *Provide a secure, encrypted method for transmitting logs from the City's information security systems to the analytics platform.*

- 9.1.7. *Support for newly onboarded information security systems must be provided in a timely manner, with new log sources being added including parsing and indexing set up within 30 calendar days.*
- 9.1.8. *Notify the City via email of a silent or unavailable log source within 2 hours of the source's threshold being reached. Thresholds for silent log sources will be established on an individual basis.*
- 9.1.9. *There are some security events/logs within the City's environment that must be monitored directly by City personnel. To facilitate this, the analytics platform must have the capability to alert the City immediately via email, or other messaging methods approved by the City, based on custom search parameters.*
- 9.1.10. *Access to create custom alerts on the analytics platform should be provided to the City. If such access is not feasible, creation of custom alerts should be provided within 24 hours of request.*
- 9.1.11. *Provide training regarding how to conduct investigations and analysis in the analytics platform to up to 14 City personnel.*
- 9.1.12. *The analytics platform must provide for authentication via the City's onprem Active Directory ("AD") or Security Assertion Markup Language ("SAML") via AD Federation Services ("AD FS").*
- 9.1.13. *Provide management, maintenance, and technical support for the analytics platform, with response to support issues provided within 24 hours of an issue being reported.*
- 9.1.14. *Must have at least two years of experience implementing similar solutions.*

Response:

CenturyLink fully complies.

10. Email Threat Monitoring and Analysis

- 10.1. *Provide an email address to which suspected malicious emails may be sent by the City. Emails sent to this address must be analyzed with the same frequency and urgency as other security data feeds.*
- 10.2. *Any email which, during analysis and investigation, is determined to be malicious and may pose a threat to the security of the City's information systems would be considered a security incident and enter the IR process.*

Response:

CenturyLink fully complies.

11. Cyber Intelligence Support

- 11.1. *In support of Security Operations and the City's efforts to secure its information systems, provide analysis of cyber intelligence. Gather, ingest, and review cyber news feeds, signature updates, incident reports, threat briefs, and vulnerability alerts from external sources and determine their applicability to the City's environment.*
- 11.2. *Interpret and compile the information received about emerging threats through data feeds from Internet security firms, Government organizations, and private industry into actionable monitoring either by developing custom content or by some other means.*
- 11.3. *Analyze threat information, determine the risk to the City's environment, and develop mitigations and/or countermeasures.*
- 11.4. *Provide situational awareness to the City through regular threat briefs and vulnerability alerts, communicate methods for detecting activities of specific threats, and plan operations to mitigate or disrupt the threat as part of the City's information security program.*
- 11.5. *At the City's request, gather, analyze, and report on intelligence regarding specified risks to the City's information systems. Reports should be provided within 12 hours of request.*

Response:

CenturyLink fully complies.

12. Security System Support

- 12.1. *The Company will be responsible for the management, administration, and operation of any systems provisioned by the Company, even systems provisioned on City infrastructure.*
- 12.2. *Additionally, the Company may be required to provide support for the systems listed in the Security System Changes section below. The Company may be responsible for supporting the City in routine maintenance, administration, and operation of these systems.*
- 12.3. *Support for all security appliances by completing policy tuning, auditing, moves, adds, or changes (“MAC”).*
- 12.4. *Layer 7 firewall support to include:*
 - 12.4.1. *OS monitoring for common vulnerability exposures (“CVE”) with associated upgrades and patching.*
 - 12.4.2. *Firewall policy MACs.*
 - 12.4.3. *Ongoing IPS tuning based on CVE notices by threat intelligence providers when applicable to the City’s environment.*
 - 12.4.4. *Anti-virus, anti-bot, and other threat blade tuning as needed to include exceptions and evaluation of false positives.*
 - 12.4.5. *Content awareness and data loss prevention policy updates and tuning.*
 - 12.4.6. *Virtual private networking (“VPN”) IPsec tunnel support as needed.*
 - 12.4.7. *VPN client support as needed.*
 - 12.4.8. *Coordinating with vendor support to prepare for custom signature creation in the event of a security incident.*
 - 12.4.9. *Coordination with vendor support to solve software bugs, address incidents, and resolve problems.*
- 12.5. *Load balancer support for Local Traffic Manager (“LTM”), Application Security Manager (ASM), and Application Performance Manager (“APM”) configuration, to include:*
 - 12.5.1. *OS monitoring for CVE with associated upgrades and patching.*
 - 12.5.2. *Virtual IP (VIP) configuration, discrete node and service health monitoring, iRule configuration, iApp deployments, and web application firewall setup and tuning.*
 - 12.5.3. *ASM updates, staging, and tuning for all VIPs.*
 - 12.5.4. *APM web portal VPN support to include portal apps, single-sign on configuration, policy editing for access management.*
 - 12.5.5. *Coordinating with vendor support to prepare for custom iRules in the event of a security incident.*
 - 12.5.6. *Coordination with vendor support to solve software bugs, address incidents, and resolve problems.*
- 12.6. *Distributed Denial of Service (“DDoS”) protection appliance support to include:*
 - 12.6.1. *OS monitoring for CVE with associated upgrades and patching.*
 - 12.6.2. *Blacklisting of habitual offenders.*
 - 12.6.3. *Coordinating with vendor support to prepare for custom signature creation in the event of a security incident.*
 - 12.6.4. *Coordination with vendor support to solve software bugs, address incidents, and resolve problems.*
- 12.7. *Automation of routine processes and tasks on security appliances.*

- 12.7.1. *Assist City InfoSec as needed in the automation of routine security tasks related to the load balancing LTM, firewall demilitarization zone (“DMZ”) creation, firewall policy rule updates and installation, and DDoS blacklisting.*
- 12.7.2. *The automation of these components will be made through an automation platform such as Ansible or Tufin.*
- 12.7.3. *Ensure the monitoring of automation processes to report failures and successful implementations.*

Response:

CenturyLink fully complies. CenturyLink proposes that these requirements be handled by the staffing proposed in response to the Onsite Services requirements that immediately follow.

13. Onsite Services

- 13.1. *Provide one (1) full time onsite Tier 3 Infrastructure Security Engineer to support on-going security appliance operational needs to include security policy MACs, appliance upgrades, IPS tuning, policy auditing, monitoring, installations, automation scripting, and other tasks as required.*
 - 13.1.1. *This engineer must have a minimum of 3 years security appliance experience in Checkpoint or Palo Alto, 3 years’ experience in a network engineering field, and experience in scripting in BASH and Python. The engineer must also possess expert research and troubleshooting skills to solve complex issues expeditiously.*
- 13.2. *Provide one (1) full time onsite Tier 3 Cyber Security Analyst to support security operations, primarily in the areas of incident response, email security analysis, threat hunting, and other tasks as required. The analyst must have:*
 - 13.2.1. *Extensive experience analyzing and synthesizing information with other relevant data sources, providing guidance and mentorship to others in cyber threat analysis and operations, and evaluating, interpreting, and integrating all sources of information.*
 - 13.2.2. *A minimum of seven (7) years of professional experience in cyber security or a bachelor’s degree in a related field with five (5) years of professional experience in cyber security. The professional experience should be in the areas of security monitoring and detection, incident response, email security analysis, or threat hunting.*
- 13.3. *The City reserves the right to interview, and possibly reject, candidates for the above positions.*
- 13.4. *In addition to the above resources, provide, monthly, 16 hours of onsite information security engineering support.*
 - 13.4.1. *During onsite visits, the engineer will build relationships with City personnel, provide security recommendations, and assist in engineering security systems.*

Response:

CenturyLink fully complies. CenturyLink will utilize a MWSBE subcontractor or subcontractors to satisfy the requirements of this section and to support the Charlotte Business INClusion (CBI) policy.

14. Threat Hunting

- 14.1. *Provide advanced analysis and threat hunting support to security operations to proactively uncover evidence of adversary presence on City networks.*
- 14.2. *Focus on threat detection, geared toward attacks that have bypassed existing security controls.*
- 14.3. *Develop hunt use cases or playbooks to look for specific tactics, techniques, and procedures (“TTPs”) that indicate a threat is active in the City’s environment.*

- 14.4. Use information and threat intelligence related to the City's information systems to identify undiscovered attacks.
- 14.5. Investigate and analyze all relevant sensor data (network, endpoint, logs, etc.), reporting on any findings and making recommendations to improve hunt operations.
- 14.6. Provide recommendations on security architecture, instrumentation, and controls to make the City's information systems more resilient.

Response:

CenturyLink fully complies.

15. Compromise Assessment

- 15.1. Provide, annually, an 80-hour engagement of dedicated compromise assessment services to evaluate the City for signs of successful intrusion or exfiltration of data.
- 15.2. This engagement must include not only analysis of information systems owned by the City, but also a search for indications that the City's data has been compromised and/or is being sold or shared online.
- 15.3. Provide full briefing to technical and management teams on findings and impact of any discovered compromise, including actionable guidance on next steps to respond to and eradicate any threats.

Response:

CenturyLink fully complies.

16. Current Environment

1. Security System Changes

The table below details the security systems on which the SOC will perform changes, including the number of devices and the types of changes the SOC will need the capacity to execute.

| Quantity | Type | Changes/Actions Required by SOC |
|----------|--|---|
| 1 | SentinelOne Management Console | Blacklist hash, whitelist hash, resolve events, disconnect system from network |
| 1 | Carbon Black Cb Response Management Console | Blacklist hash, create watchlist, tune watchlist |
| 2 | Palo Alto and Checkpoint Firewall Management Servers (in HA) – IPS, Anti-Bot, Anti-Virus, Threat Emulation (24 Clusters) | Policy MACs, IPS/Threat signature tuning, block bad IP/Host/Country, OS updates as needed. |
| 35 | Palo Alto and Checkpoint Small Appliances | Policy MACs, appliance configuration and tuning, OS updates as needed. |
| 8 | F5 ASM/LTM/APM | ASM Policy MAC and signature tuning, LTM VIP MAC, APM and SSO updates, iRule creation, OS updates as needed |

| | | |
|---|-------------------------|--|
| 2 | Radware DDoS Appliances | Block bad IP/Host/Country, OS updates as needed. |
|---|-------------------------|--|

2. *Systems Sending Logs to Analytics Platform*

The following systems will send logs to the analytics platform.

| Quantity | System |
|------------------------------|--|
| 24 clusters 35 standalone | Checkpoint firewalls (firewall, IPS, Anti-Bot, Anti-Virus, Threat Emulation) (via management server) |
| 3 clusters 3 standalone | Palo Alto firewalls (firewall, IPS, threat) (via management server) |
| 1 cluster | Radware DDoS |
| 45 | Active Directory Domain Controllers (security logs only) |
| 2 | Adaxes servers |
| 1 | Airwatch MDM server |
| 2 | Apache web servers |
| 3 | Bind DNS servers |
| 2 | Cb Response servers |
| 3 | Cisco ACS |
| 1 | Cisco ASA |
| 3 | Cisco Router |
| 3 clusters | F5 BIG-IP LTM, ASM, APM |
| 4 | Netmotion VPN |
| 1 | RedHat Syslog |
| 3 | Radware DefensePro |
| 1 | SentinelOne server (CEF) |
| 3 - 5 | Tufin servers |
| 1 cluster | SonicWALL |
| 14 | Windows file servers |
| 1 | Web server |
| 2 | RADIUS servers |
| 1 | Certificate Authority |

Response:

CenturyLink complies. The Security System Changes set forth in the first table will be performed by the CenturyLink Onsite Services team, not the SOC.

17. Total Log Volume

The current log volume that will need to be processed by the analytics platform is as follows:

- 7,000 events per second (“EPS”)
- 200 gigabytes (“GB”) per day (average, raw log volume)

Response:

CenturyLink has considered this data to calculate pricing.

3.3. Part 2- Application Performance Monitoring

Response:

Please see the Proposed Solution at the beginning of Section B (beginning on p. 1) for a holistic overview of the CenturyLink proposal that includes Application Performance Monitoring.

Primary Objectives

The City of Charlotte is looking to increase our visibility, alerting, and responsiveness to application infrastructure and performance issues. We are looking for a vendor to configure a monitoring solution for our applications, actively monitor the monitoring notifications, and provide intervention and/or alerting and escalation. The expectation is that application, database, and server monitoring data would be available in a unified view of an “application”.

Charlotte Applications Overview

The City has a diverse portfolio of applications, and application infrastructures. Primarily, the City hosts Commercial-off-the-Shelf software. There are also important custom-built applications and SaaS applications that need to be monitored.

The City is currently using Nagios to monitor applications. Nagios is providing basic up/down monitoring through “polling” checks. There are approximately 400 checks in Nagios for applications. The monitoring is managed by the City’s current NOC provider.

Some example applications that would be under the proposed monitoring service are the following:

- Tyler Munis Financials
- PeopleSoft HRMS
- Microsoft SharePoint
- Hansen Banner
- Azteca CityWorks (single infrastructure, 15 applications)
- Emerald (custom Oracle Forms/reports application)
- Emerald Web (custom react.js / C#.Net application)
- ESRI infrastructure
- Tableau infrastructure
- Mobile apps (custom iOS and Android)

Response:

CenturyLink has considered this information in developing the solution.

Project Implementation

The project implementation will consist of onboarding the 10 application areas listed above. This will involve the following:

1. Requirements gathering for monitoring specifics for each of the 10 application areas, based on the level of application monitoring the vendor can provide;
2. Implementation of monitoring, alerting, and reporting,
3. Tweaking monitoring to filter out “noise;”
4. Defining a change process for updating application monitoring “checks” or areas of interest; and
5. Defining application onboarding process to bring new applications into monitoring.

Response:

CenturyLink fully complies.

Ongoing Operations

In similar fashion to a standard NOC, provide 24x7x365 operational monitoring of Applications, intervention, alerting, and escalation of Application issues.

The vendor service must notify the City of suspected events in accordance with the requirements in the following table.

| Incident Risk Level | Notification to City Within | Required notification method(s) |
|---------------------|-----------------------------|---------------------------------|
| Critical | 5 minutes | Call first, then email |
| High | 30 minutes | Call first, then email |
| Medium | 60 minutes | Email |
| Low | 24 hours | Email |

As part of operations, the vendor will update monitoring “checks” as needed or requested.

The implementation project will document an onboarding process for new applications. As part of operations, the vendor will onboard new applications into monitoring as requested.

Response:

CenturyLink complies except for Incident Risk Level Critical of Notification to the City Within 5 minutes. In our experience, 5 minutes is an inadequate amount of time to detect, route to an analyst, quickly evaluate, and react to a suspected event without generating an excessive number of false positives. Industry standard for this target is 15 minutes and that is what CenturyLink proposes.

Key Requirements for Application Monitoring

The Company shall be responsible for providing the following application performance monitoring.

| Section | Key Requirements - Application Performance Monitoring | Critical Important Nice to Have |
|----------------|--|--|
| 1.0 | Deployment Options | |
| 1.1 | <i>Flexibility to monitor applications deployed both internally (incl. virtualized environments and /or private cloud) and externally (Amazon Cloud, Microsoft Azure etc.)</i> | <i>Critical</i> |
| 1.2 | <i>Vendor encrypts data transmissions end-to-end across the environment</i> | <i>Critical</i> |
| 2.0 | Installation | |
| 2.1 | <i>Ability to install Agent into application container</i> | <i>Important</i> |
| 2.2 | <i>Web based feature rich GUI without need for fat client (no installation, ongoing maintenance or management for web client)</i> | <i>Important</i> |
| 3.0 | Configuration | |
| 3.1 | <i>Automatically create a visualization of the entire application topology with all components.</i> | <i>Critical</i> |
| 3.2 | <i>Automatically discover business transactions</i> | <i>Critical</i> |
| 3.3 | <i>Automatically discover standard back end systems (database, web services, SAP etc.)</i> | <i>Critical</i> |
| 3.4 | <i>Agents will not consume more than 4% of cpu / ram / disk / network utilization.</i> | <i>Critical</i> |
| 3.5 | <i>Automatically baseline every component within the Business Transaction</i> | <i>Important</i> |
| 3.6 | <i>SSL Encrypted data transmission between EVERY monitoring component.</i> | <i>Critical</i> |
| 4.0 | Better Application Visibility and Control | |
| 4.1 | <i>Provide correlated views of distributed Business Transactions between tiers/services</i> | <i>Important</i> |
| 4.2 | <i>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.</i> | <i>Important</i> |
| 4.3 | <i>Provide code level diagnostics (class & method-level visibility) of poorly performing business transactions</i> | <i>Important</i> |
| 4.4 | <i>Monitor JVM health information (heap, GC, generational spaces, etc.)</i> | <i>Important</i> |
| 4.6 | <i>Report application errors & exceptions</i> | <i>Critical</i> |
| 5.0 | Reduce Mean Time To Repair | |
| 5.1 | <i>Identify slow and stalled Business transactions without manual intervention</i> | <i>Important</i> |
| 5.3 | <i>Identify error business transactions without manual intervention</i> | <i>Important</i> |
| 5.4 | <i>Identify slow SQL queries without manual intervention</i> | <i>Important</i> |
| 5.5 | <i>Identify slow backends systems or external services without manual intervention</i> | <i>Important</i> |
| 5.6 | <i>Automatically discover code deadlocks</i> | <i>Nice to Have</i> |
| 5.7 | <i>Provide quick cross launching into problem areas within the UI through hyper-linked alerts</i> | <i>Nice to Have</i> |
| 5.8 | <i>Automatically send email containing hyperlink to identified problem</i> | <i>Important</i> |
| 6.0 | Using Business Transactions as Key Unit of Monitoring and Management | |

| Section | Key Requirements - Application Performance Monitoring | Critical Important Nice to Have |
|----------------|---|--|
| 6.1 | Automatically discover business transactions (no need to configure the classes/methods for monitoring) | Nice to Have |
| 6.2 | Automatically learn and baseline performance of discovered business transactions | Important |
| 6.3 | Monitor performance and analyze customer experience through various network connections (on-site wired, on-site wireless, via VPN, via cellular) | Important |
| 6.4 | Discover complete transaction flow/architecture (support for synchronous, asynchronous and multi-threaded business transactions) | Important |
| 7.0 | Provide Real-Time Business Metrics | |
| 7.1 | Provide the facility to create custom dashboards for business metrics and related application behavior | Important |
| 7.2 | Provide pre-built performance reports on business transaction summary and business transaction trends | Important |
| 7.3 | Capture usage statistics for all urls, pages, web services, external calls, locations, servers. | |
| 7.4 | Automatically correlate business transactions with environment monitoring (OS, JMX etc.) | Important |
| 8.0 | Usability | |
| 8.1 | Provide automatic & dynamic baselining of all metrics to reduce false alarms and elimination of static thresholds | Important |
| 8.2 | Solution offers ability to visualize multiple applications and the connectivity/dependencies between them. | Important |
| 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 |
| 8.4 | Ability to link business transaction directly back to log entries on the respective components involved in the transaction | Important |
| 9.0 | Historical Trending Capabilities | |
| 9.1 | Provide long term historical trending (metric persistence to enable historical observation (and comparison to baselines) | Critical |
| 10.0 | 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 |
| 10.2 | Automatically baseline new components – no manual intervention required – no unnecessary alert storms or false negatives | Important |
| 10.3 | Allow regression analysis to compare and highlight application performance regressions/improvements | Nice to Have |
| 11.0 | Pre-Production Performance Tuning | |
| 11.1 | Identify application hotspots (quickly spot the longest running methods in poorly performing business transactions) | Nice to Have |
| 11.2 | Enable scalability analysis (determine impact and relationship between increased load and application average response times) | Nice to Have |

| Section | Key Requirements - Application Performance Monitoring | Critical Important Nice to Have |
|----------------|---|--|
| 11.3 | Identify worst backend calls (Database, Web Services, other backends) automatically | Nice to Have |
| 12.0 | Workflow Orchestration and Alerting | |
| 12.1 | Ability for automated problem remediation through scripts, workflows, etc. | Critical |
| 12.2 | Ability for automated or manually execute processes, workflows to gather more troubleshooting details, remediate problems, or to dynamically scale resources. | Critical |
| 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 |
| 13.0 | Memory Management | |
| 13.1 | Identify JVM memory leaks caused by leaky collections | Important |
| 13.2 | Enable tracking of object instantiations/destructions to troubleshoot JVM heap thrash | Important |
| 14.0 | Scalability and Infrastructure Efficiency | |
| 14.1 | Ability to support high availability APM infrastructure servers | Important |
| 15.0 | 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 |
| 15.2 | Ease of integration via RESTful API | Important |
| 16.0 | Web Real User Monitoring | |
| 16.1 | Support for modern desktop browsers | Critical |
| 16.2 | Support for mobile browsers | Critical |
| 16.3 | Monitor all page requests | Critical |
| 16.4 | Monitor all AJAX requests | Critical |
| 16.5 | Monitor all iFrame requests | Nice to Have |
| 16.6 | Monitor all web platforms (Apache Tomcat, Jboss, Java, IIS) | Critical |
| 16.7 | Full support for monitoring single page applications properly | Critical |
| 16.8 | Automatically detect JavaScript errors | Critical |
| 16.9 | Correlate web transactions with server side transactions for drill down | Important |
| 16.10 | Provide detailed browser traces for poor performing end user requests | Important |
| 16.11 | Provide usage based analytics showing browser types and versions | Important |
| 16.12 | Provide usage based analytics showing device and OS types | Important |
| 16.13 | Provide cache metrics for each page request | Important |
| 16.14 | Show server side response time for all pages | Important |
| 16.15 | Provide tracking for various entities, such as sessions, ports, IPs, user logins. | Critical |

| Section | Key Requirements - Application Performance Monitoring | Critical Important Nice to Have |
|----------------|---|--|
| 17.0 | Synthetic Visibility | |
| 17.1 | Real browser endpoints running scripts not simulated browsers | Important |
| 17.2 | Simulate mobile network speeds | Nice to Have |
| 17.3 | External website testing | Critical |
| 17.4 | Ability to script tests | Critical |
| 17.5 | Auto-retest after failed test | Critical |
| 17.6 | Flexible alerting system | Critical |
| 17.7 | Variable bandwidth testing | Nice to Have |
| 17.8 | Standards based scripting language (Selenium) | Important |
| 17.9 | Synthetic data analytics | Important |
| 17.10 | Synthetic session tracking | Important |

Response:

CenturyLink complies with every requirement listed in the table. This is also set forth in the worksheet entitled “Application Performance Monitoring” in Attachment A.

3.4. Part 3 - Network Operation Center

Response:

Please see the Proposed Solution at the beginning of Section B (beginning on p. 1) section for a holistic overview of the CenturyLink proposal that includes Network Operation Center.

Primary Objectives

The mission of a Network Operations Center (“NOC”) is to assure the highest possible uptime for key business applications and the services that enable those applications. This means a NOC monitors network and application dynamics, responds to outages and maintains the functionality of the environment. This environment includes over 3,000 devices which is all City servers, network and wireless infrastructure devices.

Charlotte Operations Overview

The following is a rough outline of Charlotte’s production compute environment:

1. *Approximately 1,483 Servers including:*
 - *1,343 Windows servers*
 - *140 Linux servers*
 - *69% of the servers are virtualized with VMWare*
2. *Approximately 1,700 network devices including:*
 - *Two (2) Data Centers running on Cisco Nexus 9000, 7000, 5000, and 2000.*
 - *An assortment of Cisco route / switch platforms*

- Including but not limited to Cisco 6500, 3700, 3500, 2900, and 2600
- Approximately 550 Cisco LWAPP access points
 - Two (2) controllers for LWAPP infrastructure

Response:

CenturyLink has considered this data to calculate pricing.

Key Requirements for Performance Monitoring

The company shall be able to provide the following:

| Key Requirements | Impact Description |
|---|---|
| Incident Initiation Capabilities | |
| <i>Compatibility with Cherwell</i> | <i>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.</i> |
| Monitoring Capabilities - Server | |
| <i>Monitor Machine availability</i> | <i>The ability to monitor basic UP/DOWN of servers to ensure service.</i> |
| <i>Monitor CPU usage</i> | <i>The ability to watch CPU and gather statistics and tie consumption to specific processes.</i> |
| <i>Monitor Disk performance</i> | <i>The ability to monitor disk I/O IOPS metrics.</i> |
| <i>Monitor Volume usage</i> | <i>The ability to see disk consumption along with top consumers with trending metrics.</i> |
| <i>Monitor Machine load</i> | <i>The ability to monitor machine load to determine when/if scale needs to go up or down.</i> |
| <i>Monitor Memory</i> | <i>The ability to monitor memory for consumption and who the top consumers are with trending metrics.</i> |
| <i>Monitor SWAP</i> | <i>The ability to monitor SWAP utilization and see page events tied to specific processes along with trending metrics.</i> |
| <i>Monitor Processes</i> | <i>The ability to monitor processes and tie to other collected metrics for correlation along with trending metrics.</i> |
| <i>Monitor Network Adapter(s)</i> | <i>The ability to monitor network metrics with trending data along with the ability to monitor active/passive failover groups.</i> |
| <i>Dynamic Baselineing</i> | <i>The ability to determine what normal behavior is and build baselines on system behavior for any available metric.</i> |
| <i>Synthetic page checker</i> | <i>The ability to ping a web page as a basic availability and performance checker within corporate firewalls.</i> |

| | |
|---|---|
| Monitoring Capabilities - Network | |
| <i>Monitor Machine availability</i> | <i>The ability to monitor basic UP/DOWN of network equipment to ensure service.</i> |
| <i>SNMP Traps on core / distribution / data center switches</i> | <i>The ability to watch and gather statistics and tie consumption to specific processes</i> |

| | |
|--|--|
| | <ul style="list-style-type: none"> - CPU/Memory - Temperature - Power Supplies |
| <i>Monitor Critical Interfaces on core / distribution / data center switches</i> | <i>The ability to monitor critical network interfaces.</i> |
| <i>Backup Switch Configurations</i> | <i>The ability to backup switch configurations</i> |
| <i>Netflow</i> | <ul style="list-style-type: none"> - Response time/latency - Bandwidth utilization on core/distribution/ datacenter switches/firewalls - reporting |
| Monitoring Capabilities – Microsoft | - |
| <i>Microsoft Exchange</i> | - <i>Must interface with MailScape</i> |
| <i>Microsoft Active Directory</i> | - <i>Ability to monitor Active Directory Health</i> |
| <i>Monitoring Capabilities – Security Appliances</i> | - |

Response:

CenturyLink complies with every requirement listed in the table. This is also set forth in the worksheet entitled “NOC Performance Monitoring” in Attachment A.

Project Activities and Milestones

There shall be a project lead assigned to the project that shall oversee the project. That project lead shall pull from the technical team of engineers and other architects as needed to meet technical deliverables.

Response:

CenturyLink fully complies.

Network Operations Architecture

The purpose of the startup process is to learn the in-scope production data environment, learn the use and function of any relevant Charlotte tools and information that will be available to NOC personnel, analyze Charlotte server and network infrastructure, and begin to work on the initial Charlotte operations guide that defines NOC day to day operations.

The operations guide defines how the NOC and Charlotte communicate and is a detailed inventory of the NOC’s work on behalf of SLAs to Charlotte.

The NOC must notify the City of suspected events in accordance with the requirements in the following table.

| Incident Risk Level | Notification to City Within | Required notification method(s) |
|----------------------------|------------------------------------|--|
| <i>Critical</i> | <i>5 minutes</i> | <i>Call first, then email</i> |
| <i>High</i> | <i>30 minutes</i> | <i>Call first, then email</i> |
| <i>Medium</i> | <i>60 minutes</i> | <i>Email</i> |
| <i>Low</i> | <i>24 hours</i> | <i>Email</i> |

Response:

CenturyLink complies except for Incident Risk Level Critical of Notification to the City Within 5 minutes. In our experience, 5 minutes is an inadequate amount of time to detect, route to an analyst, quickly evaluate, and react to a suspected event without generating an excessive number of false positives. Industry standard for this target is 15 minutes and that is what CenturyLink proposes.

Operations Standup, Tuning, and Reporting

Operations standup is the deployment of the new monitoring solution into production and initial tuning. The NOC shall deploy necessary hardware and software components into the Charlotte production environment and perform a soft launch of the operations service. During this time Charlotte's infrastructure environment will be categorized, operations software tuned, hardware infrastructures validated, and initial reports will be released for review and revision.

The NOC will commit to uplifting 600 devices per month onto the NOC operations platform. Once a device has been configured, it will be monitored 24x7. Baselineing, trending, and server/network health normalization will be ongoing.

The operations guide continues to be expanded and refined throughout this process.

Ongoing Operations

The production operations process starts 24x7x365 single pane of glass monitoring of the Charlotte server and network infrastructure.

Reoccurring operations tasks include, but are not limited to, the following:

- Perform systems analysis of the server / network infrastructure hardware, operating systems, and applications using the NOC toolsets*
- Monitor server/network alerts through the NOC toolsets to troubleshoot, triage, and escalate as needed*
- Provide both strategic and near real time analysis, investigation, reporting, remediation, coordination, and tracking of server/network related activities*
- Availability to implement City network device and server changes that are within process change management workflow procedures*
- Perform correlation of events from network, enterprise, and host sensors*
- Perform preliminary forensic case investigation of notable events*

Continuing Service Improvement include, but are not limited to, the following:

- Review network, server, and application events that are detrimental to overall infrastructure availability*
- Analyze data and prepare reports that document network vulnerabilities and recommend actions to prevent, repair, or mitigate these vulnerabilities*
- Provide updates to Charlotte management*
- Incorporate updates into the NOC operations guide*

Response:

CenturyLink fully complies.

3.5. Reporting Requirements.

Project Reporting Requirements.

For the length of the engagement, the Company shall provide monthly utilization analysis of all services to ensure the City's financial responsibilities to its citizens are being met.

Progress Reports.

Throughout the development and implementation period, the Company will be required to prepare and submit weekly written reports to the City Project Manager. The weekly reports shall: Update the Project Plan indicating progress for each task; Identify and report the status of all tasks that have fallen behind schedule and the reason and cure period; Identify and summarize all risks and problems identified by the Company which may affect the Project; For each risk and problem, identify the action and person(s) responsible for mitigating the risk and resolving the problem; For each risk and problem identified, state the impact on the Project Plan; and Identify all changes in the Project Plan that affect personnel, equipment, facilities and resources of the City which will be required for the Company to perform the Services two (2) weeks in advance of the need.

Response:

CenturyLink fully complies.

3.6. Training Plan.

Explain the training curriculum available to support the Company's Proposed Solution. The Company shall schedule training classes and modules to align with appropriate phases of the Project and all training shall be conducted on site at City facilities.

The Company shall submit a preliminary Training Plan outlining the content, sequence and duration of each segment of each training session necessary to thoroughly and comprehensively train City personnel to fully utilize the Deliverables (the "Training Plan"). Additionally, the Training Plan will:

- *Outline all subjects necessary to train City staff to fully understand and utilize the Deliverables.*
- *Provide comprehensive "train the trainer" training for the designated numbers of City designated personnel.*
- *Take into account classroom resources and personnel scheduling.*
- *Include a written description of the training classes that will be conducted, the number of persons that can be trained in each session, and the total number of hours required for each person to be trained.*
- *The cost of all training referenced in this Section must be included in the Proposal Pricing.*

Response:

CenturyLink fully complies. Training will be primarily focused on effectively interacting with the CenturyLink SOC and using the portal. This can be readily be performed by the Security Account Manager on an informal basis in one-on-one sessions or small groups. Training to interact with the Adaptive Service Desk would be similar and be handled by the Customer Success Manager.

3.7. Disaster Recovery.

In the event that a hosted solution is proposed, the Company must indicate the capability to recover from natural, human-caused, and electronic disasters (including security compromises) that could interrupt service to the City and the City's customers. The Company will detail their solution to include:

- *Procedures for off-site storage of information;*
- *Capabilities and availability of alternate processing, communications, and operations facilities;*
- *Plans for maintaining business processes, including communications with the City, the City's customers, and suppliers of goods and services.*
- *Estimated time to recover from disaster events, and service level expectations for business continuity following a disaster;*
- *Cost to the City, if any, for disaster recovery services; and*
- *A documented disaster recovery and business continuity plan, including dates of disaster recovery tests and schedule for future tests.*

Response:

CenturyLink has implemented a network of SOCs. If one fails, the workload can be moved to another. Supporting systems are located in multiple data centers. Data is backed up near-real-time by simultaneously streaming to both primary and secondary data centers. Integrity verification of primary and secondary data transferred runs as a background process also near real-time. This implementation enables high availability and an inherent disaster recovery capability.

3.8. City Hardware/ Software Requirements.

Compatibility and standardization are key concerns in City technology procurements. This is important to optimize interoperability and achieve better overall performance, and to reduce the costs of maintenance, inventory, training and administration. To that end, the City has established certain standards and preferences regarding implementation of new hardware and software. Proposed solutions must adhere to these where noted in the first column of the following table. In the remaining cases, adherence is preferred, but not required. Standards documentation for any technology category can be provided upon request. Version references in the matrix below are as of the time of publication. Vendors are expected to adhere to the current city-supported versions and will need to request those version updates from the City.

| Standards Apply / Adherence Required | Technology Category | Current Architecture Summary | Target Architecture (where different) | Compliant? (Y/N) |
|---|----------------------------|--|--|-------------------------|
| | Telephony | | | |
| | Telephony | AT&T POTS analog lines / Cisco / / True Image Interactive (TII) IVR (Formerly GetAbby) | Cisco | Not Applicable |
| | Call Recording System | Eventide / Verint / Cisco | Eventide / Verint | Not Applicable |

| Standards Apply / Adherence Required | Technology Category | Current Architecture Summary | Target Architecture (where different) | Compliant? (Y/N) |
|---|--|--|--|-------------------------|
| | Mobile Device Services | Apple iPhone 6s or higher (Excluding iPhone 10) all Apple iPads Samsung Android Devices (with approved exception) VMWare AirWatch Managed Devices | Apple iOS version 12.1.2 or higher | Not Applicable |
| Networking | | | | |
| x | Network Cabling | CAT6e /Corning fiber optic | CAT6 Plenum rated Systimax or better | Not Applicable |
| x | Network Hardware | Cisco Systems Hardware and Software including all portions of their Borderless Networking, Collaboration, Data Center and Virtualization product lines | | Not Applicable |
| | Multiple Domains | Any technology the City adopts must work within a multiple domain environment, including the ability to distinguish between users with the same username in multiple domains. | Microsoft 2016 (Summer 2018) Active Directory or higher | Not Applicable |
| | Network Communication Protocol (standards apply) | IP, current protocol is IPv4, but new equipment should support IPv6 | New technologies should support both IPv4 and IPv6 | Not Applicable |
| | Wi-Fi | Wi-Fi enabled systems should support 80211a,b,g,n and ac protocols , AES 256 bit encryption, PEAP and MS-CHAPv2 authentication New Access point equipment should support Cisco CAPWAP architecture, IEEE 802.11i | Wi-Fi enabled systems should support 80211a,b,g,n, and ac protocols | Not Applicable |
| | Load Balancing | F5 | | Not Applicable |
| Data Center | | | | |
| x | Server Hardware | HP Proliant series, Dell | HP Proliant Series | Not Applicable |
| x | Server Operating Systems | Windows Server 2008 and above, Red Hat 5 and above | Windows Server 2016, Red Hat 7.3 minimum, preferred last OS version 1+ years in production | Not Applicable |

| Standards Apply / Adherence Required | Technology Category | Current Architecture Summary | Target Architecture (where different) | Compliant? (Y/N) |
|---|--|--|--|-------------------------|
| x | Virtual Operating Environments | VMWare, Microsoft App-V, and Hyper-V, Nutanix ver. 5.1.3.2, | All servers will be VMWare Hyperconverged on Nutanix, where possible VDI/RDS: Microsoft Hyper-V, Microsoft AppV | Not Applicable |
| | Storage | HP, Pillar, SolidFire & EMC Isilon SAN / NAS storage, | HP, NetApp, SolidFire | Not Applicable |
| | Backup Software | Symantec Netbackup 7.5, EMC Avamar 6, EMC Data Domain | EMC Avamar 7.5.1 | Not Applicable |
| | Backup Hardware | Spectrallogic T-50, HP ESL9326 | EMC Avamar 7.5.1 / Data Domain 6.0.2 | Not Applicable |
| | Data | | | |
| x | Database Systems | Oracle Database Server 12.1.0.1 and above, MS SQL Server 2012 and above | SQL 2017 and later Oracle 12.2.0.1, 18.1.0 and later Postgres 9.6.x MariaDB 10.2.x Encourage open source DBs | Not Applicable |
| | ETL/Data Mapping Services/Data Warehousing | SQL Server Integration Services, SQL Server Analysis Services, WhereScape (RED, 3D and Data Vault Express), R, Python | Preferred last version 1+ years in production | Not Applicable |
| | Business Intelligence / Data Visualization | Tableau, Excel, Microsoft SQL Reporting Services (SSRS), Esri's Insights | | Not Applicable |
| | Reporting Services | Third-party products such as Business Objects / Crystal, COGNOS, Oracle Reports, and Microsoft SQL Server Reporting Services (SSRS) are supported for application-specific reporting. Tableau Enterprise Server and SSRS are the products supported by I&T. | SQL Server Reporting Services 2017 and later Tableau Enterprise Server | Not Applicable |
| | Application Servers | .NET Framework, Oracle WebLogic | .NET Framework 4.5.2 | Not Applicable |

| Application | | | | |
|-------------|---------------------------------|--|---|----------------|
| | Web Servers | Microsoft Internet Information Services (IIS) v7.x and 8.x | IIS 8.x | Not Applicable |
| | Application Languages | MS VB.NET, ASP.NET, MVC, C#.NET, PL/SQL, JSP, JavaScript, and Java J2EE are among the City's development toolsets in use. | , C#.NET Core, JavaScript, Swift (iOS), Java(Android) | Not Applicable |
| | Enterprise Integration Platform | Microsoft BizTalk 2016, Apache Active MQ, .NET Framework | Apache Active MQ 5.14+, .NET Framework 4.5.2 | Not Applicable |
| x | Desktop Operating System | Windows 7, Windows 8, Windows 10 | Windows 10 Enterprise | Not Applicable |
| x | Application Client | Client operating systems may include Windows 7 and above. Browser clients should support Microsoft Internet Explorer Version 11 and above. If an actual client installation is required, it must be tested by the City to confirm that it does not conflict with other existing desktop components. | Windows 10 Enterprise. Browser-based implementation is preferred, and where applies, with both mobile friendly and responsive design delivery capability across all devices | Not Applicable |
| | Portal Services | Microsoft Office SharePoint Services | SharePoint 2013 | Not Applicable |
| x | Geospatial Platform | The City's Geospatial Platform is based on ESRI's ArcGIS technology. All spatial databases should be compatible with the City's implementation of the ESRI Geodatabase. Web-based GIS tools, components or extended custom functionality should use ArcGIS API's. Google Maps API is used for Virtual Charlotte, Emerald Web. AutoCAD is also used by a number of departments. | ESRI ArcGIS 10.5.1 Google Maps for Android/iOS | Not Applicable |
| x | E-mail Services | The City uses Microsoft Exchange 2016 on-premise with the Microsoft Outlook e-mail client. | Exchange Server | Not Applicable |
| x | Business Productivity | MS Office 2010 | MS Office 365 – local install | Not Applicable |
| | Scanning software | Kofax 10, OnBase scanning module | OnBase scanning module | Not Applicable |
| | Cloud Storage & Sharing | Various shadow IT tools like Dropbox, box, Drive and OneDrive | Microsoft OneDrive | Not Applicable |

| | | | | |
|---|--------------------------|---|---|-----------------------|
| | <i>Document Viewers</i> | <i>Adobe Acrobat Reader and Professional</i> | <i>2018 (2015 if required by City approved application)</i> | Not Applicable |
| | <i>Data Protection</i> | | | |
| x | <i>Security</i> | <i>Security Access to the Software must be restricted by assigning user credentials to authorized users. Enterprise authentication services are provided by Active Directory. All data should be encrypted during transmission and data defined as restricted in the City's Restricted Data Policy should be encrypted at rest.</i> | <i>SAML authentication via ADFS</i> | Not Applicable |
| | <i>Endpoint Security</i> | <i>SentinelOne Agent, Windows Firewall, Cisco IronPort (Edge protection for in-bound email)</i> | | Not Applicable |

Response:

CenturyLink is proposing remotely delivered services (also called hosted or cloud services). These hardware and software requirements are not applicable.

In addition to the standards and preferences included in the above table, one of the factors that the City will consider in procuring new hardware or software is the number of changes that will be required to existing City systems. The fewer the changes the better. It is also preferred that new software use architectures (e.g. database and reporting solutions) building upon or compliant with those already implemented at the City. Similarly, where system integration is required, new software installation should include the implementation of these interfaces, and the Service Provider should identify means of minimizing any changes to the systems being interfaced with.

1. *Requirements specific to Application Packages*

The following requirements will be included in the technical requirements section of each RFP or solicitation document.

| Category | Requirement | Compliant? (Y/N) |
|--|--|-------------------------|
| General Architectural Requirements: | <i>Application must be n-tier architecture, separating data, business logic, and presentation layers (at a minimum)</i> | Not Applicable |
| | <i>Application modules that are part of the proposed product suite shall be extensions of a core product and not an aggregation of acquired products. This requirement applies to all application modules available, not just the ones proposed.</i> | Not Applicable |
| | <i>Functionality shall be grouped around business processes and accessed via interoperable services</i> | Not Applicable |
| | <i>Services shall be engineered to improve agility and to be generic and reusable</i> | Not Applicable |

| Category | Requirement | Compliant? (Y/N) |
|---|---|-----------------------------|
| Data Layer Requirements: | <i>Any disparate system components shall share related data to ensure consistency</i> | Not Applicable |
| | <i>Application components shall share a single, common data model.</i> | Not Applicable |
| | <i>Application components shall share a single, common database.</i> | Not Applicable |
| | <i>Application shall have the ability to archive and purge data that has reached aging limits defined by the City</i> | Not Applicable |
| Reporting Requirements: | <i>Data dictionary with table and field descriptions shall be available that can be used for internal custom report development</i> | Not Applicable |
| | <i>A single, common data repository shall be available that internal reports can be developed against.</i> | Not Applicable |
| | <i>Packaged reporting capabilities shall include imbedded report distribution management capabilities.</i> | Not Applicable |
| | <i>In addition to built-in, packaged reporting, the application shall provide an ad-hoc reporting capability that is end-user friendly and can produce data exports for additional analysis within external tools such as Microsoft Excel.</i> | Not Applicable |
| Integration Requirements: | <i>Application shall provide the ability to interact with other systems via flat files, staging tables, functionally oriented web services, and/or application programming interfaces (API's)</i> | Not Applicable |
| | <i>All available integration channels shall be itemized and described in program documentation</i> | Not Applicable |
| | <i>Application shall support external flat file import of historical data to accommodate migration of existing information into the system.</i> | Not Applicable |
| Application Configuration Requirements | <i>The City shall have the option to adjust the behavior of application components to meet future business needs through direct manipulation of an explicit business process model, making design manageable by business users without the need for substantial IT support.</i> | Not Applicable |
| | <i>Vendor modifications / updates to the application shall be delivered via a consistent, pre-defined process that includes complete instructions on how modifications shall be applied to the City of Charlotte code environment.</i> | Not Applicable |
| Security Requirements Overview: | <i>The City of Charlotte is committed to protecting its information resources from accidental or intentional intrusion. To accomplish this, the City will require Information Security features be included with software/hardware purchases, etc (e.g. access permissions, encryption for restricted data and data that passes from trusted to untrusted networks, common authentication (Active Directory)). Please describe the security capabilities of the proposed technology, and your company's security procedures to include handling of electronic data, hard copy information, and employee security. If the software/hardware will process credit cards, please include PCI and PA-DSS compliance letters. Specific Information Security policies, procedures, and standards can be supplied upon request.</i> | Not Applicable |

| Category | Requirement | Compliant? (Y/N) |
|--|--|-----------------------------|
| Security Requirements Detail: | <i>Security-related patches to supported operating systems shall be supported by the application within two weeks of operating system patch release. If OS patch cannot be supported, mitigation steps must be provided.</i> | Not Applicable |
| | <i>Application shall use windows login credentials for authentication</i> | Not Applicable |
| | <i>Access levels shall be definable to restrict use of system level functions (such as user authorization), and to provide data access levels to restrict the use of data entry, data approval, data retrieval, data modification, database structure creation or modification functions.</i> | Not Applicable |
| | <i>The server-side components of any Citizen-facing capability shall be able to be isolated and segregated from the rest of the server environment so additional security measures can be applied to it.</i> | Not Applicable |
| Operational Requirements: | <i>Procedures and mechanisms for performing both online and offline application backups shall be available</i> | Not Applicable |
| | <i>If the application requires any batch job processing, native scheduling and schedule management capabilities shall be provided</i> | Not Applicable |
| | <i>Application monitoring and logging capabilities shall be available to report / alert on things like performance bottlenecks, failed/hung processes, communication failure, etc. Monitoring shall include all aspects of the solution environment, such as application server, database, and operating system.</i> | Not Applicable |
| | <i>Application shall respond to any end-user requests within 4 seconds.</i> | Not Applicable |
| | <i>Server mail notifications shall support SMTP according to specification FRC 2821.</i> | Not Applicable |
| Disaster Recovery Requirements: | <i>The Service Provider must indicate the capability to recover from natural, human-caused, and electronic disasters (including security compromises) that could interrupt service to the City and the City's customers. The Service Provider will detail their solution to include:</i> | Not Applicable |
| | <i>Procedures for off-site storage of information;</i> | Not Applicable |
| | <i>Capabilities and availability of alternate processing, communications, and operations facilities;</i> | Not Applicable |
| | <i>Plans for maintaining business processes, including communications with the City, the City's customers, and suppliers of goods and services.</i> | Not Applicable |
| | <i>Estimated time to recover from disaster events, and service level expectations for business continuity following a disaster;</i> | Not Applicable |
| | <i>Cost to the City, if any, for disaster recovery services; and</i> | Not Applicable |
| | <i>A documented disaster recovery and business continuity plan, including dates of disaster recovery tests and schedule for future tests.</i> | Not Applicable |
| <i>Procedures for off-site storage of information;</i> | Not Applicable | |

| Category | Requirement | Compliant? (Y/N) |
|--------------------------------|--|------------------|
| Additional Information: | <i>Itemization of all software required to run this application (server & client) shall be included within the proposal. Example: database server, application server, java, .net, compilers, runtime engines, etc. If there is a separate cost associated with supporting software, this fact shall be clearly noted in the proposal, and estimates of those costs shall be provided if possible.</i> | Not Applicable |
| | <i>In addition to the above information submit a complete system architecture diagram showing all hardware recommended for the system. For each server or other hardware shown in the architecture diagram, provide complete recommended specifications.</i> | Not Applicable |

Response:

CenturyLink is proposing remotely delivered services (also called hosted or cloud services). These application requirements are not applicable.

2. *Software Customizations*

The City generally differentiates customization and configuration of software as follows:

Customization: requires software code changes, generally done by the vendor, must be readdressed if the software is upgraded

Configuration: implies no code changes, can be performed by the customer through a user interface and are capable of being ported to new releases of vendor software

Where possible, the City prefers solutions that do not have to be customized to meet business requirements. Configuration changes to meet requirements are an acceptable alternative.

Response:

The CenturyLink solution uses several different software tools to remotely deliver service to the City. Whether customizations are “customization” or “configuration” as defined above, CenturyLink will perform the necessary tasks. Our objective, like the City’s, is that most customizations are “configuration.” These software customizations requirements are not applicable.

3. *Service Oriented Architecture.*

The City is implementing a Service Oriented Architecture and prefers new technologies that apply the following Service Oriented Architecture elements:

- *The system groups functionality around business processes and provides access to this functionality via interoperable services*
- *Supplied services are engineered to improve system agility and to be generic and reusable*
- *Disparate system components share related data to ensure consistency*
- *Web services or integration delivered as part of a COTS application should adhere to City of Charlotte SOA Standards and Development Guidelines (available upon request)*
- *Web services or integration developed for the City of Charlotte as part of any engagement must adhere to City of Charlotte SOA Standards and Development Guidelines (available upon request)*

Response:

CenturyLink is proposing remotely delivered services (also called hosted or cloud services). These architecture requirements are not applicable.

4. *Compliance with State and Federal Procurement Law*

The City intends to comply with all state and federal laws and regulations that apply to this procurement. If any entity interested in submitting a Proposal believes that any of the requirements or standards included in this RFP violate state or federal law, it is incumbent on such entity to bring this concern to the attention of the City contact identified in Section 2.3 of this RFP, on or before the deadline stated in this RFP for submitting questions.

Response:

CenturyLink fully complied. CenturyLink did not identify a requirement or standard of this procurement that we believed violated State or Federal law before the deadline.

5. *Source Code Escrow*

Depending on the nature of the procurement, the City may require the Technology Provider to deliver all source code for the Software to a source code escrow agent approved by the City. If the Technology Provider will be creating Customizations for the City, the City may (again depending on the nature of the procurement) require the Technology Provider to deliver the source code for such Customizations to the City as a condition of acceptance. If applicable, requirements regarding source code will be included either in the proposed Contract included with this RFP, or in the technical requirements section of this RFP.

Response:

CenturyLink is proposing remotely delivered services (also called hosted or cloud services). If issues arise with software that we use to deliver the service, it is CenturyLink's responsibility to rectify the issue. Source code escrow by the City is not applicable.

6. *Support and Maintenance*

During the period of time the Software is in use, the Software Provider shall provide to the City Maintenance Services, subject to the terms outlined elsewhere in the RFP.

The City prefers that maintenance fees begin no earlier than the Date of Acceptance.

Response:

CenturyLink is proposing remotely delivered services (also called hosted or cloud services). Maintenance and support agreements for software providers that we use to deliver the service are a CenturyLink responsibility. This requirement is not applicable.

7. *Public Records Requirements*

To ensure compliance with North Carolina public records laws, the Technology Provider agrees that:

- *In accordance with the North Carolina electronic data-processing records law N.C.G.S. §1326-1:*

All software and documentation provided by the Technology Provider or its subcontractors will have sufficient information and capabilities to enable the City to permit the public inspection and examination and to provide electronic copies of public records stored, manipulated or retrieved by the System; and

All software and documentation provided by the Technology Provider or its subcontractors will have sufficient information to enable the City to create an index containing the following information with respect to each database used by the System without extraordinary commitments of staff or resources: (i) annotated list of data fields: name, description, and restricted field indicator; (ii) description of the format or record layout; (iii) frequency with which the database is updated; (iv) list of any data fields to which public access is restricted; (v) description of each form in which the database can be copied or reproduced; (vi) title of the database; (vii) owner of the data; (viii) narrative description of the database; (ix) person creating the index; and (x) purpose of the database. The Technology Provider agrees that the information set forth in the preceding sentence constitutes a public record and may be disclosed by the City without the Technology Provider's consent.

Response:

CenturyLink is proposing remotely delivered services (also called hosted or cloud services). We are not providing software or any material amount of document, other than the Operating Guide. This requirement is not applicable.

8. DATA AND NETWORK SECURITY

8.1 Data Security and Privacy.

- 8.8.1. Contract Data.** *The parties acknowledge that the City has exclusive ownership of all Contract Data. The Company will treat the Contract Data as Confidential Information under the Confidentiality Requirements. The Company will not reproduce, copy, duplicate, disclose, or use the Contract Data in any manner except as necessary to perform this Contract.*
- 8.8.2. General Requirements.** *With respect to Contract Data, the Company shall: (i) establish and maintain safeguards against the destruction, loss, unauthorized alternation of or unauthorized access to the Contract Data; (ii) comply with all laws and regulations that may apply to the Contract Data including, without limitation, all laws relating to identity theft; (iii) store all Contract Data in accordance with Peripheral Component Interconnect (or successor) standards then in effect; (iv) encrypt all personally identifiable information and credit card data that is transmitted to or from the Company's systems in connection with this Contract; (v) ensure that Contract Data storage complies with all relevant laws, regulations and standards, including but not limited to, states laws, and applicable regulatory and professional standards; and (vi) ensure that transmission of Contract Data to and from the Company's system is secure.*
- 8.8.3. Authentication.** *The Company will require an authentication process approved by the City as a condition to releasing Contract Data to City employees. At a minimum, such process will require a City user ID and password. It may also require validation challenge questions if specified by the City in writing from time to time.*
- 8.8.4. Preventing Unauthorized Access.** *The Company shall identify in writing a security administrator to coordinate with the City. The Company shall take appropriate measures to protect against the misuse of and/or unauthorized access to the Contract Data, including the use of passwords and validated user identification for Company employees. The Company will take appropriate measures to address any such misuse or unauthorized access.*
- 8.8.5. If Unauthorized Access is suspected.** *The Company shall promptly investigate any suspicion or allegation of misuse or unauthorized access to Contract Data. If the Company learns or has reason to believe that Contract Data has been disclosed or accessed by an unauthorized party, the Company shall notify the City immediately and shall take at the Company's expense all remedial action required by law or as reasonably requested by the*

City to remedy such disclosure or unauthorized access. All remediation for third party software security vulnerabilities that are clearly identified as such by the Company are the responsibility of the third party to provide. This in no way limits the Company's responsibility for notifying the City of the identified vulnerability.

- 8.8.6. City's Right to Obtain Contract Data.** *The Company shall provide the City with prompt access to Contract Data when requested (subject to the authentication requirements referenced herein), which such access shall in any event be within three (3) business days after the request. The Company shall retain all Contract Data through the duration of this Contract. When requested by the City from time to time, the Company shall provide the City with a copy of all Contract Data accumulated to date (or such smaller subset as may be requested by the City) in a format in which the City can use, search, copy and access the Contract Data. Within thirty (30) days after expiration or termination of this Contract for any reason, the Company shall: (a) return all Contract Data to the City in a format in which the City can use, search, copy and access the Contract Data; and (b) following such return destroy all copies of the Contract Data in the Company's possession, except to the extent the Company is required to maintain copies of such Contract Data by state or federal law or regulation. If requested by the City, the Company shall allow the City access to the Company's systems if reasonably needed to use, search, and copy or access the Contract Data. The Company shall comply with its obligations under this Section at no cost to the City.*
- 8.8.7. Contract Data to Remain in the U.S.** *The Company will ensure that all Contract Data remains within the confines of the United States including any backup data, replication sites, and disaster recovery sites.*
- 8.8.8. Right of Audit by City.** *The City shall have the right to review the Company's information security program prior to the commencement of Cloud Services and from time to time during the term of this Agreement. During the performance of the Cloud Services, on an ongoing basis from time to time and without notice, the City, at its own expense, shall be entitled to perform, or to have performed, an on-site audit of the Company's information security program. In lieu of an on-site audit, upon request by the City, the Company agrees to complete, within 45 days of receipt, an audit questionnaire provided by Customer regarding Service Provider's information security program.*
- 8.2 Other Security Constraints.** *In order to assist the Company to comply with the City's requirements regarding security under the Contract, Company's security strategy will be to protect Contract Data at multiple levels, which includes data security, data integrity, and data privacy.*
- 8.2.1 Hosting Facility Security.** *All servers and network equipment are housed in locked cabinets at the hosting facility which provides 24x7 security. To access the cabinets there must be several levels of security that must be passed where each entry point provides state of the art card readers, scanners, and other access devices.*
- 8.2.2 Network Security.** *Company's network must be protected by redundant firewalls and monitored for unauthorized access. City access will be configured through a dedicated VLAN. Firewall logs must be constantly monitored, and the logs reviewed on a regular basis. Leading-edge firewall equipment must be provided by the Company to protect the network. The network must be architected to be highly reliable and redundant. If a router, load balancer, or firewall should fail, there must be redundancy built in that would allow failover to take place, without causing a loss of service to our customers. Company shall use ssh encryption via RSA (ssh1) and DSA (ssh2) public keys for communication between servers or as otherwise directed by the City's Project Manager.*
- 8.2.3 Firewall Management.** *Within Company's data centers, the Company shall complete the following firewall management activities: (i) monitoring and management of firewall appliances, and VPN connectivity to the Company data centers; (ii) VPN City connectivity to the City's on-premise firewall; (iii) management of firewall firmware upgrades; (iv) get*

approval from the City before making any changes to the firewall configuration; (v) logging for the firewall and servers shall be sent to the City SIEM solution at the City's discretion; (vi) in the event Company identifies a suspected security breach, Company will notify the City of the breach immediately; (vii) provide check point firewall, IPS and web security logs via OPSEC integration with the hosted check point SmartCenter; and (viii) restrict database users to controlled lists, individual activities to be restricted, logged and monitored.

- 8.2.4 *Server Security. The City's installation will be implemented on dedicated virtual or physical servers, meaning these server environments will be used for and accessible only by the City of Charlotte and Company staff;*
- 8.2.5 *Anti-Virus. Company shall complete the following activities: (i) install anti-virus software on Company managed servers; (ii) maintain all anti-virus and anti-spam system with the latest patches, engines and heuristics; and (iii) scan, quarantine and clean all in-bound and out-bound files (including email attachments) for viruses.*
- 8.2.6 *Cloud Services Security. Company shall provide that Customers that access any applicable Cloud Services must use password authentication. The design of the application must be robust so as to prevent one of the Company's customers from accessing another customer's data. There must be several layers of protected servers that stand between the web page where the customer logs in and the actual data.*
- 8.2.7 *Security Patches. Where it does not impact application supportability, security patches to Platform Software will be applied within 6 months of being released.*
- 8.2.8 *Passwords. Company must use tightly controlled passwords on its servers and network equipment. Passwords must be changed on a regular basis. Company's Platform Software shall not share the same passwords.*

Response:

While CenturyLink believes we substantially comply with the preceding section, CenturyLink respectfully takes exception to this Section until the parties are able to discuss the final solution and negotiate applicable terms and conditions.

C. Addenda Receipt Confirmation

Required Form 3 “Proposal Submission Form” is provided on the following pages.

Response:

Required Form 2 “Addenda Receipt Confirmation” is provided on the following pages.

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

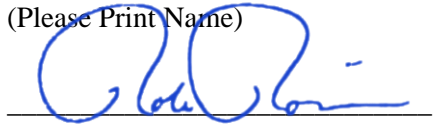
**DATE ADDENDUM
DOWNLOADED FROM NC IPS:**

6/28/19

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

Rob Robinson

(Please Print Name)



Authorized Signature

July 15, 2019

Date

on behalf of Dennis Fisher, Director,
Pricing and Offer Management

Title

CenturyLink Communications, LLC

Company Name

D. Proposal Submission

Response:

Required Form 3 “Proposal Submission Form” is provided on the following pages.

REQUIRED FORM 3 – PROPOSAL SUBMISSION FORM
RFP # 269-2019-109

Managed Security Services This Proposal is submitted by:

Company Name: CenturyLink Communications, LLC

Representative (printed): Rob Robinson, on behalf of Dennis Fisher, Director, Pricing & Offer Management

Address: 11006 Rushmore Drive
Suite 200

City/State/Zip: Charlotte, NC 28227

Email address: Rob.Robinson@CenturyLink.com

Telephone: (704) 213-4113
(Area Code) Telephone Number

Facsimile: _____
(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: L

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):  _____

* CenturyLink complies with all applicable civil rights, human rights, immigration and labor laws. This includes providing equal employment opportunities to job applicants and employees, and maintaining a workplace free from illegal discrimination, harassment and retaliation. To the best of our knowledge there has not been a complaint filed or pending regarding discrimination of a subcontractor, vendor or supplier.



E. Pricing Worksheet

Response:

Required Form 4 “Pricing Worksheet” is provided on the following pages.

**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.

The Pricing Worksheet can be found in Excel spreadsheet in Attachment A- Pricing Worksheet and Specifications found at the following website:

<https://charlottenc.gov/DoingBusiness/Pages/ContractOpportunities.aspx>.

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 | Comments |
| 1.0 | Security Operations Services | \$ 87,002.41 | \$ 87,002.41 | \$ 87,002.41 | \$ 87,002.41 | \$ 87,002.41 | |
| 1.1 | Core Security Operations Services | \$ 17,220.00 | \$ 17,220.00 | \$ 17,220.00 | \$ 17,220.00 | \$ 17,220.00 | Plus non-recurring charge shown below. |
| 1.2 | Analytics Platform Operations | \$ 6,420.00 | \$ 6,420.00 | \$ 6,420.00 | \$ 6,420.00 | \$ 6,420.00 | This item should not be considered an optional selection. It is required for effective Security Log Monitoring. |
| 1.3 | Email Threat Monitoring and Analysis | \$ 5,078.40 | \$ 5,078.40 | \$ 5,078.40 | \$ 5,078.40 | \$ 5,078.40 | MRC is based on 9,200 Users. |
| 1.4 | Cyber Intelligence Support | \$ 10,800.00 | \$ 10,800.00 | \$ 10,800.00 | \$ 10,800.00 | \$ 10,800.00 | |
| 1.5 | Security System Support | \$ - | \$ - | \$ - | \$ - | \$ - | Security System Support can be satisfied by the same staff providing Onsite Services (1.6). |
| 1.6 | Onsite Services | | | | | | |
| 1.6.1 | Onsite Tier 3 Infrastructure Security Engineer | \$ 23,174.86 | \$ 23,174.86 | \$ 23,174.86 | \$ 23,174.86 | \$ 23,174.86 | 160 Hours/month |
| 1.6.2 | Onsite Tier 3 Cyber Security Analyst | \$ 17,474.29 | \$ 17,474.29 | \$ 17,474.29 | \$ 17,474.29 | \$ 17,474.29 | 160 Hours/month |
| 1.6.3 | Onsite Information Security Engineering support | \$ 2,334.86 | \$ 2,334.86 | \$ 2,334.86 | \$ 2,334.86 | \$ 2,334.86 | 16 Hours/month |
| 1.7 | Threat Hunting | \$ 4,500.00 | \$ 4,500.00 | \$ 4,500.00 | \$ 4,500.00 | \$ 4,500.00 | |
| 1.8 | Compromise Assessment | \$ - | \$ - | \$ - | \$ - | \$ - | Plus non-recurring charge shown below. |
| Non-Recurring Charges | | Year 1- Non Recurring Cost | Year 2- Non Recurring Cost | Year 3- Non Recurring Cost | Optional Renewal Year 1- Non Recurring Cost | Optional Renewal Year 2- Non Recurring Cost | |
| 1.1 | Core Security Operations Services | \$ 35,400.00 | \$ 35,400.00 | \$ 35,400.00 | \$ 35,400.00 | \$ 35,400.00 | Non-recurring charges are billed once at beginning of year. CenturyLink may consider amortizing the NRCs upon further discussion. |
| 1.8 | Compromise Assessment | \$ 23,600.00 | \$ 23,600.00 | \$ 23,600.00 | \$ 23,600.00 | \$ 23,600.00 | Non-recurring charges are billed once at beginning of year. CenturyLink may consider amortizing the NRCs upon further discussion. |

| 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 | Comments |
| 2.0 | Network Operations Center (NOC) | \$ 74,779.00 | \$ 74,779.00 | \$ 74,779.00 | \$ 74,779.00 | \$ 74,779.00 | MRC includes ebonding maintenance charges if required. |
| | | Year 1- Non Recurring Cost | Year 2- Non Recurring Cost | Year 3- Non Recurring Cost | Optional Renewal Year 1- Non Recurring Cost | Optional Renewal Year 2- Non Recurring Cost | Non-recurring charges are billed once at beginning of year. CenturyLink may consider amortizing the NRCs upon further discussion. |
| 2.1 | Non-Recurring Services (One-Time Charge) | \$ 271,689.00 | \$ 18,334.00 | \$ 18,334.00 | \$ 18,334.00 | \$ 18,334.00 | Year 1 NRC includes \$79,000 for ebonding if required. |
| 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 | Comments |
| 3.0 | Applications Monitoring | \$ 50,184.00 | \$ 50,184.00 | \$ 50,184.00 | \$ 50,184.00 | \$ 50,184.00 | |
| | | Year 1- Non Recurring Cost | Year 2- Non Recurring Cost | Year 3- Non Recurring Cost | Optional Renewal Year 1- Non Recurring Cost | Optional Renewal Year 2- Non Recurring Cost | Non-recurring charges are billed once at beginning of year. CenturyLink may consider amortizing the NRCs upon further discussion. |
| 3.1 | Non-Recurring Services (One-Time Charge) | \$ 393,342.00 | \$ 354,056.00 | \$ 354,056.00 | \$ 375,299.00 | \$ 375,299.00 | Non-recurring charges for Years 4 and 5 are not to exceed charges. At time of request - if CenturyLink can obtain improved pricing from suppliers charges will be adjusted. |

| Additional Hourly Labor Pricing |
|--|
| Labor rate card can be supplied upon request |

F. MWSBE Utilization

Response:

Required Form 5 “MWSBE Utilization” is provided on the following pages.



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: | CenturyLink Communications, LLC |
|----------------------|---------------------------------|

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):

Reviewed information found at <https://charlotte.diversitycompliance.com>. Using commodity codes identified potential candidate firms for inclusion. Contacted nine (9) firms by email. Obtained acceptable proposals from two (2).

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):

If the candidate MWSBE firms prove unsuitable, CenturyLink will identify and contract suitable replacements.

[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 # |
|------------------------------------|----------------------------------|--------------------------------------|---------------|
| Trinity Strategic Consulting, Inc. | Requirements 13.1, 13.2 and 13.4 | M, S | |
| JCMR Technology, Inc. | Requirements 13.1, 13.2 and 13.4 | S | |
| | | | |
| | | | |

| | |
|--------------------------------|--------------|
| Total MBE Utilization | % |
| Total WBE Utilization | % |
| Total SBE Utilization | % |
| Total MWSBE Utilization | 46.8% |

Representative (signed):  _____

July 15, 2019
Date

Rob Robinson, *on behalf of Dennis Fisher,*
Director, Pricing and Offer Management
Representative Name

Estimated Total Contract Value

G. Company's Background Response

Response:

Required Form 6 "Company's Background Response" is provided on the following pages.

**REQUIRED FORM 6 – COMPANY’S BACKGROUND RESPONSE
RFP # 269-2019-109**

Managed Security Services

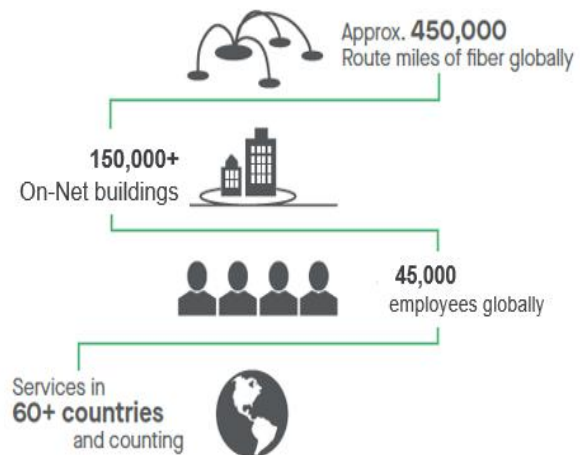
Companies shall complete and submit the form below as part of their response to this RFP. Additional pages may be attached as needed to present the information requested.

| Question | Response |
|--|---|
| Company’s legal name | CenturyLink Communications, LLC |
| Company Location (indicate corporate headquarters and location that will be providing the Services). | 100 CenturyLink Drive Monroe, LA 71203 |
| How many years has your company been in business? How long has your company been providing the Services as described in Section 3? | CenturyLink was incorporated in 1968 and has been in business for over 50 years. CenturyLink has been providing the services described in Section 3 for longer than 10 years. |
| 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). | We service more than 500 State and Local government customers. |
| List any projects or services terminated by a government entity. Please disclose the government entity that terminated and explain the reason for the termination. | Due to the size of CenturyLink and the number of CenturyLink customers, there have been contract terminations for various reasons but to the best of its knowledge, none have been terminated based upon a finding of a breach of contract or that would otherwise affect CenturyLink’s performance of the services requested herein.. |
| List any litigation that your company has been involved with during the past two (2) years for Services similar to those in this RFP. | Due to size of CenturyLink, various suits, proceedings, and claims typical for an enterprise business can be pending against CenturyLink at any one time. While it is not possible to determine the ultimate disposition and resolution of any suits, proceedings or claims, and whether they are consistent with CenturyLink's position, CenturyLink expects the outcome of such proceedings, individually |

| | |
|---|--|
| | <p>or in aggregate, will not have a materially adverse effect on the financial condition or results of CenturyLink operations or its business segments; nor negatively affect its ability to provide the services proposed.</p> <p>As a public corporation, CenturyLink is required to fully disclose material data and relevant information that may influence investment decisions to all investors at the same time. CenturyLink does not provide detailed information on litigation except through its securities filings. Please refer to CenturyLink's Annual Report on Form 10-K, available on http://www.centurylink.com/ for a description of certain litigation or claims.</p> |
| <p>Provide an overview and history of your company.</p> | <p>See below.</p> |
| <p>CenturyLink (NYSE: CTL) is the second largest U.S. communications provider to global enterprise customers. With customers in more than 60 countries, approximately 450,000 route miles of fiber globally and an intense focus on the customer experience, CenturyLink strives to be the world's best networking company by solving customers' increased demand for reliable and secure connections. The company also serves as its customers' trusted partner, helping them manage increased network and IT complexity and providing managed network and cybersecurity solutions that help protect their business.</p> <p>CenturyLink provides an integrated array of network solutions and services to business and residential customers. Our services include virtual private network (VPN), data network, private line (including business data services), Ethernet, information technology, wavelength, broadband, colocation and data center services, managed services including cybersecurity, local and long-distance voice, professional and other support services in connection with selling equipment, and network security.</p> <p>Incorporated in Louisiana in 1968, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America's largest corporations. We have a strong employee base of approximately 45,000 providing world-class services that exceed customers' expectations for quality, value, and reliability.</p> <p>CenturyLink understands the power of the digital world is related to our customers' specific needs – that life is powered by connections, and business is powered by connections. Consumers and businesses alike benefit from our fiber-rich network coupled with our commitment to delivering an outstanding customer experience.</p> | |

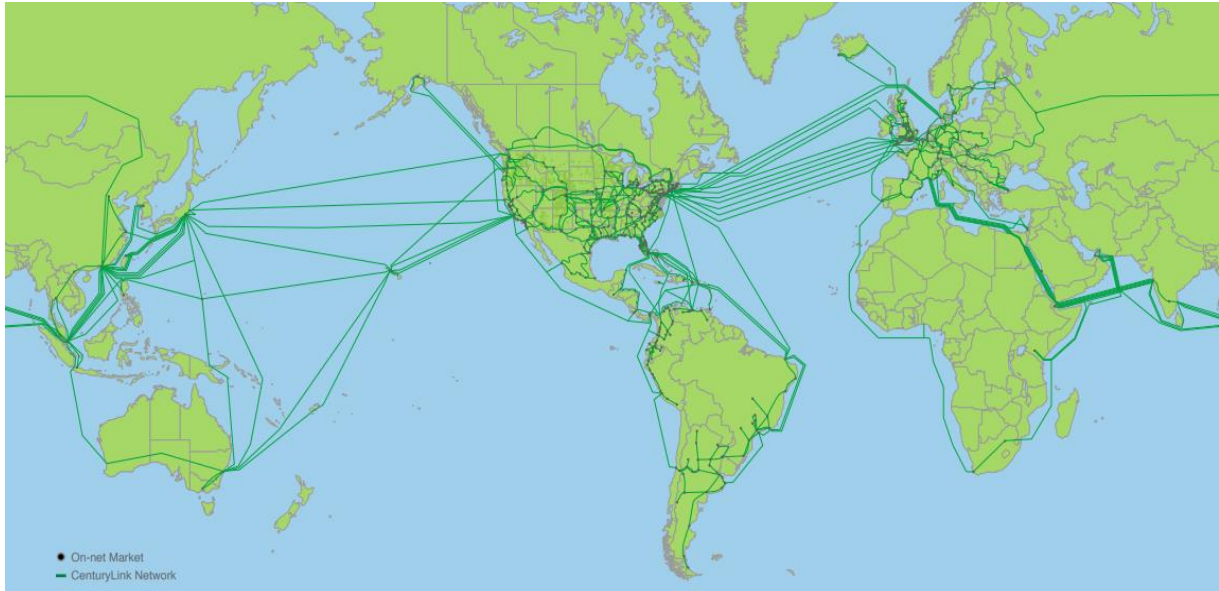
CenturyLink can help you on your digital transformation journey through:

- An extensive local reach with significant local presence
- Reliable and secure connections when, where, and how you need them
- Best-in-class network security, with scale that allows us to see more traffic and proactively thwart potential threats before they become breaches
- An expanded portfolio of innovative, adaptive technology solutions for choice and control
- Access to talented employees and partners
- Financial stability to serve as a reliable resource for your business
- A relentless focus on the customer experience with an unwavering commitment to your success



CenturyLink is a global leader in the network services market, having been recognized by key industry analyst firms for its technologies and robust network; the company is also a global leader in cloud infrastructure and hosted IT solutions for enterprises. CenturyLink provides a complete suite of products and service to support traditional and converged communications, networking, hosting, cloud, storage, security, and disaster recovery/business continuity (DR/BC) solutions on a global basis. We can provide standalone, enterprise-wide, and fully-managed solutions tailored to specific customer requirements.

CenturyLink Network



Meeting the Challenges in the Digital World

Connecting to the power of the digital world is a complex and sometimes overwhelming endeavor. The digital world is in a constant state of technological change and evolution. The Internet of Things (IoT) is becoming more pervasive. The cyber threat landscape continues to expand. All of this impacts our customers' businesses.

CenturyLink is committed to your success. We help you navigate these complexities by providing the collaboration and guidance you need to build the right networking ecosystem for your business. By leveraging our connections and comprehensive adaptive networking solutions, your business success becomes a business reality.



Connectivity

Every business is unique, which is why a combination of network solutions is required to meet your business objectives. Our hybrid connectivity leverages both public and private connectivity options via fiber or the public cloud. Couple that with our security solutions which help ensure reliable and secure access whenever — and virtually wherever — you need it.

Hybrid IT and Cloud

Creating the right networking ecosystem for your organization is an ongoing challenge. To take full advantage of digital transformation, you need to fully leverage the cloud. No matter where you are on your journey to the cloud, CenturyLink can guide you. As a neutral advisor with connections to several premier cloud service providers, our cloud ecosystem gives you both choice and control when selecting cloud connectivity — public, private, or a combination of both.

Managed and IT Services

Whether through cost savings or supporting new revenue streams, IT is being asked to contribute to the business bottom line. Today's IT organization must evolve to succeed — modernize, manage, mitigate and migrate. CenturyLink has the expertise, data, insights and innovation to help customers manage their networks, so they can focus on their core business.

Security

As the cyber threat landscape continues to expand, you can't afford to have a false sense of security. CenturyLink provides a thorough approach to network security, one that is tied to your business's overall networking strategy, enabling a comprehensive view of your networking architecture and threat environment. We see more, so we can stop more.

Real-Time Communications

Your business's success depends on its ability to effectively communicate. However, in a rapidly changing digital landscape, it's not always easy to keep the conversation and collaboration going. CenturyLink includes applications that enable you to get the most out of your connections. From TDM to VoIP, and a full suite of collaboration tools and API capabilities, we can help lower costs and increase productivity.

| | | | | |
|--|--|--|---|---|
|  <p>Connectivity</p> <p>Gain network scalability and workflow agility with a flexible public-private network that connects to the cloud.</p> |  <p>Hybrid IT and Cloud</p> <p>Migrate to hybrid cloud network and technology environments at your own pace.</p> |  <p>Real Time Communications</p> <p>Adopt scalable communication and collaboration solutions that deliver business agility for a mobile workforce.</p> |  <p>Security</p> <p>Protect people, data, and infrastructure against the advancing threat landscape.</p> |  <p>Managed and IT Services</p> <p>Rely on experienced professionals to support transformation.</p> |
|--|--|--|---|---|

Our Purpose

At CenturyLink, we improve lives, strengthen businesses, and connect communities by delivering advanced technologies and solutions with honest and personal service. We strive to be our communities’ first choice to serve their total communications needs, and we earn our customers’ trust by living out our seven unifying principles of fairness, honesty and integrity, commitment to excellence, positive attitude, respect, faith, and perseverance. With a current focus on integration, we are committed to transforming CenturyLink into the one of the world’s leading network providers.

Financial Highlights

CenturyLink has a strong financial standing as evidenced by our most recent earnings results released on May 8, 2019. CenturyLink reported revenues of \$5.647 billion for the first quarter of 2019. As of March 31, 2019, CenturyLink had cash and cash equivalents of \$441 million.

| | |
|---|---|
| <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>CenturyLink is a \$23.5B company with over 42,000 employees.</p> |
| <p>Identify the percentage of revenue used for research and/or development by the proposing company or division.</p> | <p>Less than 1%</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>CenturyLink is not reselling another company’s products in this RFP response. We are using Dynatrace and SolarWinds as tools to assist in the delivery of service.</p> |
| <p>Describe your company’s complete corporate structure, including any parent companies, subsidiaries, affiliates and other related entities.</p> | <p>See below.</p> |
| <p>CenturyLink, Inc. – is the publicly traded parent company of the CenturyLink operating companies. CenturyLink operating companies are described as follows:</p> | |

Interexchange Carriers (IXCs) – provide long distance services, IP voice services (VoIP), SIP trunking, routed services, and other business solutions

- CenturyLink Communications, LLC (Embarq Communications, Inc. and CenturyTel Long Distance, LLC merged into CenturyLink Communications, LLC, effective April 1, 2014)
- CenturyTel Broadband Services, LLC
- Level 3 Communications, LLC (including but not limited to the Level 3 affiliates Level 3 Telecom Holdings, LLC (f/k/a TW Telecom Holdings, Inc.) and Global Crossing Telecommunications, Inc., effective November 1, 2017)

Local Exchange Carriers (LECs) and Regional Bell Operating Companies (RBOCs) – provide local access lines, CPE, dedicated connections, switched services, and other tariffed services in local calling service areas

- Qwest Corporation d/b/a CenturyLink QC (indirect subsidiary of CenturyLink, Inc.) (RBOC operating in 14 states)
- Dozens of ILEC entities operating in 33 states

Competitive Local Exchange Carriers (CLECs) – provide local access lines, CPE, dedicated connections, switched services, Internet Access and other competitive services in local calling service areas

- CenturyLink Communications, LLC (Embarq Communications, Inc. and CenturyTel Long Distance, LLC merged into CenturyLink Communications, LLC, effective April 1, 2014)
- Level 3 Communications, LLC (including but not limited to the Level 3 affiliates Level 3 Telecom Holdings, LLC (f/k/a TW Telecom Holdings, Inc.) and Global Crossing Telecommunications, Inc., effective November 1, 2017)

Describe the ownership structure of your company, including any significant or controlling equity holders.

CenturyLink is a publicly traded company. CenturyLink's complete ownership information is detailed in its 10-K, which can be viewed online here – <http://ir.centurylink.com/sec-filings>

Provide a management organization chart of your company's overall organization, including director and officer positions and names and the reporting structure.

See below.

CenturyLink's corporate organization chart follows:



Describe the key individuals along with their qualifications, professional certifications and experience that would comprise your company's team for providing the Services.

Rob Robinson, *SLED Account Manager*

Rob.Robinson@CenturyLink.com

Home Office (China Grove) – (704) 855-7926

Cell – (704) 213-4113

Your Account Manager is your first point of contact for escalations and the person you would reach out to concerning contact information of other team members, along with any other concerns or issues you may have regarding your account and or service.

Rob has been with CenturyLink for almost 5 years and is a Hybrid Account Manager. He provides support services and solution to customers in both NC and SC in 911/Public Safety, Government, Higher Education and Health Care.

Prior to joining the CenturyLink team in January 2015, he worked for 30 years in Local Government as both a 911 Director and a Sworn Law Enforcement Officer. He is used to working in stressful situations and dealing with critical emergency situations. He retired from Rowan County in 2014 as the 911 Director and in 2018 at a Law Enforcement Officer.

Keefe Leiter, *Sales Engineer*

Keefe.Leiter@CenturyLink.com

Office/Cell – (612) 281-5700

The Sales Engineer works to identify technical options and define technical requirements for service implementation. Understanding your business goals, existing networks, key locations and technical needs, the Sales Engineer provides all technical information about CenturyLink services and

network solutions to support both your existing and future requirements.

The Sales Engineer manages the engineering portion of the service quote, the inventory and capacity process for new orders, and interfaces with CenturyLink Customer Care Managers to ensure timely service delivery. The Sales Engineer provides service/technology consultation and communicates the technical details necessary to implement the services properly.

Keefe Leiter, your Lead Sales Engineer, has a tenured background in providing technology solutions to a wide range of customers in both the Commercial Enterprise and Government verticals. He has held multiple Cisco and Agilent certifications for more than a decade and most recently has been involved in providing complex Managed Security Services to State and Local government entities

Bill Cozart, *Client Support Manager*

William.Cozart@CenturyLink.com

Office – (252) 214-7014

Cell – (252) 258-0469

The CSM is your on-going contact for several different support roles. A CSM will be your point of contact for order review, input and tracking through installation, and reviewing your service to ensure that it is up-to date.

Additional responsibilities include maintaining the account for inventory accuracy, assisting with implementation and review and handling of billing and credits.

| | |
|--|---|
| | <p>Bill has over 18 years with CenturyLink and over 23+ years' experience in the industry.</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>The MWSBE firms are the only subcontractors of significance being used by CenturyLink. They are less than 15% of the services.</p> |
| <p>Explain how your organization ensures that personnel performing the Services are qualified and proficient.</p> | <p>CenturyLink is confident our hiring, training, and promotion practices ensure that highly qualified staff support our customers. Should any CenturyLink personnel supporting the City prove otherwise, please let us know. We will make a change.</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>CenturyLink will staff as required to deliver the services.</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>CenturyLink has not had any disputes or strikes from our organized labor unions within the last five (5) years.</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>CenturyLink's security procedures are too voluminous to describe in the space provided here. In addition to being a leading seller of security services, internally CenturyLink has a mature security policy that is updated annually and rigorously enforced.</p> |



H. References

Response:

Required Form 7 “References” is provided on the following pages.

Info

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.

REFERENCE 1:

Name of Client: State of South Carolina Information and Security Privacy Services

Main Phone: _____

Address: _____

Primary Contact: _____ **Title:** _____

Contact Phone: _____ **Contact E-Mail:** _____

Service Dates: _____

Summary & Scope of Project: _____

Statewide Term Contract for Managed Security Services through 4/21/2022

Targets: governmental units, political subdivision, and higher education institutions (33)

CenturyLink awarded:

– Lot One (1) - Security Monitoring and Analytics Services

– Lot Two (2) - Security Incident Response Management Services

– Lot Six (6) - Application Security Assessment and Remediation Services

Contract Value: \$ _____ **Number of Client Employees:** _____

REFERENCE 2:

Name of Client: State of South Carolina Managed Security Service

Main Phone: _____

Address: _____

Primary Contact: _____ Title: _____

Contact Phone: _____ Contact E-Mail: _____

Service Dates: 6/1/2016 – 5/31/2021

Summary & Scope of Project: _____

Awarded to CenturyLink

MSS Bid Invitation: 5400010377 - MANAGED SECURITY SERVICE

<http://webprod.cio.sc.gov/SCSolicitationWeb/solicitationAttachment.do?solicitnumber=5400010377>

<http://webprod.cio.sc.gov/SCContractWeb/contractDetail.do?solicitNumber=5400010377&contractNumber=4400013117>

Contract 4400013117

Contract Value: \$\$ 19,422,214.00 Number of Client Employees: _____

REFERENCE 3:

Name of Client: Lewis Brisbois Bisgaard & Smith LLP Main Phone: _____

Address: _____

Primary Contact: Tommy Lewis Title: Chief Technology Officer

Contact Phone: _____ Contact E-Mail: tlewis@lbbslaw.com

Service Dates: _____

Summary & Scope of Project: _____

Security Log Monitoring

Contract Value: \$ _____ Number of Client Employees: _____



REFERENCE 4:

Name of Client: _____ Main Phone: _____

Address: _____

Primary Contact: _____ Title: _____

Contact Phone: _____ Contact E-Mail: _____

Service Dates: _____

Summary & Scope of Project: _____

Contract Value: \$ _____ Number of Client Employees: _____

REFERENCE 5:

Name of Client: _____ Main Phone: _____

Address: _____

Primary Contact: _____ Title: _____

Contact Phone: _____ Contact E-Mail: _____

Service Dates: _____

Summary & Scope of Project: _____

Contract Value: \$ _____ Number of Client Employees: _____



I. Additional Company Questions

Response:

Required Form 8 “Additional Company Questions” is provided on the following page(s).

**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?

Response:

CenturyLink uses a proven transition process to smoothly assume responsibility for delivery of services from the current provider and to minimize risk to the City. Transition activities are primarily focused on obtaining the knowledge, especially of processes, to support the existing environment and to effectively interact with the City. This is a multi-phase process:

1. Discovery Phase
 2. Transition Phase
 3. Stabilization Phase
 4. Steady-State Delivery
2. Prepare and submit a Project Plan to describe all times, tasks and resources associated with the performance of Services.

Response:

Please refer to Form 8 Supplement Sample Security Log Monitoring Project.pdf and Form 8 Supplement Sample Monitoring and Management Plan.pdf.

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

Response:

CenturyLink's Business Communications Management process defines how the City and CenturyLink collaborate in defining and understanding the City's communications requirements and development of an integrated communication plan in support of impacted City stakeholder groups.

Audiences will be identified and analyzed to isolate unique needs and associated messaging to enable successful Transition. All approval processes and communication team responsibilities (both CenturyLink and the City) are documented. The resulting schedule will be implemented based on regular open communications with targeted messages to relevant stakeholders.

CenturyLink will work with their City colleagues to develop guiding principles, action items, and key deliverables to enable and support the critical milestones specified in the contract. Key individuals from both organizations may be engaged to support the communication leads, as requested.

Since Transition is the initial foundation for establishing the required relationship the table below is intended to proactively share our envisioned communication matrix for communicating transition status.

| Meeting Type | Frequency | Purpose | Inputs |
|------------------------------|-----------|---|--|
| Executive Steering Committee | • Monthly | <ul style="list-style-type: none"> • Assessment of overall Transition Program. • Establish Strategic directions | <ul style="list-style-type: none"> • Monthly Transition Status Report • Risks and Issue Logs • Escalations • Milestone dates |
| Management Committee | • Weekly | <ul style="list-style-type: none"> • Review Transition Weekly work stream progress against plan. • Review Risk, Issues, Action • Escalation Prioritization | <ul style="list-style-type: none"> • Weekly work stream progress • Risks and Issue Logs • Milestone dates |
| Service Transition Meeting | • Daily | <ul style="list-style-type: none"> • Review daily progress against plan • Review and action Issues • Review and action Risks • Review of | <ul style="list-style-type: none"> • Transition work stream progress • Risks and Issue Logs • Milestone dates |

Frequent and structured communication among the operational support teams is critical for successful steady state delivery. With City input, CenturyLink will craft a communications scheme as part of an overall governance model that best suits the City’s needs.

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

Response:

CenturyLink believes the risks inherent in this contract are low. The services being offered have been proven in productive use at other customers. The great risk is of delay in transition, which is typically attributable to unavailability of key customer personnel due to other priorities.

Effective risk management during Transition is a key differentiator for CenturyLink and a requirement of any integrated plan. It is intrinsic to what CenturyLink does. CenturyLink will take a stringent, unwavering approach to risk management, leveraging technology and a structured set of tools and proven processes to keep risks from jeopardizing the City’s business.

Risks will be captured as they are identified over the course of the Transition phases using an agreed-on risk management system. Formal risk reviews will be performed both at prescribed points and on an ad hoc basis. CenturyLink’s risk management approach enables reporting,

assessment, assignment, and monitoring of resolution and action plans throughout the project. It will also provide for a smooth transfer of any open risks or issues to the ongoing support team at transition exit.

CenturyLink will conduct a risk identification workshop with the City at an early stage in Transition to jointly identify potential risks and establish risk mitigation plans. Owners will be assigned to the identified risks, and they will be responsible for conducting risk impact analyses, establishing mitigation and containment plans, and conducting risk response planning. Together, CenturyLink and the City will institute a process of periodically monitoring these risks, taking necessary mitigation actions and updating the risk management plans.

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>.

Response:

“Application Performance Monitoring and NOC Performance Monitoring worksheet in Attachment A – Pricing Worksheet and Specifications” are provided on the following pages.

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 | |

| Section | Key Requirements - Application Performance Monitoring | Critical | Can provide | Cannot Provide |
|---------|---|--------------|-------------|----------------|
| 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 | |

| Section | Key Requirements - Application Performance Monitoring | Critical | Can provide | Cannot Provide |
|---------|--|--------------|-------------|----------------|
| 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 | | | |

J. Certification Regarding Debarment, Suspension and Other Responsibility Matters

Response:

Required Form 9 “Certification Regarding Debarment, Suspension and Other Responsibility Matters” is provided on the following page(s).

**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:

Rob Robinson

(Print Name)



Signature

*on behalf of Dennis Fisher, Director,
Pricing and Offer Management*

Title

July 15, 2019

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

K. Byrd Anti-Lobbying Certification

Response:

Required Form 10 “Byrd Anti-Lobbying Certification” is provided on the following page(s).

REQUIRED FORM 10 – BYRD ANTI-LOBBYING CERTIFICATION
RFP # 269-2019-109

Managed Security Services

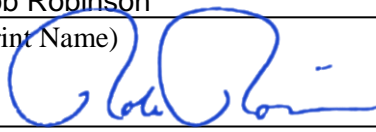
The undersigned certifies, to the best of his or her knowledge and belief, that:

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.

CenturyLink Communications, LLC (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.

Rob Robinson
(Print Name)


Authorized Signature

July 15, 2019
Date

CenturyLink Communications, LLC
Company Name

11006 Rushmore Dr, Suite 200
Address

Charlotte, NC 28227
City/State/Zip

L. Exceptions to the Remainder of the RFP, including Sample Contract in Section 7

Exceptions must be submitted in accordance with Section 1.6.12 of this RFP. If exceptions are not identified in your Proposal they may not be considered during Contract negotiation and could result in Proposal being rejected from further consideration. If legal counsel needs to review the Sample Contract prior to signature, reviews must be completed before your Proposal is submitted.

The City intends to enter into a City-drafted Contract with the successful Company that contains the terms and conditions set forth in Section 7 (“Sample Terms”). The number and extent of any exceptions and proposed additions to the Sample Terms will be one of the City’s evaluation criteria.

Accordingly, each Company must state specifically in its Proposal any exceptions to the Sample Terms, or any such exceptions will be waived. Any Company-proposed additional terms or conditions must also be included in the Proposal, and the City reserves the right to refuse consideration of any terms not so included. Any proposed changes to the Sample Terms after tentative contract award may constitute a material change to the Company’s Proposal and be grounds for revoking the award. Notwithstanding the foregoing, the City reserves the right to modify the Sample Terms prior to or during contract negotiations if it is in the City’s best interest to do so.

EXCEPTIONS:

As permitted by Sections 1.6.12 and 4.1.4, CenturyLink respectfully takes the following exceptions to the RFP terms and conditions and Sample Contract. If awarded, CenturyLink is committed to negotiating an agreement containing mutually acceptable terms and conditions that addresses both parties’ concerns and potentially utilizing the City’s Sample Contract with mutually agreeable terms and conditions. Upon request or for the City’s convenience, CenturyLink can provide a redlined version of the Sample Contract including the below requests during negotiations.

RFP Terms and Conditions:

1. CenturyLink respectfully takes exception to Section 1.6.2 of the RFP, Trade Secrets and PPI, as it relates to PII and indemnification obligations. At this time, CenturyLink does not believe PII will be accessible with our proposed solution. If awarded, CenturyLink is willing to negotiate this Section.
2. CenturyLink respectfully takes exception to Section 8 of the RFP Data Network and Security, at this time, as CenturyLink has provided service exhibits specifically applicable to the services proposed in CenturyLink’s response and adequately protect the State’s interest while also describing the solution and process requirements. If awarded, CenturyLink is willing to negotiate this Section to include provisions to adequately protect both parties’ interests.
3. CenturyLink respectfully takes exception to Section 5, Source Code Escrow, as CenturyLink is not proposing a software solution and does not believe this section is applicable.

Sample Contract Terms and Conditions:

1. CenturyLink respectfully takes exception to Section 1 of the Sample Contract as CenturyLink has provided service exhibits with its response detailing the services proposed in CenturyLink’s response. Since each service is provisioned differently and each exhibit has more specific terms, the exhibits are drafted to take precedence over the broader contract terms. Thus, until the

parties can negotiate a mutually agreeable contract, CenturyLink takes exception, but is willing to negotiate this Section upon award.

2. CenturyLink respectfully takes exception to Section 4.7 to the extent it requires reimbursement for audit expenses. CenturyLink requests further clarification as to extent of this audit and reimbursement requirement. CenturyLink is willing to negotiate this Section upon award.
3. CenturyLink respectfully takes exception to Section 12 and offers that Customer may request, and CenturyLink will consider in good faith, replacement of an Account Team member based on specific, reasonable, and lawful objections or concerns as to the Account team member's performance or performance failures. If Customer is not satisfied that its Account Team meets Customer's needs, customer must provide CenturyLink with written notice of Customer's concerns, and CenturyLink will use commercially reasonable efforts to address Customer's concerns within thirty (30) days of receipt of written notice.
4. CenturyLink respectfully takes exception to Section 18.4 at this time and until it is determined through further discussions the applicability. CenturyLink agrees to negotiate in good faith.
5. CenturyLink respectfully takes exception to Section 18.5 only to the extent required of subcontractors, but CenturyLink is willing to negotiate this Section upon award.
6. CenturyLink respectfully takes exception to Section 19 to the extent it provides cost of cover, the ability to withhold payment or set off, or requires specific performance as such remedies may not be practicable considering the nature of services requested. Thus, until the parties can negotiate a mutually agreeable contract, CenturyLink takes exception, but is willing to negotiate this Section upon award.
7. CenturyLink respectfully takes exception to Section 23, City Ownership of Work Product. CenturyLink has provided its language regarding this subject in the response and requests that any city ownership be limited to Work Product designed specifically and exclusively for the City. CenturyLink is willing to negotiate this Section upon award.
8. CenturyLink respectfully takes exception to Section 25, Indemnification to comply with CenturyLink's policies and procedures. Thus, until the parties can negotiate a mutually agreeable contract, CenturyLink takes exception, but is willing to negotiate this Section upon award and include an Indemnification provision that adequately protects both parties' interests.
9. CenturyLink respectfully takes exception to Section 27, Confidential Information and proposes the language attached in CenturyLink's Master Services Agreement and Service Exhibits. Thus, until the parties can negotiate a mutually agreeable contract, CenturyLink takes exception, but is willing to negotiate this Section upon award to include a provision that adequately protects both parties' interests.
10. CenturyLink respectfully takes exception to Section 31.5 to the extent it includes a unilateral waiver of consequential damages. CenturyLink respectfully requests the waiver be mutual and also requests inclusion of a mutually agreeable Limitation of Liability.
11. CenturyLink respectfully takes exception to Section 31.6, Force Majeure, and respectfully requests that labor strikes/disputes also be included as force majeure events (i.e., deletion of 31.6.4) and that 'immediately' be changed to 'as soon as reasonably possible' and 5 days be

changed to 30 days.

12. CenturyLink respectfully takes exception to Section 31.12, Change in Control, to the extent it requires notice within 10 days. CenturyLink respectfully requests this be changed to 30 days.
13. CenturyLink respectfully takes exception to Exhibit C, Federal Contract Terms and Conditions and requests that the terms apply only to the extent applicable to the provision of services contemplated in this RFP.
14. CenturyLink respectfully takes exception to Section 28, Insurance. CenturyLink purchases sufficient insurance limits to protect the company from risks and liabilities associated with providing its commercial services and products. CenturyLink's standard coverage is in accordance with generally accepted industry standards for the type services and/or work proposed. CenturyLink requests minimal changes to comply with its policies including reference to minimal rating, carrier approval, clarification as to subcontractor's coverage, notification of cancellation. CenturyLink is willing to discuss further during negotiations.
15. CenturyLink respectfully takes exception to Section 4, Compensation and points to the Charges and Invoices sections in the provided agreement for the City's consideration and discussion.
16. CenturyLink respectfully takes exception to Section 7, Non-Appropriations and points to its Non-Appropriations language to ensure funding is requested. CenturyLink is willing to discuss this language during negotiations.
17. CenturyLink respectfully takes exception to Section 20, Term and Termination of Contract and offers Term and Termination sections in its response for consideration and inclusion in the resultant contract.
18. CenturyLink respectfully takes exception to Section 20.5 as CenturyLink requests some ability to suspend or limit depending on the nature of the dispute. CenturyLink should not be required to continue providing services for indefinite periods of time without payment. CenturyLink is willing to discuss this language further during negotiations.
19. CenturyLink respectfully takes exception to Section 20.10 to the extent the parties have not reached mutually agreeable terms in Section 19 and thus takes exception until the parties are able to discuss further during negotiations.
20. CenturyLink respectfully takes exception to Section 31.19 Taxes until the parties are able to discuss the applicability considering the nature of services contemplated in this bid. CenturyLink agrees to negotiate this Section upon award.

ATTACHMENTS

| | |
|--------------|--|
| Attachment A | R041265 City of Charlotte MSA 7.10.19 |
| Attachment B | Form 8 Supplement Sample Security Log Monitoring Project |
| Attachment C | Form 8 Supplement Sample Monitoring and Management Project |

Attachment A

R041265 City of Charlotte MSA 7.10.19

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION**

This Master Service Agreement ("Agreement") is between **CENTURYLINK COMMUNICATIONS, LLC** ("CenturyLink") and **CITY OF CHARLOTTE** ("Customer") and is effective on the date the last party signs it (the "Effective Date"). This Agreement provides the terms and conditions applicable to Customer's purchase of products and services ("Service") from CenturyLink.

1. Term. The term of the Agreement will commence on the Effective Date and continue until the expiration of the last Service term, unless earlier terminated in accordance with the Agreement ("Term").

2. Service. CenturyLink will provide Service in accordance with the Agreement, including all applicable Service Schedules, Service Exhibits, Statements of Work, Order(s), pricing attachments, and any other documents that are attached or expressly incorporated into the Agreement ("Service Attachments"). The following Service Attachments, if any, are initially attached and incorporated into the Agreement. At CenturyLink's discretion, additional Service Attachments may be added by Amendment or by Customer placing an Order.

- **CenturyLink TS Service Exhibit**
- **IT Services Exhibit**
- **Professional Security Services Schedule**
- **CenturyLinkSM Adaptive Threat Intelligence Service**

3. Order(s). Customer may submit requests for Service in a form designated by CenturyLink ("Order"). The term for a Service is defined in the applicable Service Attachment ("Service Term"). Unless otherwise set forth in a Service Attachment, Service will continue month-to-month at the expiration of the Service Term at the existing rates, subject to adjustment by CenturyLink on 30 days' written notice. CenturyLink will notify Customer of acceptance of requested Service in the Order by delivering (in writing or electronically) the date by which CenturyLink will install Service (the "Customer Commit Date"), by delivering the Service, or by the manner described in a Service Attachment. Renewal Orders will be accepted by CenturyLink's continuation of Service. For moves, adds or changes agreed to by CenturyLink, Customer will pay CenturyLink's then current charges unless otherwise specifically stated in a Service Attachment.

4. Billing and Payment.

4.1 Commencement of Billing. Unless otherwise set forth in a Service Attachment, CenturyLink will deliver written or electronic notice (a "Connection Notice") to Customer when Service is installed, at which time billing will commence ("Service Commencement Date"). If Customer notifies CenturyLink within three days after delivery of the Connection Notice that Service is not functioning properly, CenturyLink will correct any deficiencies and, upon Customer's request, credit Customer's account in the amount of 1/30 of the applicable monthly recurring charge (MRC) for each day the Service did not function properly. If CenturyLink cannot complete installation due to Customer delay or inaction, CenturyLink may begin charging Customer for the Service, and Customer will pay such charges.

4.2 Payment of Invoices and Disputes. Unless otherwise set forth in a Service Attachment, invoices are delivered or made available monthly and due 30 days after the invoice date. Fixed charges are billed in advance and usage-based charges are billed in arrears. Customer's payments to CenturyLink must be made via an ACH transfer or any CenturyLink approved payment portal (e.g., CenturyLink Control Center) in the currency stated on the invoice. CenturyLink may charge administrative fees where Customer's payment and invoice preferences deviate from CenturyLink's standard practices. Past due amounts bear interest at 1.5% per month or the highest rate allowed by law (whichever is less). CenturyLink may charge Customer reasonable attorneys' fees and any third-party collection costs CenturyLink incurs in collecting such amounts. Customer is responsible for all charges regarding the Service, even if incurred as the result of unauthorized use. If Customer reasonably disputes an invoice, Customer must pay the undisputed amount and submit written notice of the disputed amount (with details of the nature of the dispute and the Services and invoice(s) disputed). Disputes must be submitted in writing within 90 days from the date of the invoice. If CenturyLink determines in good faith that a disputed charge was billed correctly, Customer must pay such amounts within 10 days after CenturyLink provides notice of such determination. Customer may not offset disputed amounts from one invoice against payments due on the same or another account.

4.3 Taxes and Fees. Excluding taxes based on CenturyLink's net income, Customer is responsible for all taxes and fees arising in any jurisdiction imposed on or incident to the provision, sale or use of Service. This includes value added, consumption, sales, use, gross receipts, withholding, excise, access, bypass, ad valorem, franchise or other taxes, fees, duties or surcharges (e.g., regulatory and 911 surcharges), whether imposed on CenturyLink or a CenturyLink affiliate, along with similar charges stated in a Service Attachment (collectively "Taxes and Fees"). Some Taxes and Fees, and costs of administering the same, are recovered through imposition of a percentage surcharge(s) on the charges for Service. If Customer is required by law to make any deduction or withholding of withholding Taxes from any payment due hereunder to CenturyLink, then, notwithstanding anything to the contrary in this Agreement, the gross amount payable by Customer will be increased so that, after any such deduction or withholding for such withholding Taxes, the net amount received by CenturyLink will not be less than CenturyLink would have received had no such deduction or withholding been required. Charges for Service are exclusive of Taxes and Fees. Customer may present CenturyLink with an exemption certificate eliminating CenturyLink's liability to pay certain Taxes and Fees. The exemption will apply prospectively.

4.4 Non-Appropriations. Customer intends to continue this Agreement for its entire Term and to satisfy its obligations hereunder. For each fiscal period for Customer: (a) Customer agrees to include in its budget request appropriations sufficient to cover Customer's obligations under this Agreement; (b) Customer agrees to use all reasonable and lawful means to secure these appropriations; (c) Customer agrees it will not use non-appropriations as a means of terminating this Agreement in order to acquire functionally equivalent products or services from a third party. Customer reasonably believes that sufficient funds to discharge its obligations can and will

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION**

lawfully be appropriated and made available for this purpose. In the event that Customer is appropriated insufficient funds, by appropriation, appropriation limitation or grant, to continue payments under this Agreement and has no other funding source lawfully available to it for such purpose (as evidenced by notarized documents provided by Customer and agreed to by CenturyLink), Customer may terminate this Agreement without incurring any termination charges by giving CenturyLink not less than 30 days' prior written notice. Upon termination and to the extent of lawfully available funds, Customer will remit all amounts due and all costs reasonably incurred by CenturyLink through the date of termination.

4.5 Regulatory and Legal Changes. If changes in applicable law, regulation, rule or order materially affect delivery of Service, the parties will negotiate appropriate changes to this Agreement. If the parties cannot reach agreement within 30 days after CenturyLink's notice requesting renegotiation, CenturyLink may, on a prospective basis after such 30-day period, pass any increased delivery costs on to Customer. If CenturyLink does so, Customer may terminate the affected Service on notice to CenturyLink delivered within 30 days of the cost increase taking effect.

4.6 Cancellation and Termination Charges. Unless otherwise set forth in a Service Attachment:

(a) Customer may cancel an Order (or portion thereof) prior to the delivery of a Connection Notice upon written notice to CenturyLink identifying the affected Order and Service. If Customer does so, Customer will pay CenturyLink a cancellation charge equal to the sum of: (1) for "off-net" Service, third party termination charges for the cancelled Service; (2) for "on-net" Service, one month's monthly recurring charges for the cancelled Service; (3) the non-recurring charges for the cancelled Service; and (4) CenturyLink's out-of-pocket costs (if any) incurred in constructing facilities necessary for Service delivery.

(b) Customer may terminate a specified Service after the delivery of a Connection Notice upon 30 days' written notice to CenturyLink. If Customer does so, or if Service is terminated by CenturyLink as the result of Customer's default, Customer will pay CenturyLink a termination charge equal to the sum of: (1) all unpaid amounts for Service actually provided; (2) 100% of the remaining monthly recurring charges for months 1-12 of the Service Term; (3) 50% of the remaining monthly recurring charges for month 13 through the end of the Service Term; and (4) if not recovered by the foregoing, any termination liability payable to third parties resulting from the termination and any out-of-pocket costs of construction to the extent such construction was undertaken to provide Service hereunder. The charges in this Section represent CenturyLink's reasonable liquidated damages and are not a penalty.

5. Default. If (a) Customer fails to make any payment when due and such failure continues for five business days after CenturyLink's written notice, or (b) either party fails to observe or perform any other material term of this Agreement and such failure continues for 30 days after the other party's written notice, then the non-defaulting party may: (i) terminate this Agreement and/or any Order, in whole or in part, and/or (ii) subject to Sections 6.1 (Damages Limitations) and 6.3 (Service Levels), pursue any remedies it may have at law or in equity.

6. Liabilities and Service Levels.

6.1 Damages Limitations. Neither party will be liable for any damages for lost profits, lost revenues, loss of goodwill, loss of anticipated savings, loss of data or cost of purchasing replacement services, or any indirect, incidental, special, consequential, exemplary or punitive damages arising out of the performance or failure to perform under this Agreement or any Order.

6.2 Disclaimer of Warranties. CENTURYLINK MAKES NO WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE, EXCEPT THOSE EXPRESSLY SET FORTH IN THIS AGREEMENT OR ANY APPLICABLE SERVICE ATTACHMENT.

6.3 Service Levels.

(a) Any "Service Level" applicable to Services are contained in the Service Attachments applicable to each Service. If CenturyLink does not meet a Service Level, CenturyLink will issue to Customer a credit as stated in the applicable Service Attachment on Customer's request, except that credits will not be provided for Excused Outages. CenturyLink's maintenance log and trouble ticketing systems are used to calculate Service Level events. Excused Outages mean scheduled maintenance under Section 8 and force majeure events, unless otherwise defined in a Service Attachment.

(b) Unless otherwise set forth in a Service Attachment, to request a credit, Customer must contact Customer Service (contact information is located at <http://www.level3.com>) or deliver a written request with sufficient detail to identify the affected Service. The request for credit must be made within 60 days after the end of the month in which the event occurred. Total monthly credits will not exceed the charges for the affected Service for that month. Customer's sole remedies for any nonperformance, outages, failures to deliver or defects in Service are contained in the Service Levels applicable to the affected Service.

6.4 Right of Termination for Installation Delay. Unless otherwise set forth in a Service Attachment, in lieu of installation Service Level credits, if CenturyLink's installation of Service is delayed by more than 30 business days beyond the Customer Commit Date, Customer may terminate the affected Service without liability upon written notice to CenturyLink, provided such written notice is delivered prior to CenturyLink delivering a Connection Notice for the affected Service. This Section will not apply where CenturyLink is constructing facilities to a new location not previously served by CenturyLink.

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION**

7. Customer Premises; Title to Equipment. If access to non-CenturyLink facilities is required for the installation, maintenance, grooming, movement, upgrade and/or removal of CenturyLink network or equipment, Customer will, at its expense: (a) secure such right of access and (b) arrange for the provision and maintenance of power and HVAC as needed for the proper operation of such equipment and network. Title to CenturyLink-provided equipment (including software) remains with CenturyLink. Customer will not create or permit to be created any encumbrances on CenturyLink-provided equipment.

8. Scheduled Maintenance and Local Access. Scheduled maintenance will not normally result in Service interruption. Unless otherwise set forth in a Service Attachment, if scheduled maintenance requires Service interruption CenturyLink will: (1) provide Customer seven days' prior written notice, (2) work with Customer to minimize interruptions and (3) use commercially reasonable efforts to perform such maintenance between midnight and 6:00 a.m. local time. If third-party local access services are required for the Services, Customer will: (1) provide CenturyLink with circuit facility and firm order commitment information and design layout records to enable cross-connects to CenturyLink Service(s) (provided by CenturyLink subject to applicable charges), (2) cooperate with CenturyLink (including changing demarcation points and/or equipment and providing necessary LOAs) regarding circuit grooming or re-provisioning, and (3) where a related Service is disconnected, provide CenturyLink a written disconnection firm order commitment from the relevant third-party provider. CenturyLink may re-provision any local access circuits from one off-net provider to another or to the CenturyLink owned and operated network (on-net), and such changes will be treated as scheduled maintenance.

9. General Terms.

9.1 Force Majeure. Neither party will be liable, nor will any credit allowance or other remedy be extended, for any failure of performance or equipment due to causes beyond such party's reasonable control ("force majeure event").

9.2 Assignment and Resale. Neither party may assign its rights or obligations under this Agreement or any Service Attachment without the prior written consent of the other party, which will not be unreasonably withheld. However, either party may assign its rights and obligations under this Agreement or any Order without the consent of the other party: (1) to any subsidiary, parent, or affiliate that controls, is controlled by, or is under common control with that party; (2) pursuant to the sale or transfer of substantially all of the business or relevant assets of that party; or (3) pursuant to any financing, merger, or reorganization of that party. This Agreement and all Service Attachments will apply to any permitted transferees or assignees. Any assignee of Customer must have a financial standing and creditworthiness equal to or better than Customer's. Unless otherwise set forth in a Service Attachment, Customer may provide Service to third parties or use the Services in connection with goods or services provided by Customer to third parties ("Customer Provided Services"). To the extent permitted under law, Customer will be responsible for any claims arising from or related to any Customer Provided Services. If Customer sells telecommunications services, Customer certifies that it has filed all required documentation and will at all times have the requisite authority with appropriate regulatory agencies respecting the same. Nothing in this Agreement confers upon any third party any right, benefit or remedy hereunder.

9.3 Affiliates. CenturyLink may use a CenturyLink affiliate or a third party to provide Service to Customer, but CenturyLink will remain responsible to Customer for Service delivery and performance. Customer's affiliates may purchase Service under this Agreement, and Customer will be jointly and severally liable for all claims and liabilities related to Service ordered by any Customer affiliate.

9.4 Notices. Notices will be in writing and deemed received if delivered personally, sent via facsimile, pre-paid overnight courier, electronic mail (if an e-mail address is provided below) or sent by U.S. Postal Service or First Class International Post. Unless otherwise provided for in a Service Attachment, requests for disconnection of Service (other than for default) must be submitted to CenturyLink via Customer's portal at <https://www.centurylink.com/business/login/> or via the following website / link: <http://www1.level3.com/disco/disco.html> and will be effective 30 days after receipt (or such longer period set forth in a Service Attachment). Notices for billing inquiries/disputes or requests for Service Level credits must be submitted to CenturyLink via Customer's portal at <https://www.centurylink.com/business/login/> or via Email at: billing@centurylink.com. Customer failure to follow this process and/or provide complete information may result in continued charges that will not be credited. All legal notices will be addressed to CenturyLink at: 931 14th Str., #900, Denver, CO 80202; Fax: 888-778-0054; Attn.: Notice Coordinator; and to any electronic or physical address of Customer as provided in the Agreement or in its absence, to Customer's address identified on the Order or as reflected in CenturyLink's records, Attn. General Counsel.

9.5 Acceptable Use Policy and Data Protection. Customer must comply with the CenturyLink Acceptable Use Policy ("AUP"), which is available at <http://www.centurylink.com/legal>, for Services purchased under this Agreement and acknowledge the CenturyLink Privacy Policy, which is available at <http://www.centurylink.com/aboutus/legal/privacy-policy.html>. CenturyLink may reasonably modify these policies to ensure compliance with applicable laws and regulations and to protect CenturyLink's network and customers.

9.6 Confidentiality. Except to the extent required by an open records act or similar law, neither party will: (a) disclose any of the terms of the Agreement; or (b) disclose or use (except as expressly permitted by, or required to achieve the purposes of, the Agreement) the Confidential Information received from the other party. A party may disclose Confidential Information if required to do so by a governmental agency, by operation of law, or if necessary in any proceeding to establish rights or obligations under the Agreement. Each party will limit disclosure and access to confidential information to those of its employees, contractors, attorneys or other representatives who reasonably require such access to accomplish the Agreement's purposes and who are subject to confidentiality obligations at least as restrictive as those contained herein. "Confidential Information" means any commercial or operational information disclosed by one party to the other in connection with the Agreement and does not include any information that: (a) is in the public

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION**

domain without a breach of confidentiality; (b) is obtained from a third party without violation of any obligation of confidentiality; or (c) is independently developed by a party without reference to the Confidential Information of the other party.

9.7 Intellectual Property Ownership; Use of Name and Marks. Nothing in the Agreement or the performance thereof will convey, license, or otherwise transfer any right, title, or interest in any intellectual property or other proprietary rights held by either party or its licensors. Neither party will use the name or marks of the other party or any of its affiliates for any purpose or issue any press release or public statement relating to this Agreement without the other party's prior written consent.

9.8 Governing Law; Amendment. This Agreement will be governed and construed in accordance with the laws of the State in which Customer's principal office is located, without regard to its choice of law rules. Each party will comply with all applicable laws, rules and regulations associated respectively with CenturyLink's delivery or Customer's use of the Service under the Agreement. This Agreement, including any Service Attachments, constitutes the entire and final agreement and understanding between the parties with respect to the Service and supersedes all prior agreements relating to the Service. CenturyLink is not subject to any obligations that are not explicitly identified in this Agreement. This Agreement may only be modified or supplemented by an instrument executed by an authorized representative of each party. No failure by either party to enforce any right(s) hereunder will constitute a waiver of such right(s).

9.9 Critical 9-1-1 Circuits. The Federal Communications Commission's 9-1-1 reliability rules mandate the identification and tagging of certain circuits or equivalent data paths that transport 9-1-1 calls and information ("9-1-1 Data") to public safety answering points. These circuits or equivalent data paths are defined as Critical 911 Circuits in 47 C.F.R. Section 12.4(a)(5). CenturyLink policies require tagging of any circuits or equivalent data paths used to transport 9-1-1 Data. Customer will cooperate with CenturyLink regarding compliance with these rules and policies and will notify CenturyLink of all Services Customer purchases under this Agreement utilized as Critical 911 Circuits or for 9-1-1 Data.

9.10 International Services. For Services provided outside the United States, Customer or its local affiliate may be required to enter into a separate local country addendum/agreement (as approved by local authorities) ("LCA") with the respective CenturyLink affiliate that provides the local Service(s). Such CenturyLink affiliate will invoice Customer or its local affiliate for the respective local Service(s).

9.11 Relationship and Counterparts. The relationship between the parties is not that of partners, agents, or joint venturers. This Agreement may be executed in one or more counterparts, all of which taken together will constitute one instrument. Digital signatures and electronically exchanged copies of signed documents will be sufficient to bind the parties to this Agreement.

CENTURYLINK COMMUNICATIONS, LLC

CITY OF CHARLOTTE

Authorized Signature

Authorized Signature

Name Typed or Printed

Name Typed or Printed

Title

Title

Date

Date

Customer's Address for Notices:
Customer's Facsimile Number (if applicable):
Person Designated for Notices: General Counsel

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
CENTURYLINK TS SERVICES EXHIBIT**

1. General; CenturyLink TS Service Schedules.

1.1 General. This Service Exhibit is applicable only where Customer orders one of the CenturyLink services described in the CenturyLink Service Schedules listed below ("Service") and provided by CenturyLink or a CenturyLink affiliate ("CenturyLink"). This Service Exhibit incorporates the terms of the Master Service Agreement or other CenturyLink approved service agreement under which CenturyLink provides the Services to Customer (the "Agreement"), and in the event of a conflict in any term of any documents that govern the provision of Services, the following order of precedence will apply in descending order of control: the Service Schedule, this Service Exhibit, the Agreement, any Service Guide, the SLA, the Service Order(s) and Statements of Work ("SOW(s)"). Capitalized terms not defined in this Service Exhibit or one of the Service Schedules are defined in the Agreement.

1.2 CenturyLink TS Service Schedules. Customer may purchase the Services in the following Service Schedules included within this Service Exhibit.

- **SERVICE SCHEDULE: SECURITY SERVICES ASSOCIATED WITH HOSTING, CENTURYLINK CLOUD AND CLOUD APPLICATION MANAGER SERVICES**

2. Definitions.

"BCD" or "Billing Commencement Date" means the date on which CenturyLink begins billing for a Service, as further defined in the Billing Commencement Date Section below. The BCD will apply in lieu of any other Customer Commit Date, Service Commencement Date, Connection Notice, or similar language in the Agreement.

"Customer Data" means any data, content or information of Customer or its end users that is stored, transmitted, or otherwise processed using the CenturyLink Services. CenturyLink's obligations with respect to such Customer Data will be exclusively governed by the Compliance and Security section and are further subject to all Limitation of Liability provisions of this Service Exhibit, the Service Schedule and the Agreement.

"End User" means Customer's members, end users or any other third parties who use or access the Services or access CenturyLink's network or data centers via the Services.

"MRC" means monthly recurring charge.

"NRC" means non-recurring charge.

"Service Guide" (or "SG") means the product-specific Service guide that includes technical specifications which CenturyLink may modify from time to time, effective upon posting on <http://www.ctl.io>.

"Service Order" means a service order request submitted on a form issued by CenturyLink and signed by Customer that includes the type and details of the specific Services ordered by Customer.

"Service Schedule" means those service descriptions providing additional terms pursuant to which CenturyLink may provide and Customer may purchase the Services described in the Service Schedule.

"SLA" or "SLA Attachment" or "Service Levels" means the service level agreement applicable to each individual Service, if any, which provides Customer's sole and exclusive remedies for any nonperformance, Service deficiencies, outages, interruptions or failures of any kind. SLAs may be updated from time to time upon posting on the applicable website referenced in the Service Schedule(s).

3. Term; Renewal. CenturyLink Services have a minimum term which begins on the BCD and continues for the period set forth in the relevant Service Order or SOW ("Initial Service Term"), at the conclusion of which the Service will automatically renew for successive periods equal to twelve (12) months, unless terminated by either party in writing at least sixty (60) days prior to the expiration of the then-current Service Term. Notwithstanding the foregoing sentence, if the Initial Service Term is one month, then the Services will automatically renew monthly unless terminated by either party in writing with thirty (30) days prior written notice, or as otherwise required in the associated Service Schedule. The Initial Service Term and any automatic renewal terms are collectively referred to as the "Service Term".

4. Rates; Billing; Payment.

4.1 Rates. Customer will pay all applicable rates and fees set forth in the relevant Service Order and/or SOW. Notwithstanding any other provision to the contrary and not more than once per calendar year, CenturyLink may increase the charges applicable to any Service provided under this Service Exhibit in accordance with the payment provisions of the Agreement or if no increase is provided for in the Agreement and to the extent permitted under applicable laws in an amount not to exceed the latest annual increase in the Consumer Price Index, specifically, the U.S. Department of Labor, Bureau of Labor Statistics "All Items Consumer Price Index for All Urban Consumers (CPI-U) for the U.S. City Average" or, to the extent charges in a Service Order are set forth in local currency, equivalent index for Services provided in other jurisdictions. Such increase will be effective upon the date set forth in CenturyLink's

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
CENTURYLINK TS SERVICES EXHIBIT**

written notice thereof to Customer. CenturyLink may otherwise increase applicable charges as set forth on a particular Service Order or upon prior written notice during any automatic renewal term.

4.2 Billing Commencement Date or BCD. This Section 4.2 applies in lieu of any other commencement of billing provisions that may otherwise apply in the Agreement. Unless otherwise provided in a Service Schedule, the BCD for the Service is the earlier of (a) the date on which Customer uses the Service (b) the date CenturyLink notifies Customer in writing that the initial installation or a usable part thereof is complete. If CenturyLink partially installs or activates a Service, CenturyLink reserves the right to commence billing for such Service on a pro rata basis, and if a Service installation is delayed, incomplete or is not usable by Customer through no fault of CenturyLink or its agents, CenturyLink will have the right to commence billing as installed and per the BCD.

4.3 Withholding Taxes. All invoices will be issued to Customer and paid in the currency specified in the Service Order. Customer will pay such invoices free of currency exchange costs, or bank charges. Service charges are exclusive of Taxes and presented without reduction for any Withholding Tax, all of which are the responsibility of the Customer. "Withholding Tax" means any amount on account of tax on sources of income which a payor is obliged to deduct from payments due to a recipient and account for to any tax authority. In the event that any payment to be made to CenturyLink under this Service Exhibit should be subject to reduction by reason of a Withholding Tax, Customer agrees to pay CenturyLink such amounts as would have been necessary so that the aggregate net amount received by CenturyLink after application of a Withholding Tax, is the same amount as would have been received by CenturyLink if there had been no requirement to deduct or withhold such tax.

5. Obligations.

5.1 Compliance and Security. CenturyLink will comply with all laws and regulations applicable to CenturyLink's provision of the Service, and Customer will comply with all laws and regulations applicable to Customer's use of the Service. CenturyLink has adopted and implemented, and will maintain, a corporate information security program designed to protect Customer Data from loss, misuse and unauthorized access or disclosure. Such program includes formal information security policies and procedures. The measures of the information security program generally apply to CenturyLink's standard services and certain measures may not apply or may be applied differently to customized services, configurations, or environments ordered or as deployed by Customer. The CenturyLink information security program is subject to reasonable changes by CenturyLink from time to time. Customer will ensure that all Customer Data complies with applicable law and reasonable information security practices, including those involving encryption. In addition to CenturyLink's obligations in the Agreement, CenturyLink, as of the Effective Date, has completed an AICPA sanctioned Type II audit report (i.e., SSAE18/ISAE3402 SOC 1 or AT-101 SOC 2) in certain data centers and intends to continue to conduct such audits pursuant to a currently sanctioned or successor standard. Customer will be entitled to receive a copy of the then-available report (or a summary of it) upon request and subject to a charge, which is CenturyLink Confidential Information. Customer may make such report available to its End Users subject to confidentiality terms provided by CenturyLink.

5.2 Acknowledgement and Consent. In addition to and in accordance with the applicable provisions of the Agreement, if any, Customer acknowledges and agrees that CenturyLink and its affiliates or subcontractors may use and transfer to the United States, or other countries where CenturyLink or its affiliates or subcontractors have data center based services, support or processing systems and/or operate Service data or information (including business contact information such as names, phone numbers, addresses and/or email addresses) for the sole purpose of: (i) providing and managing the Services; (ii) fulfilling its obligations and enforcing its rights under the Agreement; and (iii) complying with applicable law. CenturyLink will not disclose, modify, or access Customer Data, except (a) if Customer expressly authorizes CenturyLink to do so in connection with Customer's use of the Services, including requests for support; or (b) as necessary to provide the Services to Customer or to prevent or address Service or technical problems, or to comply with this Service Exhibit; or (c) at the request of a governmental or regulatory body, subpoenas or court order.

5.3 Equipment. Unless otherwise set forth in the applicable SG or Service Order, Customer is responsible for selecting, supplying, installing and maintaining Customer equipment used to access the Services including any related applications, systems, or hardware. If the Service includes access to or the use of CenturyLink-provided equipment including any related applications, systems or hardware ("CenturyLink Equipment"), in addition to the provisions of the Agreement, Customer will cooperate with CenturyLink to allow installation, maintenance and, upon termination, removal of the CenturyLink Equipment.

6. Cancellation; Termination; Default.

6.1 Cancellation; Termination. This Section 6.1 applies in lieu of any other cancellation and termination section, including any available rights of termination that may be in the Agreement. CenturyLink may suspend the affected Service upon five (5) days' notice in the event of any uncured payment default. If Customer terminates an ordered Service, an applicable Service Schedule or the Agreement prior to its BCD, Customer will pay a cancellation fee equal to one (1) month's projected MRC, plus all out-of-pocket costs incurred by or imposed upon CenturyLink (e.g., ordered equipment, licenses, carrier termination charges). Unless a different early termination fee applies as provided in a Service Schedule, if the Service, an applicable Service Schedule or the Agreement is terminated either by CenturyLink as a result of Customer's default or by Customer for any reason other than CenturyLink's default and prior to the conclusion of the applicable Service Term, then Customer will be liable for: (a) an early termination charge equal to 50% of the then current MRC for the affected Services multiplied by the number of months remaining in the Service Term (or committed term as applicable); (b) Service charges accrued but unpaid as of the termination date; and (c) any out-of-pocket costs incurred by or imposed

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
CENTURYLINK TS SERVICES EXHIBIT**

upon CenturyLink (e.g., ordered equipment, licenses, carrier termination charges). The parties agree that any cancellation fees and early termination charges set forth in the Agreement constitute liquidated damages and are not intended as a penalty. If a particular Service is terminated upon which another service is dependent, all such dependent services will be deemed to be terminated as well and subject to the applicable termination charges.

6.2 Default: The following clause will apply in lieu of any other default section in the Agreement: If (a) Customer fails to make any payment when due and such failure continues for five (5) business days after CenturyLink's written notice, or (b) either party fails to observe or perform any other material term of this Service Exhibit or the Agreement and such failure continues for thirty (30) days after the other party's written notice, then the non-defaulting party may: (i) terminate the applicable Service Schedule and/or any Service Order, in whole or in part; and/or (ii) subject to all applicable damages limitations and SLA Attachments, pursue any remedies it may have at law or, where applicable, in equity.

7. Scheduled Maintenance. This section 7 applies in lieu of any other scheduled maintenance and local access provisions that may be included in the Agreement. Customer acknowledges that the Services may be subject to routine maintenance or repair and agrees to cooperate in a timely manner and provide reasonable access and assistance as necessary to allow such maintenance or repair. Scheduled or emergency maintenance terms are identified in the applicable SLA, SG, portal or website referenced in the applicable Service Schedule.

8. Liabilities; Disclaimer.

8.1 Direct Damages. Except for the payment and indemnification obligations of Customer and subject to the Damages Limitations provision in the Agreement or similar waiver of consequential damages provision, the total aggregate liability of each party arising from or related to the claim will not exceed in the aggregate the total MRCs, NRCs, and usage charges paid or payable to CenturyLink for the affected Services under the applicable Service Schedule in the twelve (12) months immediately preceding the first event giving rise to the cause of action ("Damage Cap").

8.2 Additional Disclaimer of Warranties. CENTURYLINK MAKES NO WARRANTIES OR REPRESENTATIONS THAT ANY SERVICE WILL BE FREE FROM LOSS OR LIABILITY ARISING OUT OF HACKING OR SIMILAR MALICIOUS ACTIVITY, OR ANY ACT OR OMISSION OF CUSTOMER OR THAT ANY CONTENT WILL BE SECURE OR NOT OTHERWISE LOST OR ALTERED. THE PREVIOUS DISCLAIMERS WILL NOT LIMIT CUSTOMER'S ABILITY TO SEEK ANY APPLICABLE SLA REMEDIES.

9. Notices.

9.1 Notwithstanding anything to the contrary in the Agreement, Customer acknowledges and agrees that CenturyLink may also contact Customer via e-mail at the e-mail address provided to CenturyLink when Customer ordered the Service, and such email may include instructions for use of a private website for posting of such notices, for any reason relating to the Service, including for purposes of providing Customer any notices required under the Agreement. Customer agrees to provide CenturyLink with any change to its email address.

9.2 Service Notice. All Customer notices for Service disconnect and termination must be sent via email to CenturyLink at: BusinessDisconnects@centurylink.com and must contain the account name, account number, identification of the Service(s), and Service address(es). Such disconnect and termination is effective thirty (30) days after CenturyLink's receipt of the notice. All Customer notices for Service non-renewal and other routine operational notices will be provided in writing to its CenturyLink sales representative. Failure to provide disconnect, termination and non-renewal notices in accordance with the terms of this Service Exhibit may result in continued charges, and CenturyLink will not credit charges for such noncompliance.

10. Intellectual Property; Software.

10.1 Intellectual Property. CenturyLink's intellectual property and proprietary rights include any skills, know-how, modifications or other enhancements developed or acquired in the course of configuring, providing, or managing the Service. Each party agrees that it will not, directly or indirectly, reverse engineer, decompile, reproduce or otherwise attempt to derive source code, trade secrets, or other intellectual property from any information, material, or technology of the other party or its licensors. Nothing in this Service Exhibit or the performance thereof conveys, or otherwise transfers any right, title, or interest in any intellectual property or other proprietary rights held by either party or its licensors.

10.2 Software. Customer agrees that any third-party software including any corresponding documentation, provided to Customer by CenturyLink in connection with the Service will be used strictly in accordance with all applicable licensing terms and conditions. All rights in and to any such third-party software are reserved by and remain with the applicable third parties. Any software (including related documentation) that may be provided by CenturyLink or its third party licensors may be used solely as part of the Services..

10.3 Third Party Software. If Customer elects to use Customer provided and/or licensed software in connection with the Services or make such software available to its End Users, Customer is solely responsible for (a) selecting, licensing, installing and maintaining

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
CENTURYLINK TS SERVICES EXHIBIT**

any such software, including any related applications and systems; and (b) ensuring adherence to current technical documentation, all applicable licensing terms, requirements, and/or restrictions and all applicable laws with respect to such software.

11. Feedback. In the event Customer elects, in connection with any of the Services, to communicate to CenturyLink suggestions for improvements to the Service ("Feedback"), CenturyLink will own all right, title and interest in and to the same, even if Customer has designated the Feedback as confidential, and CenturyLink will be entitled to use the Feedback without restriction. Customer hereby irrevocably assigns all right, title, and interest in and to the Feedback to CenturyLink and agrees to provide CenturyLink such assistance as it may require to document, perfect and maintain CenturyLink's rights to the Feedback.

12. HIPAA. Where applicable and to the extent the Services involve the ongoing storage of or routine access to PHI (as defined under the Health Insurance Portability and Accountability Act of 1996, as amended, "HIPAA"), or CenturyLink is otherwise acting as a Business Associate (pursuant to HIPAA), CenturyLink will agree to the terms in its then-current Business Associate Agreement upon Customer's request.

13. Any provisions in the Agreement related to 9-1-1 Circuits will not apply to the Services in this Service Exhibit.

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
CENTURYLINK TS SERVICES EXHIBIT**

SERVICE SCHEDULE: SECURITY SERVICES

The services covered by this Service Schedule are the Security Services (collectively, "Security Services" or Services") associated with Customer's Hosting, CenturyLink Cloud or Cloud Application Manager services provided by CenturyLink to Customer from time to time under separate Service Schedules. Not all Security Services are available in all regions or countries and are subject to availability.

1. Customer's use of Services is subject to the Service Guides located at <https://www.centurylink.com/business/support/service-guides.html>. For Security Log Monitoring Services, in addition to the Service Guide, Customer's use of Security Log Monitoring Services is subject to the SLA and Supplemental Terms located at <https://www.ctl.io/legal/security-log-monitoring/supplemental-terms/>.
2. Customer acknowledges that the Services endeavor to mitigate security incidents, but such incidents may not be mitigated entirely or rendered harmless. Each Service is subject to limitations in its scope or performance, as may be more fully set forth in the applicable SG.
3. Customer should consider any particular Service as just one tool to be used as part of an overall security strategy and not a guarantee of security.
4. Non-standard installations (as identified by CenturyLink in its reasonable opinion), may require extended provisioning intervals and/or additional costs.
5. Customer will submit a sufficiently detailed description of any test plan to CenturyLink in advance. The test plan must adhere to any applicable testing standards or procedures provided by CenturyLink. CenturyLink may modify the test plan in its reasonable discretion and may require the execution of additional contractual documents prior to testing. CenturyLink will not respond to any security-related alarms during a scheduled testing period. CenturyLink will have no responsibility whatsoever for any loss or outages during a Customer test, including any otherwise available service credits. Customer agrees that neither it nor its agents will engage in any destructive or otherwise harmful testing.
6. Customer represents that Customer is not (a) located in, under the control of, or a national or resident of any country or territory to which export is prohibited under the laws of any country in which CenturyLink operates, or (b) on the U.S. Treasury Department List of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders.
7. The Service provided under this Service Schedule is a supplement to Customer's existing security and compliance frameworks, for which CenturyLink is not, and will not be, responsible. While CenturyLink will use reasonable commercial efforts to provide the Services accurately and completely, the Services are provided "as-is". CenturyLink does not and cannot guarantee or warrant that CenturyLink will accurately identify all risks, potential security and/or compliance gaps, that Services will be security incident free or that CenturyLink's recommendations, assessments, tests, reports or monitoring will be accurate, complete, error-free, or effective in achieving Customer's security and/or compliance related objectives. Neither CenturyLink or its subcontractors will be liable for any damages which Customer or third parties may incur as a result of Customer's (i) non-compliance with any standards which apply to Customer, and/or (ii) reliance upon (or implementation of recommendations from) results, reports, tests, or recommendations related to the Services.
8. **Direct Damages.** Notwithstanding anything to the contrary in the Service Exhibit or Service Attachments (as defined in the Agreement), the total aggregate liability of each party arising from or related to a claim will not exceed in the aggregate the total MRCs, NRCs, and usage charges paid or payable to CenturyLink for the affected Security Services under this Service Schedule in the 6 (six) months immediately preceding the first event giving rise to the cause of action ("Damage Cap").
9. CenturyLink may temporarily suspend any Service immediately in the event CenturyLink has a good faith belief that such Suspension is reasonably necessary to mitigate damage or liability that may result from Customer's continued use of the Service. In the event of any expiration or termination of any Service, Customer's access to the applicable Services will end and CenturyLink will not be responsible for assisting Customer with any transition to an alternative provider.
10. Nothing in this Service Schedule or the Agreement grants Customer any rights to, and Customer is expressly prohibited from, reselling the Services.

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
IT SERVICES EXHIBIT**

1. Applicability. This Service Exhibit is applicable only where Customer orders IT Services. This IT Services Exhibit ("Service Exhibit") is entered into between CenturyLink and Customer and is effective as of the date last signed ("Exhibit Effective Date"). This Service Exhibit is governed by and incorporates by reference the CenturyLink Master Service Agreement or other service agreement executed between the parties, or the then current standard CenturyLink Master Service Agreement if no agreement has been executed. This Service Exhibit, any attached or incorporated documents, Statements of Work ("SOWs"), SOW Change Requests, and the applicable agreement between CenturyLink and Customer collectively comprise the agreement between the parties ("Agreement"). Capitalized terms used and not otherwise defined will have the meaning set forth in the Agreement.

2. IT Services and Acceptance. This Section replaces the Orders section in the Agreement. CenturyLink will provide the professional, consulting, analytical, design and/or technical services ("IT Services" or "Services") identified in the applicable statement of work ("SOW") pursuant to this IT Services Exhibit, any attached or incorporated documents, the applicable SOW, any SOW Change Requests. CenturyLink may provide the IT Services by one or more affiliates or subcontractors. If applicable, the SOW will specifically describe and designate any Software Deliverables and Other Deliverables (collectively, "Deliverables"). Customer will comply with the responsibilities identified in the SOW or a SOW Change Request. CenturyLink's performance will be excused where the Services are contingent upon Customer's performance until Customer complies with its responsibilities; CenturyLink will receive additional time to complete the Services after Customer complies. Customer's noncompliance may result in an adjustment of the charges, including charges for additional hours required to complete the Services. Except as otherwise provided in a SOW, IT Services will be deemed accepted unless Customer provides written notice of any deficiency to CenturyLink within three business days after commencement of work or delivery of the Services, including phased delivery of Service, if applicable (the "Acceptance Period"). Such notice must detail and demonstrate the deficiency to CenturyLink's reasonable satisfaction. CenturyLink will remedy the deficiency and will notify Customer accordingly, at which time a new Acceptance Period will begin. CenturyLink will delay billing until IT Services are accepted. "Software Deliverables" means any software developed by CenturyLink solely and uniquely for Customer. Software Deliverables may include open source software, any software that requires as a condition of use, modification or distribution that the software or any other software incorporated into, derived from or distributed with such software be: (a) disclosed or distributed in source code form, (b) licensed for the purpose of making derivative works, or (c) licensed or redistributed at no charge. "Other Deliverables" means any items other than Software Deliverables developed by CenturyLink solely and uniquely for Customer.

3. Service Term. The Services will continue for the term specified in the applicable SOW ("Service Term"), unless terminated by either party pursuant to the terms of the Agreement or this Exhibit.

4. Charges; Payment. This Section replaces the Commencement of Billing section in the Agreement. Subject to the Acceptance section above, the Service Commencement Date for IT Services is the date CenturyLink begins performing IT Services or as specified in a SOW. Customer will pay all charges (including reasonable travel and living expenses and third-party charges) and any progress payments as set forth in a SOW and all applicable Taxes and Fees. If CenturyLink cannot complete installation due to Customer delay or inaction, CenturyLink may begin charging Customer for the Service, and Customer will pay such charges. "MRC" means monthly recurring charge, and "NRC" means non-recurring charge. Charges for certain Services are subject to (a) a property tax surcharge and (b) a cost recovery fee per month to reimburse CenturyLink for various governmental taxes and surcharges. Such charges are subject to change by CenturyLink and will be applied regardless of whether Customer has delivered a valid tax exemption certificate. For additional details on taxes and surcharges that are assessed, visit <http://www.centurylink.com/taxes>.

5. Termination. This Section replaces the Cancellation and Termination Charges section in the Agreement. Either party may terminate this Service Exhibit or a SOW upon 30 days prior written notice for default. Unless otherwise set forth in a SOW, if Customer terminates all or part of a SOW prior to its Service Commencement Date, Customer will pay a cancellation fee of 25% of the affected fees plus all out-of-pocket costs incurred by CenturyLink. If all or part of a SOW is terminated either by CenturyLink for default or by Customer for any reason other than default after the Service Commencement Date but prior to completion of the IT Services under such SOW, then unless otherwise set forth in the SOW Customer will be liable for: (a) an early termination charge equal to 50% of the NRC and MRC for any tasks, Deliverables or work not yet completed by CenturyLink as specified in the SOW; (b) any charges accrued but unpaid as of the termination date; and (c) any out-of-pocket costs incurred by or imposed upon CenturyLink. Customer will remain liable for charges accrued but unpaid as of the termination date.

6. Limitations; Disclaimer of Warranties. CenturyLink will not be liable for any damages incurred by Customer or third parties resulting from Customer's (a) non-compliance with any standards which apply to Customer. Except for Customer's obligations under the Charges; Payment section, each party's total aggregate liability arising from or related to the Services will be limited to the total charges paid or payable under the SOW that gave rise to the claim. Customer's sole remedy for any dissatisfaction in the performance of any of the Services or deliverables is the SLA, if applicable, or to terminate the relevant SOW. THE IT SERVICES, INCLUDING ANY DELIVERABLE AND ANY OPEN SOURCE SOFTWARE, ARE PROVIDED WITHOUT ANY WARRANTIES OF ANY KIND, WHETHER STATUTORY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, COMPLETENESS, COMPATIBILITY OF SOFTWARE OR EQUIPMENT, OR ANY RESULTS TO BE ACHIEVED THEREFROM. ANY OPEN SOURCE SOFTWARE IS PROVIDED ON AN "AS IS" BASIS. CENTURYLINK MAKES NO WARRANTIES OR REPRESENTATIONS THAT (A) ANY IT SERVICE OR ANY DELIVERABLE WILL BE FREE FROM LOSS OR LIABILITY ARISING OUT OF (I) HACKING OR SIMILAR MALICIOUS ACTIVITY, OR (II) ANY ACT OR OMISSION OF THE CUSTOMER, (B) ALL ERRORS CAN BE CORRECTED, OR (C) THAT OPERATION OF THE DELIVERABLES AND IT SERVICES SHALL BE UNINTERRUPTED OR ERROR-FREE.

7. Compliance and Security. CenturyLink has adopted and implemented, and will maintain, a corporate information security program designed to protect data transmitted or processed by CenturyLink from loss, misuse and unauthorized access or disclosure. Such program includes formal information security policies and procedures. The CenturyLink information security program is subject to

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
IT SERVICES EXHIBIT**

reasonable changes by CenturyLink from time to time. Customer will ensure that all Customer data transmitted or processed via the Service complies with applicable law and reasonable information security practices, including those involving encryption.

8. Intellectual Property.

8.1 Customer License to Deliverables. Upon receipt of full payment, CenturyLink grants to Customer a non-exclusive, perpetual, non-transferrable, royalty-free, worldwide right and license under to use, execute, reproduce, display, perform, distribute copies of and prepare derivative works of the Deliverables as expressly set forth in the applicable SOW ("Deliverable License"); provided however Customer shall treat the Deliverables as "confidential" pursuant to the Confidentiality Section below and any applicable confidentiality agreement(s) by and between Customer and CenturyLink unless otherwise specified in the applicable SOW. In the event that any CenturyLink Intellectual Property is embedded in or otherwise incorporated into a Deliverable ("Embedded CenturyLink IP"), then the Deliverable License shall extend to such Embedded CenturyLink IP solely for Customer's enjoyment of the Deliverable License and not on a standalone basis. All right, title and interest in and to the Deliverables and all CenturyLink Intellectual Property will remain solely with CenturyLink, its affiliates and their licensors. Other than the license granted in this Section, Customer is not granted any license or other right (express, implied or otherwise) to use any trademarks, copyrights, service marks, trade names, patents, trade secrets of CenturyLink or its affiliates or any other form of CenturyLink Intellectual Property. "CenturyLink Intellectual Property" shall mean any inventions, processes, functionality, systems, network components, network designs, network configurations, protocols, API's, technology, services, software (in source and object forms), software tools, hardware designs, algorithms, user interface designs, architecture, class libraries, report formats and the copyright in such reports, objects and documentation (both printed and electronic), know-how, intellectual property rights or methodologies, templates, forms, whether patented, patent pending or non-patentable, which have been invented, created, acquired, conceived, developed, designed, reduced to practice by CenturyLink and/or its affiliates or otherwise owned by or licensed to CenturyLink and/or its affiliates.

8.2 CenturyLink License to Customer Technology and Customer Data. To the extent required by CenturyLink to provide the IT Services pursuant to an applicable SOW, Customer grants to CenturyLink a non-exclusive, non-transferable, royalty-free license to use Customer Technology and Customer data, and to sublicense Customer Technology and Customer data to CenturyLink subsidiaries and affiliates and any third parties providing all or part of the IT Services on behalf of CenturyLink. All right, title and interest in and to any Customer Technology and Customer data will remain solely with Customer, its affiliates and their licensors. Other than the license granted in this Section, CenturyLink is not granted any license or other right (express, implied or otherwise) to use any trademarks, copyrights, service marks, trade names, patents, trade secrets of Customer or its affiliates or any other Customer Technology. CenturyLink may use any archival tapes containing Customer data only for back-up purposes. Customer represents and warrants that any and all Customer data provided to CenturyLink as part of the Services will not (a) violate any applicable laws, rules or regulations or otherwise violate the rights of any third party; (b) be deceptive, defamatory, obscene, pornographic or unlawful; or (c) contain any viruses, worms or other malicious computer programming codes. In addition, Customer represents and warrants that it will keep, back up and maintain its own copy of all materials and information, including Customer Data that is provided or made available to CenturyLink, and further, that Customer will encrypt any Customer data that is provided or made available to CenturyLink. If information is both Confidential Information and Customer data, it will be treated as Customer data for purposes of this Service Exhibit and CenturyLink's obligations with respect to such Customer data shall be exclusively governed by the Compliance and Security Section above and are further subject to the limitation of liability provisions identified in the applicable SOW and the Agreement. "Customer Technology" means the proprietary technology of Customer and its licensors, including Customer's Internet operations design, software tools, hardware designs, algorithms, software (in source and object forms), user interface designs, architecture, class libraries, objects and documentation (both printed and electronic), know-how, trade secrets and any related intellectual property rights throughout the world and also including any derivatives, improvements, enhancements or extensions of Customer Technology conceived, reduced to practice, or developed by Customer during the Term.

8.3 Freedom of Action. Nothing in the Agreement will preclude CenturyLink from developing, marketing, and distributing any software or integration code or performing any services similar to the IT Services for itself or for any third party, provided that CenturyLink is in compliance with confidentiality obligations under the Agreement.

9. Confidentiality. In addition to the confidentiality terms contained in the Agreement, confidential information also includes CenturyLink Technology and Customer Technology. CenturyLink Technology and all enhancements and improvements are the exclusive property and confidential information of CenturyLink. Customer Technology and all enhancements and improvements are the exclusive property and confidential information of Customer. Confidential information will not include Customer data, the obligations for which are governed by the Compliance and Security section above.

10. Non-solicitation. Until twelve months after the Term, each party will not directly or indirectly Solicit an Assigned Resource either to accept employment or a consulting or contractor relationship directly with it or to terminate his or her employment, agency or other relationship with the other party, unless it first obtains the other party's prior written consent. "Solicit" means any intentional contacts with Assigned Resource, regardless of who (*i.e.*, the party to this Agreement or the Assigned Resource) initiates the contact, that relates to the acceptance or termination of employment. "Assigned Resource" means an employee, consultant or contractor of the other party assigned by CenturyLink to perform the IT Services or by Customer to directly manage the IT Services.

11. Miscellaneous. Notices for disconnection of Service must be submitted to CenturyLink via Email at: BusinessDisconnects@Centurylink.com. Notices of non-renewal for Services must be sent via e-mail to: CenturyLink, Attn.: CenturyLink NoRenew, e-mail: Norenew@centurylink.com. Notices for billing inquiries/disputes or requests for Service Level credits must be submitted to CenturyLink via Customer's portal at <https://www.centurylink.com/business/login/> or via Email at: Care.Inquiry@Centurylink.com. All other routine operational notices will be provided by Customer to its CenturyLink sales representative. If a conflict exists between the terms of the Agreement, the order of priority will be this Service Exhibit, the SOW, the

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
IT SERVICES EXHIBIT**

Change Request Form and then the Agreement. Notwithstanding anything to the contrary in the Agreement, Customer is prohibited from reselling Services provided pursuant to this Service Exhibit or any SOW without the express written consent of CenturyLink and, if applicable, CenturyLink's subcontractor. To the extent the Services involve the ongoing storage of or routine access to PHI (as defined under the Health Insurance Portability and Accountability Act of 1996, as amended, "HIPAA"), or CenturyLink is otherwise acting as a Business Associate (pursuant to HIPAA), CenturyLink will agree to the terms in its then-current Business Associate Agreement upon Customer's request. CenturyLink and its affiliates or subcontractors may use and transfer to the United States, or other countries, data or information (including business contact information such as names, phone numbers, addresses and/or email addresses) for the sole purpose of: (i) providing and managing the IT Services; (ii) fulfilling obligations related to the IT Services under this Service Exhibit and the Agreement; and (iii) complying with applicable law governing the IT Services.

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
PROFESSIONAL SECURITY SERVICES SCHEDULE**

This Professional Security Services Schedule ("Schedule") is entered into between CenturyLink and Customer and is effective as of the date last signed ("Schedule Effective Date"). This Schedule is governed by and incorporates by reference the CenturyLink Master Service Agreement ("MSA") executed between the parties, or the then current standard CenturyLink Master Service Agreement if no MSA has been executed. This Schedule, any attached or incorporated documents, Statements of Work ("SOWs"), SOW Change Requests, and the applicable CenturyLink Master Service Agreement between CenturyLink and Customer collectively comprise the agreement between the parties ("Agreement"). Capitalized terms used and not otherwise defined will have the meaning set forth in the Agreement.

1. Professional Security Services Description. CenturyLink will provide security consulting, analytical, professional, design and/or technical services ("Professional Security Services" or "Services") identified in an applicable SOW. Services are provided by the CenturyLink affiliate identified in the SOW. CenturyLink may provide the Services with its own employees or subcontractors and may change, modify, or replace any of its network hardware, software, or equipment used to deliver Services. Customer will comply with the responsibilities identified in the SOW or a SOW Change Request. CenturyLink's performance will be excused where the Services are contingent upon Customer's performance until Customer complies with its responsibilities; CenturyLink will receive additional time to complete the Services after Customer complies. Customer's noncompliance may result in an adjustment of the charges, including charges for additional hours required to complete the Services.

2. Service Term. The Services will continue for the term specified in the applicable SOW ("Service Term"), unless terminated by either party pursuant to the terms of the Agreement or this Schedule.

3. Acceptance. Except as otherwise provided in a SOW, Services will be deemed accepted unless Customer provides written notice of any deficiency to CenturyLink within three business days after commencement of work or delivery of the Services, including phased delivery of Service, if applicable, (the "Acceptance Period"). Such notice must detail and demonstrate the deficiency to CenturyLink's reasonable satisfaction. CenturyLink will remedy the deficiency and will notify Customer accordingly, at which time a new Acceptance Period will begin. CenturyLink will delay billing until Services are accepted. The acceptance and Customer Commit Date in the Orders Section of the MSA will not apply to Services purchased under this Schedule.

4. Charges; Payment. This Section replaces the Commencement of Billing Section in the MSA. Customer will pay all charges as set forth in a SOW and applicable Taxes and Fees in accordance with the Agreement. If installation is delayed due to Customer, CenturyLink may begin charging Customer for Services, and Customer will pay such charges. Subject to the Acceptance section above, the Service Commencement Date for the Services is the date CenturyLink begins performing the Services or as provided in a SOW.

5. Termination. Either party may terminate a SOW upon 30 days prior written notice for default. CenturyLink may temporarily suspend any Service immediately in the event CenturyLink has a good faith belief that such suspension is reasonably necessary to mitigate damage or liability resulting from Customer's continued use of the Service. Cancellation charges will be identified in the SOW. Customer will remain liable for charges accrued but unpaid as of the termination date.

6. Software. Unless stated otherwise in a SOW, all software used to provide or provided in association with the Service will be subject to a separate End User License Agreement between Customer and the licensor of such software. All rights and remedies related to the software are strictly between Customer and such licensor. In addition, CenturyLink may require Customer to purchase vendor supported upgrades at an additional cost where needed for CenturyLink's continue provision of Services; CenturyLink may charge Customer for support or additional tasks incurred from Customers' continued use of an unsupported configuration. Customer acknowledges and agrees that it is solely responsible for ensuring its software and systems are current and supportable. Customer's failure to do so may result in CenturyLink's inability to provide the Services and CenturyLink will have no liability in such events.

7. Limitations; Disclaimer of Warranties. CenturyLink will not be liable for any damages incurred by Customer or third parties resulting from Customer's non-compliance with any standards which apply to Customer. Except for Customer's obligations under the Charges; Payment section, each party's total aggregate liability arising from or related to the Services will be limited to the total charges paid or payable under the SOW that gave rise to the claim. Customer's sole remedy for any dissatisfaction in the performance of any of the Services or deliverables is the Service Level Agreement ("SLA"), if applicable, or to terminate the relevant SOW. THE SERVICES, INCLUDING ANY DELIVERABLE AND ANY OPEN SOURCE SOFTWARE, ARE PROVIDED "AS IS" WITHOUT ANY WARRANTIES OF ANY KIND, WHETHER STATUTORY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, COMPLETENESS, COMPATIBILITY OF SOFTWARE OR EQUIPMENT, OR ANY RESULTS TO BE ACHIEVED THEREFROM. ANY OPEN SOURCE SOFTWARE IS PROVIDED ON AN "AS IS" BASIS. CENTURYLINK MAKES NO WARRANTIES OR REPRESENTATIONS THAT (A) ANY SERVICE OR ANY DELIVERABLE WILL BE FREE FROM LOSS OR LIABILITY ARISING OUT OF (I) HACKING OR SIMILAR MALICIOUS ACTIVITY, OR (II) ANY ACT OR OMISSION OF THE CUSTOMER, (B) ALL ERRORS CAN BE CORRECTED, (C) ALL RISKS, POTENTIAL SECURITY AND COMPLIANCE GAPS WILL BE ACCURATELY IDENTIFIED; OR (D) THAT THE DELIVERABLES AND SERVICES SHALL BE UNINTERRUPTED, ERROR-FREE, ACCURATE, COMPLETE OR EFFECTIVE IN ACHIEVING CUSTOMER'S SECURITY AND COMPLIANCE RELATED OBJECTIVES.

8. Business Contact Information. Customer and CenturyLink acknowledge that the performance of each party's obligations under this Schedule may require certain information, such as business contact information and credentials to access the applicable Customer portal(s), to be submitted to the other party. Each party shall be independently and separately responsible for complying with its obligations as a controller under applicable protection laws in its capacity as a data controller with respect to the business information it provides to the other party and/or receives from the other party.

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
PROFESSIONAL SECURITY SERVICES SCHEDULE**

9. Compliance and Security. CenturyLink has adopted and implemented, and will maintain, a corporate information security program designed to protect data transmitted or processed by CenturyLink from loss, misuse and unauthorized access or disclosure. Such program includes formal information security policies and procedures. The CenturyLink information security program is subject to reasonable changes by CenturyLink from time to time. Customer will ensure that all Customer data transmitted or processed via the Service complies with applicable law and reasonable information security practices, including those involving encryption.

10. Intellectual Property.

10.1 Customer License to Deliverables. Upon receipt of full payment CenturyLink grants to Customer irrevocable, perpetual, non-exclusive, world-wide, right and limited license under Level 3's copyright rights to internally use, reproduce, distribute copies of and prepare derivative works of the Document Deliverables ("Deliverable License"); provided however, Customer shall treat the Document Deliverables as "confidential" pursuant to the terms of the Agreement and any applicable confidentiality agreement(s) by and between Customer and CenturyLink unless otherwise agreed to by CenturyLink. For purposes of this Section, "Document Deliverables" shall mean any reports or other documentation prepared by CenturyLink exclusively for Customer pursuant to an applicable SOW under this Service Schedule. Other than the Deliverable License granted in this Section, Customer is not granted any license or other right (express, implied or otherwise) to use any trademarks, copyrights, service marks, trade names, patents, trade secrets, technology, know-how, or any other form of intellectual property rights, methodologies, report formats, templates, documentation or forms of CenturyLink or its affiliates.

10.2 CenturyLink License to Customer Technology and Customer Data. To the extent required by CenturyLink to provide the Service pursuant to an applicable SOW, Customer grants to CenturyLink a non-exclusive, non-transferable, royalty-free license to use Customer Technology and Content, and to sublicense Customer Technology and Content to CenturyLink subsidiaries and affiliates and any third parties providing all or part of the Services on behalf of CenturyLink. All right, title and interest in and to any Customer Technology and Content will remain solely with Customer, its affiliates and their licensors. Other than the license granted in this Section, CenturyLink is not granted any license or other right (express, implied or otherwise) to use any trademarks, copyrights, service marks, trade names, patents, trade secrets, technology, know-how, or any other form of intellectual property rights, methodologies, report formats, templates, documentation or forms of Customer or its affiliates. Customer represents and warrants that Customer will keep, back up and maintain its own copy of all materials and information, including Customer Technology and Content, that is provided or made available to CenturyLink hereunder. "Customer Technology and Content" means the technology, content and other information of Customer and its licensors, including Customer's Internet operations design, software tools, hardware designs, algorithms, software (in source and object forms), user interface designs, architecture, class libraries, objects and documentation (both printed and electronic), know-how, trade secrets and any related intellectual property rights throughout the world and also including any derivatives, improvements, enhancements or extensions of the foregoing created, conceived, reduced to practice, or developed by Customer during the Term.

10.3 Freedom of Action. Nothing in the Agreement will preclude CenturyLink from developing, marketing, and distributing any software or integration code or performing any services similar to the Services for itself or for any third party, provided that CenturyLink is in compliance with confidentiality obligations under the Agreement.

11. Non-solicitation. Until twelve months after the Term, each party will not directly or indirectly Solicit an Assigned Resource either to accept employment or a consulting or contractor relationship directly with it or to terminate his or her employment, agency or other relationship with the other party, unless it first obtains the other party's prior written consent. "Solicit" means any intentional contacts with Assigned Resource, regardless of who (*i.e.*, the party to this Agreement or the Assigned Resource) initiates the contact, that relates to the acceptance or termination of employment. "Assigned Resource" means an employee, consultant or contractor of the other party assigned by CenturyLink to perform the Services or by Customer to directly manage the Services.

12. Miscellaneous. In the event of a conflict between the terms in the MSA, this Schedule, any SOW, and any Change Request Form, the order of priority will be this Schedule, the SOW, the Change Request Form and then the MSA. Notwithstanding anything to the contrary in the Agreement, Customer is prohibited from reselling Services provided pursuant to this Schedule or any SOW without the express written consent of CenturyLink and, if applicable, CenturyLink's subcontractor. To the extent the Services involve the ongoing storage of or routine access to PHI (as defined under the Health Insurance Portability and Accountability Act of 1996, as amended, "HIPAA"), or CenturyLink is otherwise acting as a Business Associate (pursuant to HIPAA), CenturyLink will agree to the terms in its then-current Business Associate Agreement upon Customer's request.

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
CENTURYLINKSM ADAPTIVE THREAT INTELLIGENCE SERVICE
SERVICE SCHEDULE**

1. Applicability. This Service Schedule is applicable only where Customer orders CenturyLinkSM Adaptive Threat Intelligence service ("Service") provided by CenturyLink or a CenturyLink affiliate ("CenturyLink"). Adaptive Threat Intelligence service may be designated as "TI", "TIS", "Threat Intelligence", "Adaptive Threat Intelligence", "ATI" or "Threat Intelligence Service", in Customer Orders, Order acceptance, service delivery, billing and related documents. This Service Schedule incorporates the terms of the Master Service Agreement or other CenturyLink approved services agreement under which CenturyLink provides Services to Customer (the "Agreement"). In the event of any conflict between the Service Schedule and the Agreement, the Service Schedule will govern and control.

2. Definitions. Capitalized terms used and not otherwise defined herein shall have the meanings set forth in the Agreement or as commonly known in the industry.

"Event(s)" means the record of a data sample or other security abnormality indicating interaction between Customer's network and a known Malicious Entity detected by the Service or reported by Customer to the SOC.

"Excused Outage" shall also mean, for purposes of this Schedule, the Service Levels will not apply, and Customer will not be entitled to receive a credit or exercise a termination right under the applicable Service Level, for (a) the acts or omissions of Customer, its employees, contractors or agents or its end users; (b) the failure or malfunction of equipment, applications, the public Internet, or systems not owned or controlled by CenturyLink; (c) force majeure events; (d) Regularly Scheduled Maintenance or emergency maintenance, alteration or implementation; (e) the unavailability of required Customer personnel or the inability of CenturyLink to contact Customer related to the Service, including as a result of failure to provide CenturyLink with accurate, current contact information (including email) and an up to date escalation list; (f) CenturyLink's lack of access to the Customer premises where reasonably required to restore the Service; (g) Customer's failure to release the Service for testing or repair and/or continuing to use the Service on an impaired basis; (h) Customer's failure to provide timely approvals and/or consents, including allowing CenturyLink to retune the Service as required for CenturyLink to provide the Service; (i) improper or inaccurate network specifications provided by Customer; or (j) Customer fails to fulfill any of its responsibilities or obligations as detailed in the Agreement, this Service Schedule and/or any other guidelines or policies applicable to the Service.

"Malicious Entity" is an internet protocol address(es) or network domain(s) associated with attempts to commit spam, fraud, hacking, denial of service, and other malicious or illegal activities.

"Portal" means the Service specific web-based portal to which Customer will have access in order to monitor Customer's traffic and view Events.

"Regularly Scheduled Maintenance" means any scheduled maintenance performed to the Service. Regularly Scheduled Maintenance will not normally result in Service interruption. If Regularly Scheduled Maintenance requires an interruption, CenturyLink will: (a) provide Customer seven (7) days' prior written notice, (b) work with Customer to minimize such interruptions, and (c) use commercially reasonable efforts to perform such maintenance between midnight and 6:00 a.m. local time where the Service is located on which such maintenance is performed. Emergency maintenance may be performed on less or no notice.

"Secure DNS" is a feature designed to block malicious communications or Malicious Entities based on criteria established by Customer. Blocked communications or Malicious Entities are redirected to a warning page for Customer review.

"Service Outage" means that the Portal is unavailable to Customer.

"Service Validation" is confirmation by CenturyLink that the Service is operational and ready for use by the Customer.

"SIEM" means the security information event management platform configured, operated and maintained by Customer.

"SIEM Notification" is an optional feature available with the Service that allows customers to receive log and security event data at Customer's designated infrastructure destination.

"SOC" means CenturyLink's security operations center that among other duties, monitors the CenturyLink network infrastructure and security services provided to CenturyLink customers. Any third party network service provided by Customer is not supported or monitored by the SOC and instead, Customer is responsible for setting up and streaming all logs to CenturyLink for ingestion.

"Suspension" means CenturyLink's suspension of the Service as permitted by this Service Schedule or as otherwise allowed under the Agreement.

3. Service Description.

3.1 The Adaptive Threat Intelligence Service identifies Customer traffic flow interacting with known Malicious Entities identified by either IP address or network domain. If Customer purchases Internet service from a third party, Customer is required to provide CenturyLink with the IP addresses in order for CenturyLink to monitor the traffic. The Service uses meta data in the following principal techniques to identify these interactions:

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
CENTURYLINKSM ADAPTIVE THREAT INTELLIGENCE SERVICE
SERVICE SCHEDULE**

- Interactions automatically sensed from the CenturyLink Internet infrastructure via configured software installed on CenturyLink infrastructure
- DNS interactions for those customers who elect to use CenturyLink’s Secure DNS feature (available with Premium Option)
- Customer device logs (e.g. NetFlow, Firewall, DNS, etc.). Customer must elect to send logs to CenturyLink in order for CenturyLink to monitor them.

Customers that do not subscribe to CenturyLink Internet Services, elect not to use CenturyLink’s DNS services, and elect not to send device logs to CenturyLink will derive limited benefit from the Service, as there will be limited visibility into interactions with potentially Malicious Entities.

3.2 The Service provides notification for Events on an advisory basis only. Due to the varying nature of malicious activity and the sampled network approach, CenturyLink cannot guarantee that all Malicious Entities will be identified, detected and/or alerted; nor does CenturyLink guarantee that all Events are actual security events. To increase the robustness of the Service, Customer should report to CenturyLink any Events not effectively detected by the Service and reported Events that were not actual security events. It is Customer’s sole responsibility to review/investigate the reports and initiate action on the Event information. Customers with the Premium Option as further described below may request that SOC initiate blocking activity designed to prevent Event(s) or malicious communications. Customer acknowledges that CenturyLink is implementing actions at Customer’s request and in accordance with Customer identified criteria and CenturyLink is not responsible for the effectiveness of the blocking.

3.3 The Service is available in two (2) software as a service options, which Customer will select upon ordering: (i) Enhanced Threat Intelligence Service (“Enhanced Option”), and (ii) Premium Threat Intelligence Service (“Premium Option”).

Enhanced Option includes the following features:

- Monitoring of Customer’s traffic as it passes through CenturyLink Internet infrastructure based on sampled network analysis
- Correlation of meta data against Malicious Entities utilizing CenturyLink proprietary analysis and threat information
- Correlation with Customer device logs that are transmitted to the ATI
- Near real-time forwarding of Events to the Portal
- Portal-based reporting utilizing Events
- Set number of hours (identified in the table below) of SOC support per service package tier, to obtain additional Event information, if available.

| Service package tier (identified on the Order) | Hours of Support per month |
|--|----------------------------|
| Small | 4 |
| Medium | 8 |
| Large | 12 |

Premium Option includes the following:

- All features included in the Enhanced option of the Service; plus
- Near real-time Event feed to Customer’s SIEM
- Secure DNS feature. Customer will initiate a request for CenturyLink to initiate blocking via the Portal
- Set number of hours (identified in the table below) of SOC support per service package tier, to obtain additional Event information, if available.

| Service Package tier (identified on the Order) | Hours of Support per month |
|--|----------------------------|
| Small | 8 |
| Medium | 12 |
| Large | 16 |

3.4 SIEM Notification. The Enhanced Option does not require configuration changes in Customer’s environment. For the Event notification to Customer’s SIEM included in the Premium Option, Customer is responsible for configuring its SIEM platform and third party network environment to accept Events sent by CenturyLink. The Premium Option delivers Event notifications via syslog feed for up to 2 Customer provided SIEMs. Customer acknowledges that Event notifications sent to the SIEM are delivered over the Internet and such delivery may fail due to Internet connectivity issues outside of CenturyLink’s control. Customer acknowledges and agrees that SIEM Notification is provided “as-is” and “as available” and CenturyLink shall have no liability related to or arising from use by Customer of this feature.

For SIEM Notification Customer, and not CenturyLink, is responsible for storage of the logs received; however, CenturyLink has the ability to send/resend buffered logs if needed for up to 14 days. Customer acknowledges that CenturyLink’s ability to provide the SIEM Notification feature requires Customer to first provide CenturyLink with a digital certificate to be loaded on to the SIEM Notification platform in order for the log and security event traffic to be monitored by CenturyLink.

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
CENTURYLINKSM ADAPTIVE THREAT INTELLIGENCE SERVICE
SERVICE SCHEDULE**

Customer is responsible for configuring Customer's SIEM platform and network environment to allow, accept and store logs and/or security events transmitted by CenturyLink.

3.5 The Service correlates the threat meta data with the sampled information from the CenturyLink network. Consequently, if the Internet access is provided by a carrier other than CenturyLink, CenturyLink will be able to perform Service only for the traffic that transits the CenturyLink network. For example, the Service will not work on traffic that is transitted solely on a third-party carrier's network or traffic where the source and destination carrier transit does not involve CenturyLink.

3.6 Notwithstanding anything in the Agreement to the contrary, CenturyLink may, in its sole discretion, subcontract any or all of the work to be performed under this Service Schedule, including but not limited to, installation, monitoring, detection, correlation, and alerting services, provided that CenturyLink will remain responsible for the performance of its obligations hereunder. CenturyLink reserves the right at any time to, by way of example: (i) change or supplement the monitoring tools, algorithms and Event correlation techniques; (ii) increase or decrease the monitoring and correlation tools' sensitivity to anomalous IP traffic patterns; and (iii) modify the algorithms that identify IP traffic patterns that may indicate malicious activity. In addition, CenturyLink continually makes improvements to the Service and reserves the right to make any updates, error corrections, bug fixes, and other feature changes or modifications to any software, equipment or hardware utilized by CenturyLink to provide the Services, at any time. CenturyLink will use reasonable efforts to make changes during Regularly Scheduled Maintenance.

3.7 Any non-emergency changes or Service design changes that may be required outside of prefix additions, changing the users that are notified about Events, and changing Customer IPs for the delivery of Events require Customer to initiate a change request.

3.8 Portal Use. Use of the Service includes access to the Portal, and Portal access is limited to ten (10) Customer users via two factor authentication token ("2FA Token"). If a Customer user does not access the Portal for more than six (6) months, the Customer's 2FA Token will be disabled. If Customer wishes to have more than ten (10) users, additional recurring and non-recurring charges may apply. Customer will accept and comply with the End User Rules of Use associated with use of the 2FA Token. No Service Level applies to availability or use of 2FA Tokens.

3.9 Portal Data. CenturyLink, through its third party provider, collects a minimal amount of information about Customer personnel that are authorized to access the Portal. The personal data collected and used with respect to the Portal includes portal enrollment information, consisting of name, business email address, administrative authorizations and login credentials, and Portal event data, consisting of high-level information about individual user's actions within the Portal. CenturyLink will only use this information to provide access to the Portal and provide Customer with information about actions taken within the Portal.

3.10 In providing the Service, CenturyLink's access to Customer information is generally limited to machine/system generated logs and/or metrics that allows CenturyLink to provide the Service. Certain tools, features, or requests by Customer, including those related to deep packet access may require that CenturyLink have visibility to additional Customer data.

4. Charges; Early Termination.

4.1 Customer will be billed monthly in advance based on predefined amounts of IP addresses as shown on the Customer Order. The charges for Adaptive Threat Intelligence Service consist of 2 components: (a) a non-recurring installation charge ("NRC"); and (b) a monthly recurring charge ("MRC"). Charges for certain Services are subject to (a) a property tax surcharge and (b) a cost recovery fee per month to reimburse CenturyLink for various governmental taxes and surcharges. Such charges are subject to change by CenturyLink and will be applied regardless of whether Customer has delivered a valid tax exemption certificate. For additional details on taxes and surcharges that are assessed, visit <http://www.centurylink.com/taxes>.

4.2 The Service Commencement Date begins upon issuance of a CenturyLink Connection Notice. The Connection Notice will be issued on the first to occur of: (i) successful completion of Service Validation; or (ii) five (5) business days after CenturyLink notifies Customer that it has provisioned all components of the Service that CenturyLink can provision without Customer's assistance.

4.3 The Service Term will be identified in the relevant Order. Either party may terminate the Service at any time and without early termination liability during the Service Term by providing 30 days prior written notice to the other party.

5. IP Addresses.

5.1 If CenturyLink assigns Customer an IP address as part of the provision of Service (e.g. to provide a real time feed of Events to Customer's SIEM), the IP address shall, to the extent permitted by law, revert to CenturyLink after termination or expiration of the applicable Customer Order, and Customer shall cease using such address. At any time after such termination or expiration, CenturyLink may re-assign the IP address to another user.

5.2 If CenturyLink does not assign an IP address to Customer as part of the provision of Service, Customer represents and warrants that all title, right and interest in and to each IP address used by Customer in connection with the Service is owned exclusively by Customer and/or Customer has all permissions necessary from the owner to enable CenturyLink and Customer to perform their

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
CENTURYLINKSM ADAPTIVE THREAT INTELLIGENCE SERVICE
SERVICE SCHEDULE**

obligations hereunder. Customer shall defend, indemnify and hold CenturyLink harmless from any claim, demand or action arising in connection with a breach of the foregoing representation and warranty.

6. Work Product. If CenturyLink or any employee of CenturyLink develops or creates any intellectual property as part of the ATI Service ("ATI Intellectual Property"), that ATI Intellectual Property shall be, and remain, the exclusive property of CenturyLink and shall not be considered a work for hire. ATI Intellectual Property includes, by way of example, playbooks, runbooks, operational processes, and CenturyLink equipment configuration settings. Customer shall have no right to sell, lease, license or otherwise transfer, with or without consideration, any ATI Intellectual Property to any third party or permit any third party to reproduce or copy or otherwise use or see the ATI Intellectual Property in any form and shall use all reasonable efforts to ensure that no improper or unauthorized use of the ATI Intellectual Property is made. Customer shall not reverse engineer or de-compile any ATI Intellectual Property. Customer will promptly, upon termination of this Service Schedule or upon the request of CenturyLink, deliver to CenturyLink all such ATI Intellectual Property without retaining any copy or duplicate thereof.

7. Customer Responsibilities/Obligations.

7.1 Customer is obligated to provide CenturyLink with (i) accurate and current contact information and escalation lists, including an up-to-date point of contact with 24x7 availability who CenturyLink will coordinate with upon detection of Events; (ii) all IP addresses that will be monitored.

7.2 Customer must cooperate with CenturyLink and CenturyLink's vendors or subcontractors in coordinating setup of the Service, including but not limited to, configuring the Customer's SIEM platform to accept Event delivery from CenturyLink (if applicable).

7.3 Customer understands and expressly consents that in the performance of its obligations hereunder, Customer traffic may originate or terminate in a country other than the country of origination and/or destination of traffic.

7.4 Notwithstanding anything to the contrary in the Agreement, Customer agrees that CenturyLink may use meta data that it generates, monitors and/or captures in connection with providing the Service and metadata (not attributable to any customer) for forecasting trends, threat intelligence or correlating Customer traffic information on the Service infrastructure, and Customer represents and warrants that it has in place any necessary third party consents, permissions and/or rights to grant the foregoing rights to CenturyLink.

7.5 Customer must establish and consistently maintain reasonable and adequate security policies and devices for defense and protection of its assets. Customer is solely responsible for properly configuring and using the Service and taking its own steps to maintain appropriate security, protection and backup of meta data and logs, and information that transits the Internet, which may include the use of encryption technology to protect meta data, logs and other Customer information from unauthorized access and routine archiving. Given that Customer can self-provision and self-configure the Services and the Customer environment in ways that may reduce their security, notwithstanding anything else to the contrary in this Service Schedule or the Agreement, Customer acknowledges that it and not CenturyLink will be responsible for whether the Services and Customer environment are configured in a secure manner and no security requirements or obligations of CenturyLink shall apply. In addition, Customer is solely responsible to ensure that its use of the Service does not violate any laws, security policies or regulations, including the manner in which the Service is used or accessed by Customer or its authorized users.

8. In the event Customer or CenturyLink determine that the Service is being affected by a continuing error, conflict or trouble report, or similar issue (in each case a "Chronic Problem") caused by the Customer, Customer shall resolve any Chronic Problem by taking whatever steps are deemed necessary to rectify the same, including, but not limited to: (i) removing or modifying the existing Service configuration (or requesting CenturyLink to remove the same); or (ii) replacing Customer's equipment providing that be deemed necessary. If Customer has not remedied the Chronic Problem within 30 days of request by CenturyLink, then CenturyLink may suspend or terminate the Service. Service Levels shall not apply and Customer will not be entitled to receive a credit or exercise a termination right under an applicable Service Level during periods of Chronic Problems caused by Customer.

9. Business Contact Information. Customer and CenturyLink acknowledge that it may be necessary to provide the other party with certain personal data necessary for the performance of each party's obligations under this Service Schedule, such as business contact information and credentials to access the applicable Customer portal(s). The parties acknowledge and agree that each is a data controller in its own right with respect to any such personal data exchanged under this Service Schedule, and any such personal data is provided on a controller-to-controller basis. Any personal data exchanged under this Service Schedule shall be limited solely to the extent necessary for the parties to perform their obligations or exercise their rights under this Agreement. As used herein, the terms "personal data" and "controller" shall have the meanings ascribed to them in applicable data protection laws, including, without limitation, the European Union General Data Protection Regulation (Regulation (EU) 2016/679). Each party shall be independently and separately responsible for complying with its obligations as a controller under applicable data protection laws in its capacity as a data controller with respect to the personal data it provides to the other party and/or receives from the other party.

10. Disclaimer/Liability.

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
CENTURYLINKSM ADAPTIVE THREAT INTELLIGENCE SERVICE
SERVICE SCHEDULE**

10.1 Disclaimer. Customer acknowledges that the Services endeavor to mitigate security Events, but Events may not always be identified and if identified may not be mitigated entirely or rendered harmless. Customer further acknowledges that it should consider any particular Service as just one tool to be used as part of an overall security strategy and not a guarantee of security. The Service provided herein is a supplement to Customer’s existing security and compliance frameworks, network security policies and security response procedures, for which CenturyLink is not, and will not be, responsible. While CenturyLink will use reasonable commercial efforts to provide the Services hereunder in accordance with the SLA, the Services are otherwise provided “as-is”. CENTURYLINK MAKES NO WARRANTY, GUARANTEE, OR REPRESENTATION, EXPRESS OR IMPLIED, THAT ALL SECURITY THREATS AND VULNERABILITIES WILL BE DETECTED, THAT THE PERFORMANCE OF THE SERVICES WILL RENDER CUSTOMER’S SYSTEMS INVULNERABLE TO SECURITY BREACHES, THAT ANY THIRD PARTY SOFTWARE PROVIDED BY CUSTOMER WILL BE COMPATIBLE WITH THE SERVICE AND/OR THAT CENTURYLINK’S RECOMMENDATIONS, ASSESSMENTS, TESTS, REPORTS OR MONITORING WILL BE ACCURATE, COMPLETE, ERROR-FREE, OR EFFECTIVE IN ACHIEVING CUSTOMER’S SECURITY AND/OR COMPLIANCE RELATED OBJECTIVES. Neither CenturyLink or its subcontractors will be liable for any damages or liabilities however classified including third party claims which Customer or third parties may incur as a result of: (i) non-compliance with any standards which apply to Customer, and/or (ii) reliance upon (or implementation of recommendations from) results, reports, tests, or recommendations related to the Services; or (iii) loss or corruption of data or information transmitted through the Service.

10.2 Direct Damages. Except for the payment and indemnification obligations of Customer and subject to the waiver of consequential damages provision in the Agreement, the total aggregate liability of each party arising from or related to a claim shall not exceed in the aggregate the total MRCs, NRCs, and usage charges paid or payable to CenturyLink for the affected Services under this Service Schedule in the six months immediately preceding the first event giving rise to the cause of action (“Damage Cap”).

11. Resale Restriction. Notwithstanding anything to the contrary in the Agreement, Customer is prohibited from reselling any Service provided pursuant to this Schedule without the express written consent of CenturyLink.

12. Service Level Agreement (“Service Levels” or “SLA”), Service Objectives and Service Credits. The Service Levels are not available until completion of Service Validation. Whether a Service issue constitutes a Service Level outage or failure for Service credit purposes will be determined by CenturyLink in its good faith discretion supported by records, trouble tickets, data and other evidence, including through the use of third party monitoring tools. Service Credits are only available against the MRC for the affected Service. Service Levels do not apply to Excused Outages, periods of Suspension or periods of Chronic Problems.

12.1 Portal Availability Service Level. CenturyLink shall use commercially reasonable efforts to have the Portal available to Customer one hundred percent (100%) of the time after completion of Service Validation (the “Portal SLA”).

12.2 Portal Availability Service Credit. Portal Unavailability means access to the Portal is not available and Customer is unable to access and/or receive Event information via the Portal, even though Customer has entered appropriate credentials. If the aggregate Portal Unavailability during a calendar month meets or exceeds the durations identified below, the following remedies will apply.

| Aggregate Portal Unavailability Duration in a calendar Month (hrs:mins:secs) | Service Level Credit |
|---|----------------------|
| 00:00:01 – 00:04:59 | No Credit |
| 00:05:00 – 04:00:00 | 25% |
| 04:00:01 or greater | 50% |

12.3 Chronic Outage. In addition to the above credit(s) and as Customer’s sole remedy for any non-performance of the Service, Customer may elect to terminate an affected instance of the Service without termination liability within 30 calendar days of the date/time the right of termination is triggered if a single instance of Portal Unavailability meets or exceeds five consecutive days.

12.4 Time to Notify Service Level. For Customers (i) with the Enhanced Option, CenturyLink will notify Customer of an Event via the Portal within two (2) minutes of CenturyLink awareness of the Event; or (ii) with the Premium Option, CenturyLink will notify Customer of an Event via the Portal and a feed to the SIEM within two (2) minutes of CenturyLink awareness of the Event (individually and collectively the “TTN SLA”). Each time CenturyLink fails to meet the TTN SLA is a “Time to Notify Failure”. Regardless of the number of Time to Notify Failures in a single calendar day, Customer’s maximum credit per calendar day is one service level credit equal to 10% of the applicable MRC.

**CENTURYLINK MASTER SERVICE AGREEMENT
STATE, LOCAL AND EDUCATION GOVERNMENT AGENCIES VERSION
CENTURYLINKSM ADAPTIVE THREAT INTELLIGENCE SERVICE
SERVICE SCHEDULE**

12.5 Event Response Time Objective. The following are CenturyLink objectives only, no service credits will apply.

| Priority Level | Target Response Objective Enhanced Option | Target Response Objective Premium Option |
|---|---|--|
| <p style="text-align: center;">Priority 1 – High</p> <p>A critical Event is detected by the Service and Customer is under imminent threat of compromise.</p> | 24 hours | 2 hours |
| <p style="text-align: center;">Priority 2 – Medium</p> <p>An Event is detected by the Service and Customer can mitigate but requires additional information from CenturyLink.</p> | 24 hours | 8 hours |
| <p style="text-align: center;">Priority 3 – Low</p> <p>Standard informational request about threat signatures that may be explained in Portal FAQs, but nonetheless Customer would like to speak about the issue. This includes tuning requests.</p> | 1 business day | 1 business day |

12.6 General Terms for all Service Levels. To be eligible for credits, Customer must be current in its obligations, and Customer must contact CenturyLink Billing Inquiries via the contact information provided on the invoice, open a ticket in the Portal or contact their account manager to report any issue for which Customer thinks a Service Level may apply within 30 calendar days after the issue occurs. Credits will not apply to any other services provided by CenturyLink. Duplicative credits (e.g., for both a Portal Availability SLA and Time to Notify SLA) will not be awarded for a single failure, incident or outage. The aggregate credits in any calendar month shall not exceed 100% of the MRC of the affected Service. The Service Level credits and termination rights stated in this Service Schedule shall be Customer's sole and exclusive remedies with respect to any service failure or outage.

12.7 CenturyLink's Service Levels only apply to the respective vendors' supported configurations at the time SLA support requests are triggered. If any configuration, version, system or third party software is identified as "unsupported" by a vendor, CenturyLink's SLA (including availability of Service Credits) will no longer apply and any support by CenturyLink will be reasonable efforts only. In addition, and at CenturyLink's reasonable discretion: 1) Customer may be required to purchase vendor supported upgrades at an additional cost to allow CenturyLink to continue to provide the Services or; (2) CenturyLink may elect to charge the Customer for any support or additional tasks/work incurred resulting from Customers' continued use of an unsupported configuration. Customer acknowledges and agrees that it is solely responsible for selecting and ensuring its software and systems are up to date and supportable. Customer's failure to do so may result in CenturyLink's inability to provide the Services and CenturyLink shall have no liability therefrom.

Attachment B

Form 8 Supplement Sample Security Log Monitoring Project

Project Name: CLIENT NAME – Security Log Monitoring [Eval]



| PROJECT PROFILE | | |
|---|---|----------|
| <u>CLIENT Stakeholders:</u> | CL Owners: John Diogo, Dale Jordan Project Manager: <u>SLM Deployment Lead:</u> | |
| <u>Scope:</u> Descriptive narrative per the contract. | | |
| Overall Project Status: | 0% Complete | G |

| WEEKLY PROGRESS REPORT |
|---|
| <u>HEADLINES</u> |
| <u>NEAR TERM FOCUS</u> |
| <u>MISCELLANEOUS NOTES/ACTION ITEMS</u> |

| METRICS | ORIGIN TARGET | REVISED TARGET | ACTUAL | OUTLOOK | STATUS |
|--------------------------|---------------|----------------|--------|----------|--------|
| Targeted Completion Date | | | | On Track | G |

| MILESTONE | OWNER | TARGET DATE | ACTUAL DATE | STATUS |
|---|------------|-------------|-------------|----------|
| Initial Kick-Off Meeting | CTL/CLIENT | | | COMPLETE |
| Initiated Log Collector Appliance (LCA) | CTL/CLIENT | | | G |
| Completed Log Collector Appliance Build | CTL/CLIENT | | | G |
| Initiated Log Collection Services | CTL/CLIENT | | | G |
| Portal Training | CTL/CLIENT | | | G |
| Initiate Phase 3 – Tuning | CTL/CLIENT | | | G |
| Complete Log Collection Services | CTL/CLIENT | | | G |
| Billing/Evaluation Period Begins | CTL/CLIENT | | | G |
| Complete Phase 3 – Tuning | CTL/CLIENT | | | G |
| Go Live - Move Security Operations Center | CTL/CLIENT | | | G |
| Project Closure | CTL/CLIENT | | | G |
| Evaluation Period Ends | CTL/CLIENT | | | G |

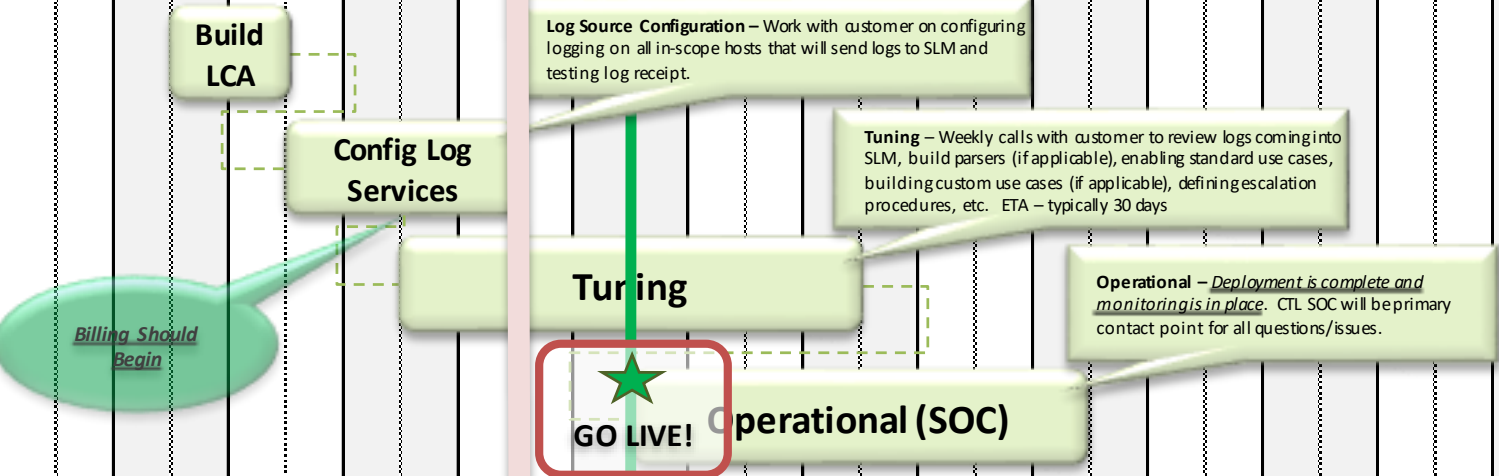
| RISK/ISSUES/CONCERN | OWNER/ CONTACT | REQD DATE | ACTUAL CLOSE | STATUS |
|---------------------|----------------|-----------|--------------|--------|
| | | | | |

| DEPENDENCIES/ KEY ENABLERS | OWNER/ CONTACT | REQD DATE | ACTUAL CLOSE | STATUS |
|----------------------------|----------------|-----------|--------------|--------|
| | | | | |

Project Name: CLIENT NAME - Security Log Monitoring [Eval]



| DATES | MAY | | | | | | | | JUNE | | | | | | | | JULY | | | | | | | AUGUST | | | | | | | | | | | | |
|-------------------------------|-------|-------|--------|-----------------------|--------|---------------------|--------|----------------------------|--------|-------|-------|----------------------------|--------|----------------------|--------|--------|--------|-------|-------|-------|--------|--------|--------|--------|--------|--------|-------|-------|-------|--------|--------|--------|--------|--------|--------|--|
| | 3-May | 6-May | 10-May | 13-May | 17-May | 20-May | 24-May | 27-May | 31-May | 3-Jun | 7-Jun | 10-Jun | 14-Jun | 17-Jun | 21-Jun | 24-Jun | 28-Jun | 1-Jul | 5-Jul | 8-Jul | 12-Jul | 15-Jul | 19-Jul | 22-Jul | 26-Jul | 29-Jul | 2-Aug | 5-Aug | 9-Aug | 12-Aug | 16-Aug | 19-Aug | 23-Aug | 26-Aug | 30-Aug | |
| WEEKS | | | | 1 | | 2 | | 3 | | 4 | | 5 | | 6 | | | | | | | | | | | | | | | | | | | | | | |
| Phase/Milestones | | | | ▲ Kick Off Meeting | | ▲ Status Meeting | | ▲ Status/Tuning Meeting | | | | ▲ Status/Tuning Meeting | | ▲ Closure Meeting | | | | | | | | | | | | | | | | | | | | | | |
| Security Log Monitoring (SLM) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |



Independence Day Holiday

Project Name: CLIENT NAME - Security Log Monitoring [Eval]



| Task Name | Durati | Start | Finish | Pri | Resource Names | % Work |
|---|----------------|--------------------|--------------------|-----------|---------------------------|-----------|
| CLIENT - Secure Log Monitoring | 6.8 wks | Wed 2/13/19 | Mon 4/1/19 | | CenturyLink,CLIENT | 0% |
| Statement of Work Approved | 0 days | Wed 2/13/19 | Wed 2/13/19 | | CLIENT | 0% |
| Assign Project Manager | 0 hrs | Wed 2/13/19 | Wed 2/13/19 | 2 | CenturyLink | 100% |
| Assign Deployment Lead | 0 hrs | Wed 2/13/19 | Wed 2/13/19 | 2 | CenturyLink | 100% |
| Project Kick-Off | 0 hrs | Wed 2/13/19 | Wed 2/13/19 | 3,4 | CenturyLink,CLIENT | 0% |
| Security Log Monitoring Deployment | 6.6 wks | Thu 2/14/19 | Mon 4/1/19 | 5 | CenturyLink,CLIENT | 0% |
| Phase 1 – Log Collector Setup | 7 days | Thu 2/14/19 | Fri 2/22/19 | | CenturyLink | 0% |
| Install VM/Log Collector Appliance (LCA) and test connectivity | 7 days | Thu 2/14/19 | Fri 2/22/19 | | CLIENT | 0% |
| Phase 2 – Log Source Configuration | 10 days | Mon 2/25/19 | Fri 3/8/19 | 7 | CenturyLink | 0% |
| Customer resources need to configure logging on all in-scope hosts that will send logs to SLM | 9 days | Mon 2/25/19 | Thu 3/7/19 | | CLIENT | 0% |
| Test log receipt | 1 day | Fri 3/8/19 | Fri 3/8/19 | 10 | CenturyLink | 0% |
| Phase 3 - Tuning, Parsing, Rule Deployment | 15 days | Mon 3/11/19 | Fri 3/29/19 | 11 | CenturyLink,CLIENT | 0% |
| Weekly calls with customer to review logs coming into SLM | 1 day | Mon 3/11/19 | Mon 3/11/19 | | CenturyLink | 0% |
| Build parsers (if applicable), enabling standard use cases, building custom use cases (if applicable) | 20 days | Mon 3/4/19 | Fri 3/29/19 | | CenturyLink | 0% |
| Conduct Client Portal Training | 1 day | Mon 3/25/19 | Mon 3/25/19 | | CenturyLink,CLIENT | 0% |
| Define escalation procedures, etc. | 1 day | Tue 3/26/19 | Tue 3/26/19 | 15 | CenturyLink | 0% |
| Project Closure Meeting | 0 days | Wed 3/27/19 | Wed 3/27/19 | | CenturyLink,CLIENT | 0% |

Attachment C

Form 8 Supplement Sample Monitoring and Management Project

| ID | Task Name | Duration | Start | Finish | Resource Names | % Complete | Notes | 16, '18 | M | T | W | T | F | S | Sep 23, '18 | S | M |
|----|---|-----------|--------------|--------------|--|------------|-------|---------|---|---|---|---|---|---|-------------|---|---|
| 1 | CTL Intelligent Monitoring and Management Program (CIMM) | 335 days? | Tue 9/18/18 | Fri 12/27/19 | | 84% | | | | | | | | | | | |
| 2 | Project #1 Present CIMM Solution using devices in DC3 | 85 days | Tue 9/18/18 | Mon 1/14/19 | | 100% | | | | | | | | | | | |
| 3 | Tasks Applicable to Entire Program | 195 days | Tue 9/18/18 | Fri 6/14/19 | | 88% | | | | | | | | | | | |
| 4 | Need Network diagram/visual of all new/current Tools, integrations, how model will work, i.e., tools -> Netcool->Vantive-->Remedy | 4 days | Wed 10/31/18 | Mon 11/5/18 | Ryan Cassily | 100% | | | | | | | | | | | |
| 5 | Create Test Plan with Use Cases for all projects--"living" document | 51 days | Wed 10/31/18 | Wed 1/9/19 | | 100% | | | | | | | | | | | |
| 6 | Connectivity: meet with CUSTOMER Security as CUSTOMER Security is gate keeper to provide connectivity | 1 day | Mon 11/19/18 | Mon 11/19/18 | Ben Fisher | 100% | | | | | | | | | | | |
| 7 | New Systems (4) Gen9s in AT1 and DC3 | 30 days | Tue 12/4/18 | Mon 1/14/19 | Andy Weber | 100% | | | | | | | | | | | |
| 8 | Need to address list of questions in document from CUSTOMER for Security | 1 day | Wed 11/21/18 | Wed 11/21/18 | | 100% | | | | | | | | | | | |
| 10 | Complete accurate count for devices for licenses for Monitoring Toolset | 1 day | Tue 11/20/18 | Tue 11/20/18 | Brian Booker,Casey Pope | 100% | | | | | | | | | | | |
| 11 | Integrate Monitoring Toolset with Netcool through Email Alerts available currently | 60 days | Fri 3/22/19 | Wed 6/12/19 | CTL Teams,Ryan Cassily,Missy White,Vaibh | 100% | | | | | | | | | | | |
| 12 | Monitoring Toolset APIs by CTL Tools Team | 60 days | Fri 3/22/19 | Wed 6/12/19 | CTL Teams,Ryan Cassily,Missy White,Vaibh | 50% | | | | | | | | | | | |
| 13 | Complete Runbooks for Support Center | 45 days | Mon 2/18/19 | Fri 4/19/19 | Tony Martin | 100% | | | | | | | | | | | |
| 14 | Support Center | 45 days | Mon 2/18/19 | Fri 4/19/19 | Tony Martin | 100% | | | | | | | | | | | |
| 15 | Set up Monitoring Toolset for HA in AT1 and DC3 and with 3rd VM | 6 days | Mon 4/29/19 | Mon 5/6/19 | Missy White,Ben Fisher | 100% | | | | | | | | | | | |
| 16 | Project #2 Support Center | 76 days? | Mon 3/18/19 | Fri 6/28/19 | | 85% | | | | | | | | | | | |
| 17 | First Support Center Device | 17 days | Mon 3/18/19 | Tue 4/9/19 | | 100% | | | | | | | | | | | |
| 18 | Monitoring Toolset Agent in Support Center | 47 days | Wed 1/16/19 | Thu 3/21/19 | | 100% | | | | | | | | | | | |
| 19 | Confirmed NUK for Monitoring Toolset Agent in Support Center | 9 days | Thu 2/21/19 | Tue 3/5/19 | | 100% | | | | | | | | | | | |
| 20 | VB complete config for NUK for Support Center Monitoring Toolset agent, then ship NUK to Support Center | 4 days | Mon 3/18/19 | Thu 3/21/19 | | 100% | | | | | | | | | | | |
| 21 | VB work with Russ when NUK onsite to complete installation. | 1 day | Mon 3/25/19 | Mon 3/25/19 | | 100% | | | | | | | | | | | |
| 22 | Confirmed F/W rules to implement in CUSTOMER corporate environment | 1 day | Wed 3/20/19 | Wed 3/20/19 | | 100% | | | | | | | | | | | |
| 23 | Need access to Support Center device--need community string | 20 days | Thu 3/7/19 | Wed 4/3/19 | CUSTOMER | 100% | | | | | | | | | | | |
| 24 | Original community string removed; need another | 20 days | Thu 3/7/19 | Wed 4/3/19 | | 100% | | | | | | | | | | | |
| 25 | Ryan provide steps for devices, ties to ASAs and integrating with Monitoring Toolset | 1 day | Tue 2/26/19 | Tue 3/5/19 | | 100% | | | | | | | | | | | |
| 26 | TACACS Connectivity | 82 days | Mon 12/17/18 | Tue 4/9/19 | | 100% | | | | | | | | | | | |
| 27 | Determine which TACACS to use--MES, CUSTOMER, CTL | 1 day | Mon 12/17/18 | Fri 1/25/19 | | 100% | | | | | | | | | | | |
| 28 | Determined CTL TACACS; to be ordered with connectivity requirements | 7 days | Fri 1/25/19 | Mon 2/4/19 | | 100% | | | | | | | | | | | |
| 29 | Set up CTL TACACS Connectivity | 33 days | Mon 2/4/19 | Wed 3/20/19 | | 100% | | | | | | | | | | | |
| 30 | DA to allow CUSTOMER VRF built off ASA to import/export with CTL mgmt VRF | 2 days | Fri 2/22/19 | Mon 2/25/19 | Robert Stenger | 100% | | | | | | | | | | | |
| 31 | Finalize management approvals, assign resources, confirm all requirements | 33 days | Mon 2/4/19 | Wed 3/20/19 | | 100% | | | | | | | | | | | |
| 32 | Design change per Architecture Team | 1 day | Wed 3/13/19 | Wed 3/13/19 | | 100% | | | | | | | | | | | |
| 33 | Complete Access to CTL TACACS | 15 days | Mon 3/11/19 | Fri 3/29/19 | | 100% | | | | | | | | | | | |
| 34 | Change ASA management connectivity to the CTL PML networks | 3 days | Mon 3/18/19 | Wed 3/20/19 | Ryan Cassily,Dan Ho | 100% | | | | | | | | | | | |
| 35 | Create CRQ with firewall change details | 15 days | Mon 3/11/19 | Fri 3/29/19 | Ryan Cassily | 100% | | | | | | | | | | | |
| 36 | enable routing thru the management interface | 15 days | Mon 3/11/19 | Fri 3/29/19 | Paul Kliensorge | 100% | | | | | | | | | | | |
| 37 | create the ACL rules and NAT rules to access CTL TACACS | 1 day | Mon 12/17/18 | Mon 12/17/18 | Ryan Cassily | 100% | | | | | | | | | | | |
| 38 | Review with Robert Davis if any security concerns for routing to CTL PML networks | 3 days | Tue 3/26/19 | Thu 3/28/19 | CUSTOMER,Ryan Cassily | 100% | | | | | | | | | | | |
| 39 | Verify the Support Center devices are added to Vantive | 1 day | Mon 4/1/19 | Mon 4/1/19 | Ryan Cassily,Brian Booker | 100% | | | | | | | | | | | |
| 40 | Run the search and get an output | 1 day | Mon 4/1/19 | Mon 4/1/19 | Ryan Cassily,Brian Booker | 100% | | | | | | | | | | | |
| 41 | Verify we have a service account created for Monitoring Toolset to use | 8 days | Fri 3/29/19 | Tue 4/9/19 | Ryan Cassily | 100% | | | | | | | | | | | |

Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |

| ID | Task Name | Duration | Start | Finish | Resource Names | % Complete | Notes | 16, '18 | M | T | W | T | F | S | Sep 23, '18 | S | M |
|----|--|----------|--------------------|--------------------|------------------------------|------------|-------|---------|---|---|---|---|---|---|-------------|---|---|
| 42 | Work with Blair Larsen from IT services group, which manages TACACS servers, to get service account created for Monitoring Toolset | 8 days | Fri 3/29/19 | Tue 4/9/19 | Ryan Cassily | 100% | | | | | | | | | | | |
| 43 | Configure the CUSTOMER network devices for TACACS-server directed request | 10 days | Wed 3/27/19 | Tue 4/9/19 | Ryan Cassily | 100% | | | | | | | | | | | |
| 44 | Work with Russell Bruce to check the provided devices for the proper configuration | 1 day | Mon 4/1/19 | Mon 4/1/19 | Ryan Cassily,Russell Bruce | 100% | | | | | | | | | | | |
| 45 | Change in switch | 1 day | Tue 4/9/19 | Tue 4/9/19 | Russell Bruce | 100% | | | | | | | | | | | |
| 46 | Access into the Support Center Network | 6 days | Tue 4/2/19 | Tue 4/9/19 | | 100% | | | | | | | | | | | |
| 47 | SSH and Telnet needed functionality - jumpbox (Data Center) | 1 day | Tue 4/2/19 | Tue 4/2/19 | | 100% | | | | | | | | | | | |
| 48 | Need jumpbox in the DC. Dedicated VM in DC3 and AT1. | 1 day | Tue 4/2/19 | Tue 4/2/19 | | 100% | | | | | | | | | | | |
| 49 | Action Items: (Scheduled Meeting) | 1 day | Thu 4/4/19 | Thu 4/4/19 | | 100% | | | | | | | | | | | |
| 50 | Discuss with Ben Fisher re: CUSTOMER dedicated VMs | 1 day | Thu 4/4/19 | Thu 4/4/19 | | 100% | | | | | | | | | | | |
| 51 | Review with Ben to determine OS on the VMs | 1 day | Thu 4/4/19 | Thu 4/4/19 | | 100% | | | | | | | | | | | |
| 52 | Implement | 1 day | Tue 4/9/19 | Tue 4/9/19 | | 100% | | | | | | | | | | | |
| 53 | Authentication test for firewalls to verify traffic processing correctly | 1 day | Wed 4/10/19 | Wed 4/10/19 | Paul Kliensorge,Ryan Cassily | 100% | | | | | | | | | | | |
| 54 | Test Alerts after implement | 6 days | Wed 4/10/19 | Wed 4/17/19 | | 100% | | | | | | | | | | | |
| 55 | Need Test Alert to use for validation | 6 days | Wed 4/10/19 | Wed 4/17/19 | CTL Team, Missy White | 100% | | | | | | | | | | | |
| 56 | Subset of Support Center Devices | 17 days | Wed 3/27/19 | Thu 4/18/19 | | 100% | | | | | | | | | | | |
| 57 | Confirm list of devices | 3 days | Wed 3/27/19 | Fri 3/29/19 | CUSTOMER | 100% | | | | | | | | | | | |
| 58 | Verify devices can connect to CTL TACACS for authentication | 1 day | Tue 4/9/19 | Tue 4/9/19 | | 100% | | | | | | | | | | | |
| 59 | In Vantive | 1 day | Mon 4/8/19 | Mon 4/8/19 | | 100% | | | | | | | | | | | |
| 60 | Implement | 1 day | Tue 4/9/19 | Tue 4/9/19 | | 100% | | | | | | | | | | | |
| 61 | Present to CUSTOMER to obtain approval to then move to remaining Support Center devices | 1 day | Thu 4/18/19 | Thu 4/18/19 | | 100% | | | | | | | | | | | |
| 62 | All Support Center Devices | 26 days? | Sun 4/28/19 | Fri 5/31/19 | | 100% | | | | | | | | | | | |
| 63 | Finalize list of remaining devices | 3 days | Mon 4/8/19 | Wed 4/10/19 | CUSTOMER | 100% | | | | | | | | | | | |
| 64 | Verify devices can connect to CTL TACACS for authentication | 5 days | Thu 5/2/19 | Wed 5/8/19 | Missy White,Russell Bruce | 100% | | | | | | | | | | | |
| 65 | CIMM on Support Center equipment with confirmed design and to implement | 40 days? | Mon 5/20/19 | Fri 7/12/19 | | 60% | | | | | | | | | | | |
| 66 | Wireless LAN controller and Prime built in Logic Monitor | 15 days? | Tue 6/4/19 | Mon 6/24/19 | | 61% | | | | | | | | | | | |
| 67 | Expectations for CIMM to APs to see if up/down, channels up, saturation of WAPs, etc. | 15 days | Tue 6/4/19 | Mon 6/24/19 | | 45% | | | | | | | | | | | |
| 68 | Feasibility of WAP with CIMM | 15 days? | Tue 6/4/19 | Mon 6/24/19 | | 69% | | | | | | | | | | | |
| 69 | CUSTOMER to approve SNMP config | 10 days | Mon 6/3/19 | Fri 6/14/19 | | 68% | | | | | | | | | | | |
| 70 | Need to identify if any monitoring GAPS to resolve, capabilities, issues | 15 days | Tue 6/4/19 | Mon 6/24/19 | | 75% | | | | | | | | | | | |
| 71 | Submit MOP to add SNMP configuration information to WLC. Aaron King opening Cisco TAC to determine TACACS authentication to CTL servers. | 1 day | Wed 6/19/19 | Wed 6/19/19 | Aaron King | 0% | | | | | | | | | | | |
| 72 | Routers and Switches | 11 days | Tue 6/4/19 | Tue 6/18/19 | | 75% | | | | | | | | | | | |
| 73 | Integrated with health monitor--to tweak | 11 days | Tue 6/4/19 | Tue 6/18/19 | Missy White | 75% | | | | | | | | | | | |
| 74 | Confirm seeing stats and alerts | 11 days | Tue 6/4/19 | Tue 6/18/19 | Missy White | 75% | | | | | | | | | | | |
| 75 | Kim, Brian, Russ and Ryan in STL with Adaptive Support | 3 days | Wed 6/19/19 | Fri 6/21/19 | | 100% | | | | | | | | | | | |
| 76 | Integrate with Prime and WAPs for onsite engineers need access and training and remote engineers to be able to use tools | 3 days | Wed 6/19/19 | Fri 6/21/19 | | 100% | | | | | | | | | | | |
| 77 | Test alerts, document devices' locations, simulate events--P1 process | 5 days | Mon 6/24/19 | Fri 6/28/19 | | 0% | | | | | | | | | | | |
| 78 | QA and ChaosMonkey for network devices | 5 days | Mon 6/24/19 | Fri 6/28/19 | | 0% | | | | | | | | | | | |
| 79 | Pull reports | 5 days | Mon 6/24/19 | Fri 6/28/19 | | 0% | | | | | | | | | | | |
| 80 | Hand over tools to CTL TOOLS TEAM for their Ownership. Work with CTL Product | 30 days | Thu 6/20/19 | Wed 7/31/19 | | 0% | | | | | | | | | | | |
| 81 | Project #5: Deploy to remaining CUSTOMER Data Center environment | 171 days | Mon 3/11/19 | Fri 11/1/19 | | 0% | | | | | | | | | | | |

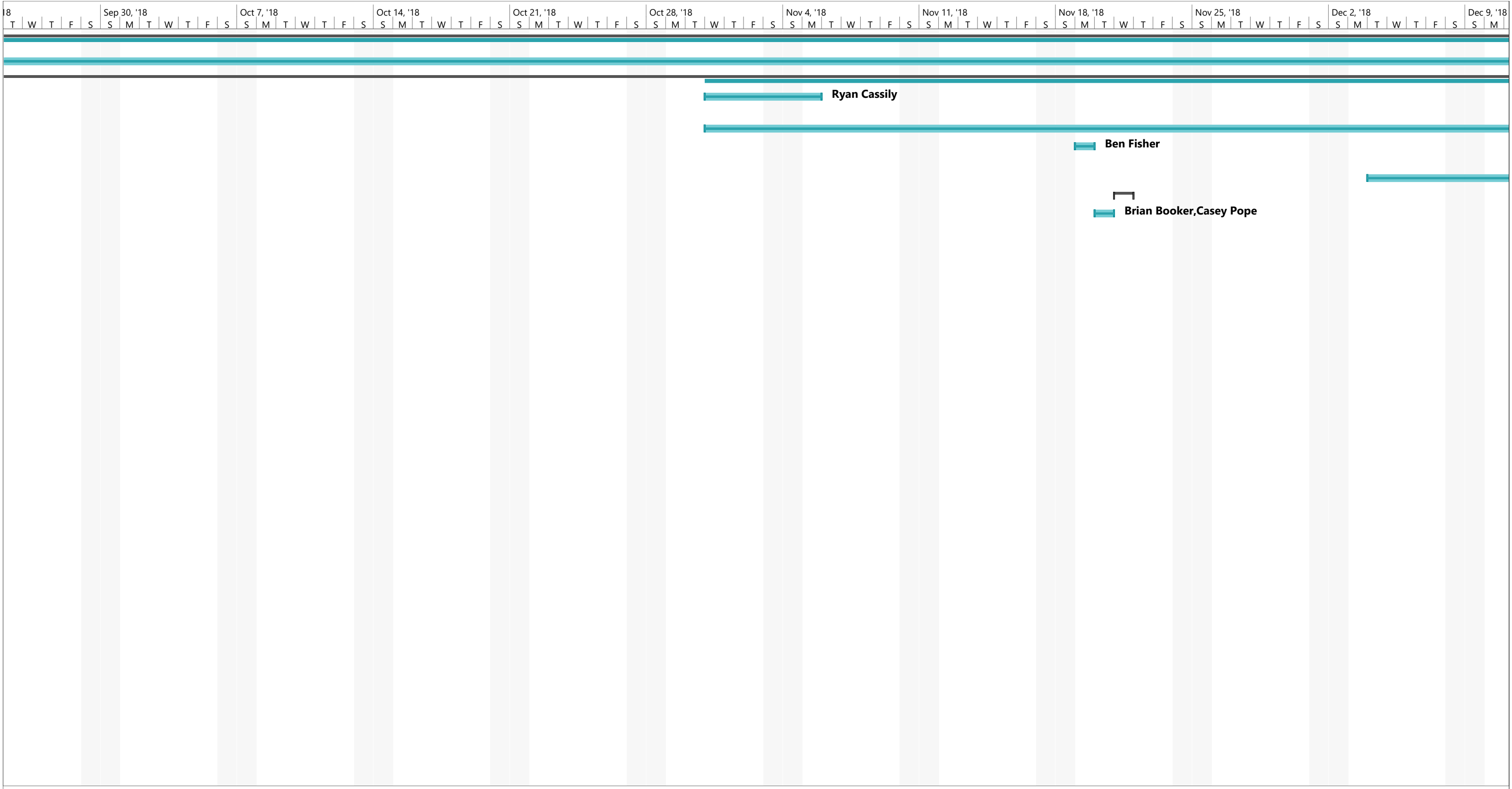
Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |

| ID | Task Name | Duration | Start | Finish | Resource Names | % Complete | Notes | 16, '18 | | | | | | | Sep 23, '18 | | | |
|----|---|----------|-------|--------------|----------------|------------|-------|---------|---|---|---|---|---|---|-------------|--|--|--|
| | | | | | | | | M | T | W | T | F | S | S | M | | | |
| 85 | Project #6: Determine CUSTOMER tools to Integrate into CTL toolset, e.g., Splunk and Logic Monitor | | | Fri 12/20/19 | | 0% | | | | | | | | | | | | |

Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



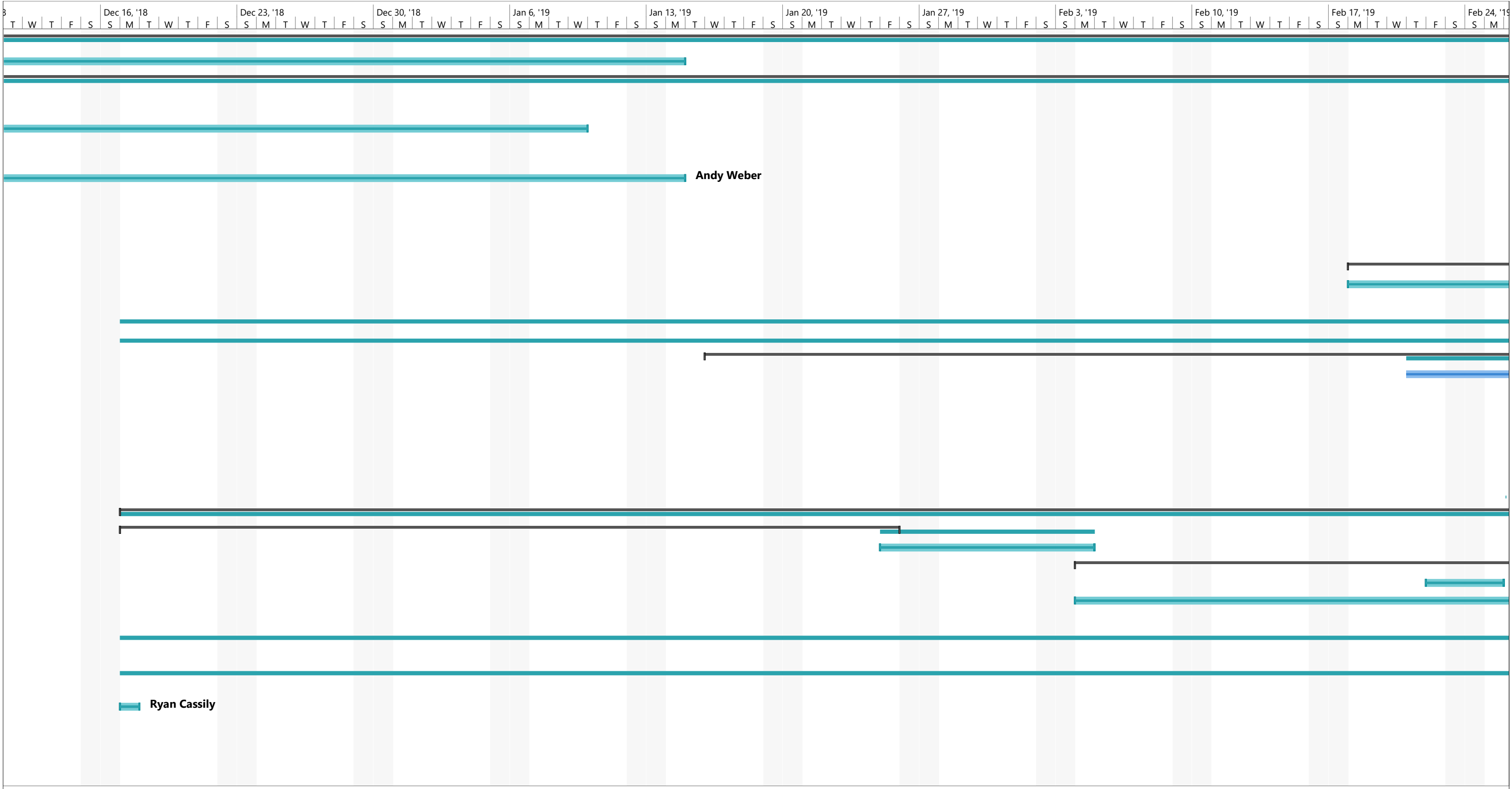
Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



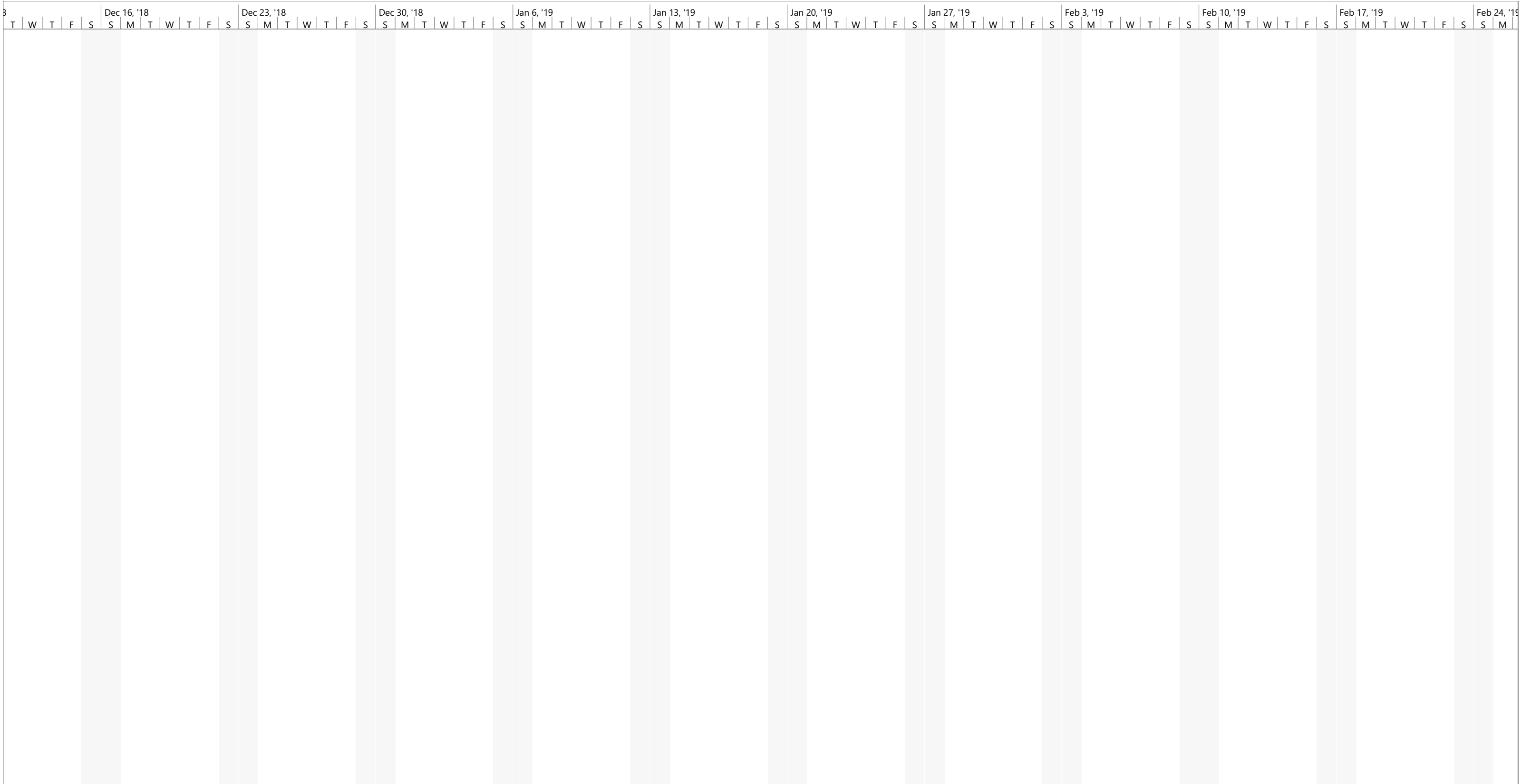
Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



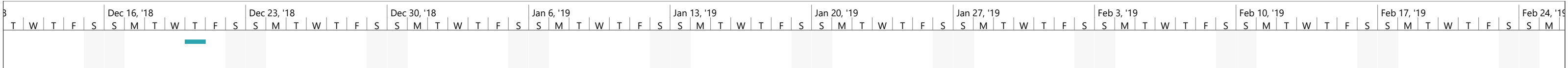
Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



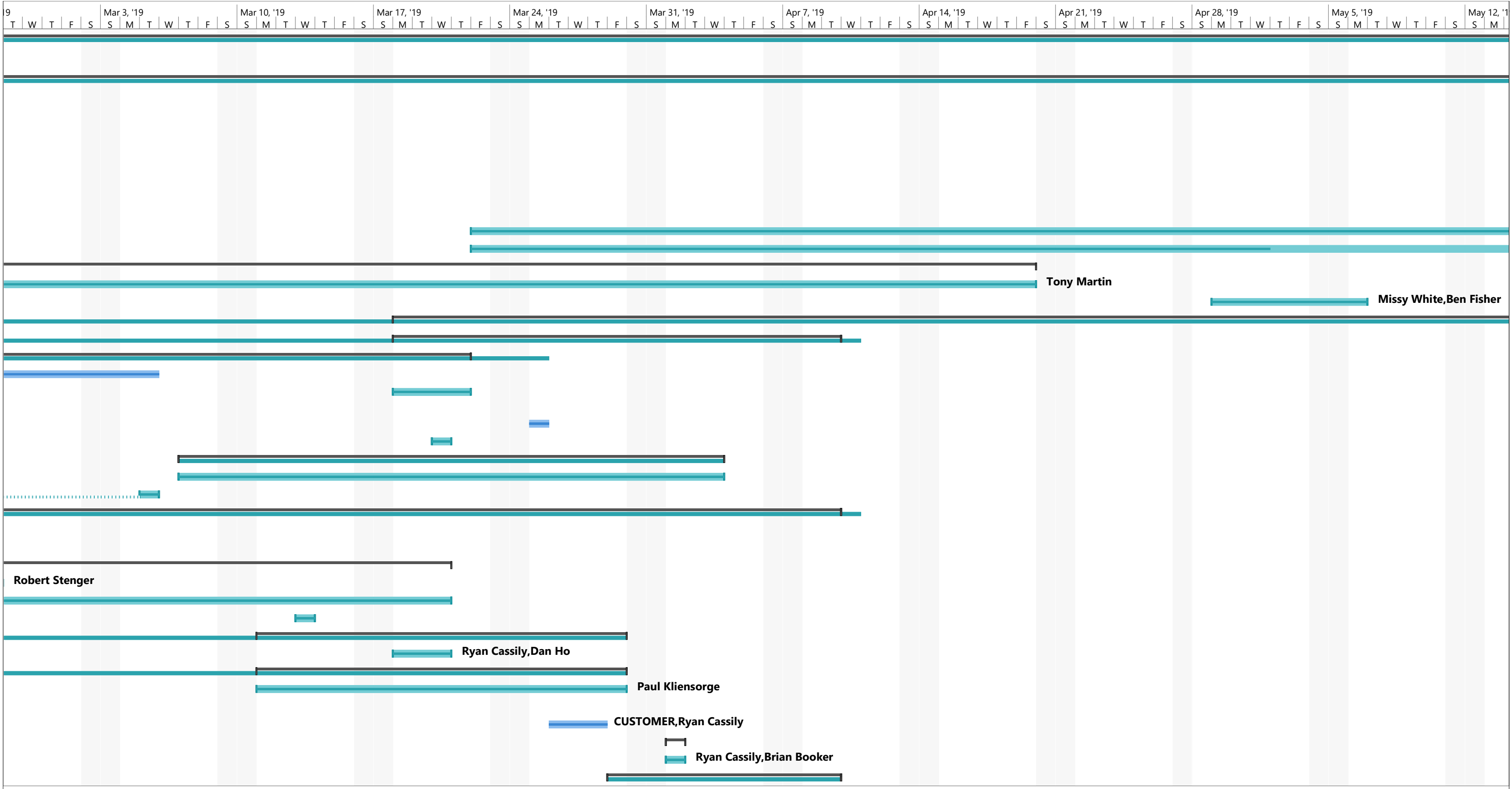
Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



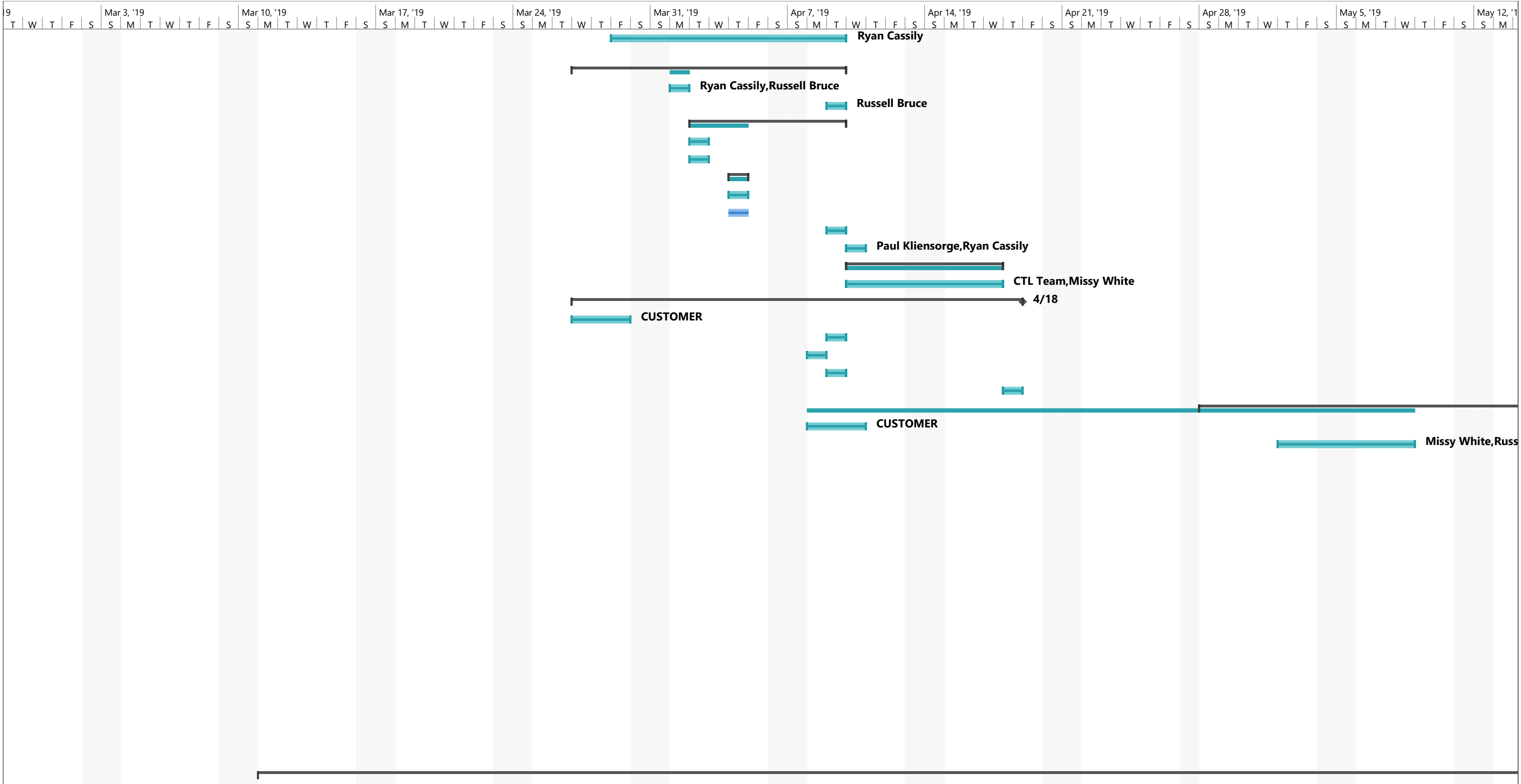
Project: CFA CIM Program Plan
 Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



Project: CFA CIM Program Plan
Date: Fri 7/5/19

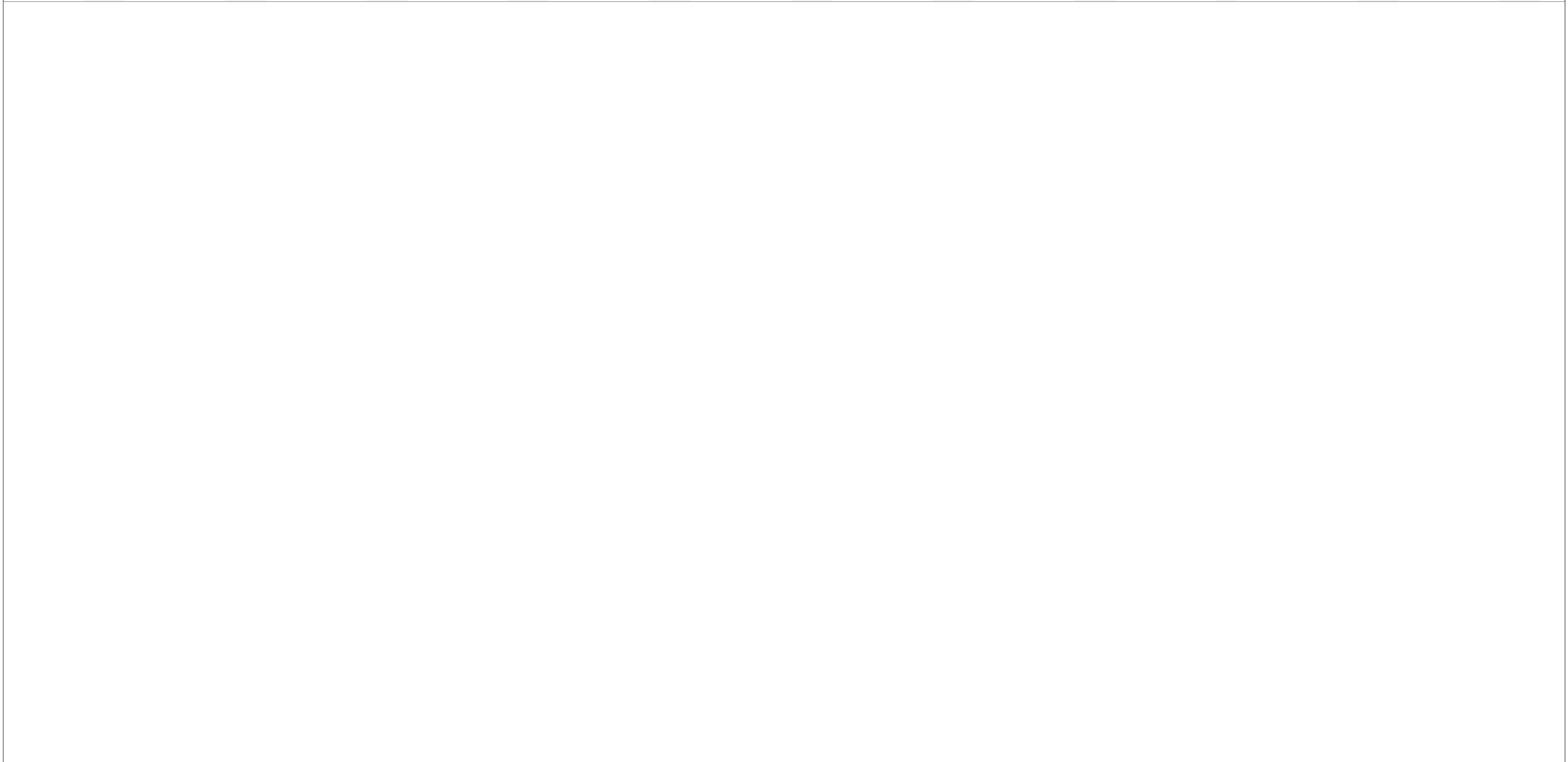
| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



Project: CFA CIM Program Plan
Date: Fri 7/5/19

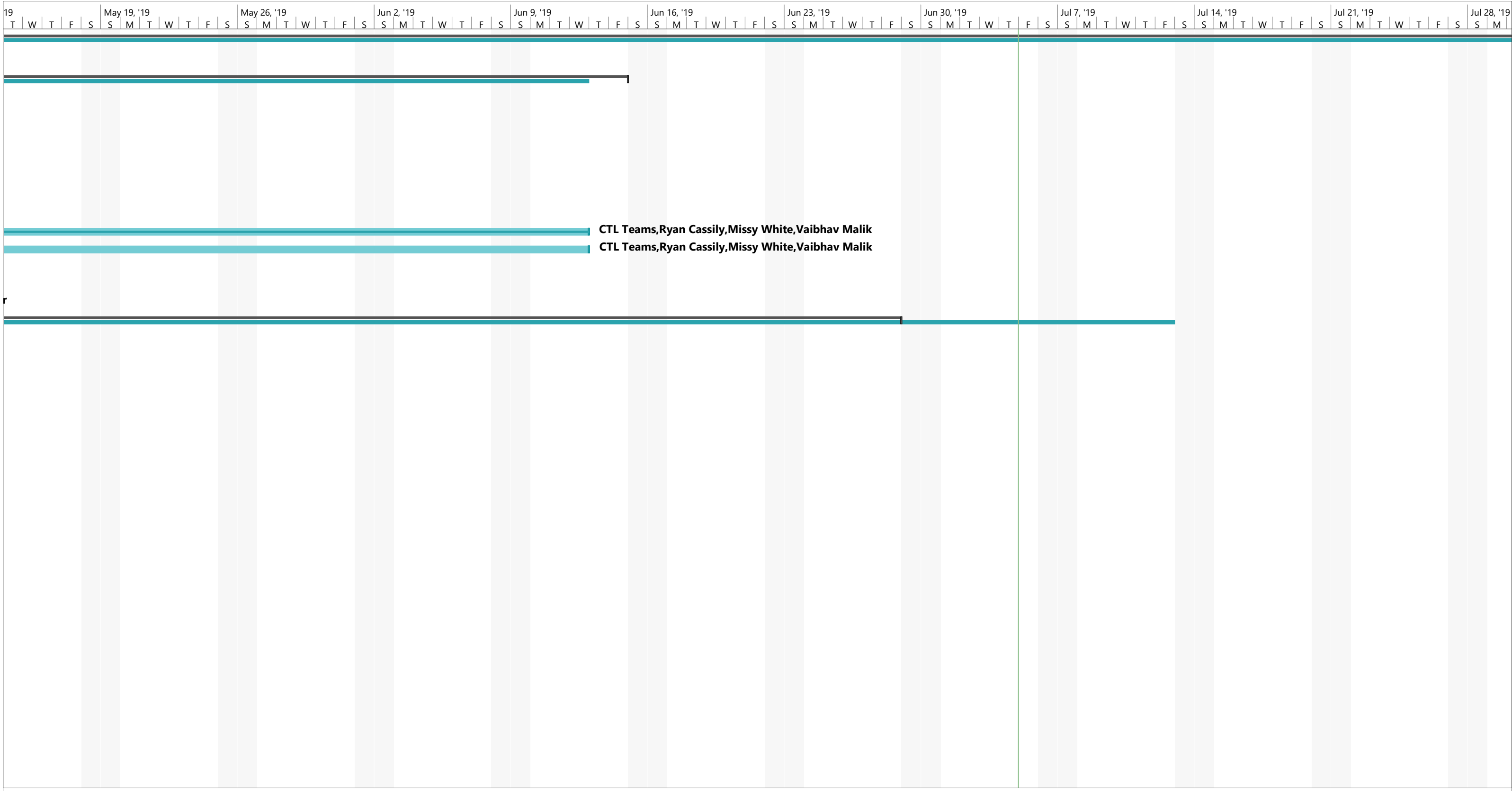
| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |

9 T W T F S Mar 3, '19 S M T W T F S Mar 10, '19 S M T W T F S Mar 17, '19 S M T W T F S Mar 24, '19 S M T W T F S Mar 31, '19 S M T W T F S Apr 7, '19 S M T W T F S Apr 14, '19 S M T W T F S Apr 21, '19 S M T W T F S Apr 28, '19 S M T W T F S May 5, '19 S M T W T F S May 12, '19



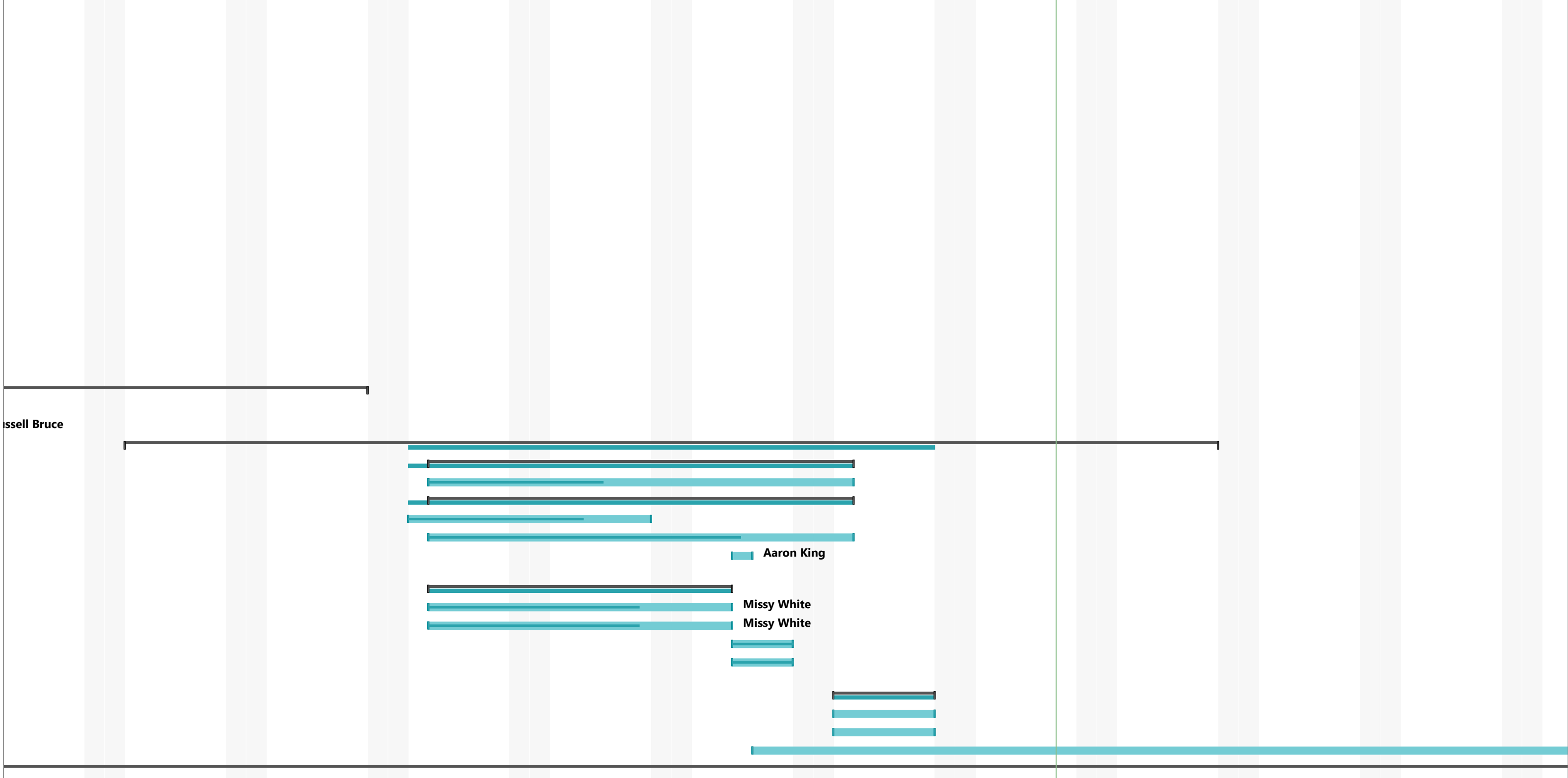
Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



Project: CFA CIM Program Plan
Date: Fri 7/5/19

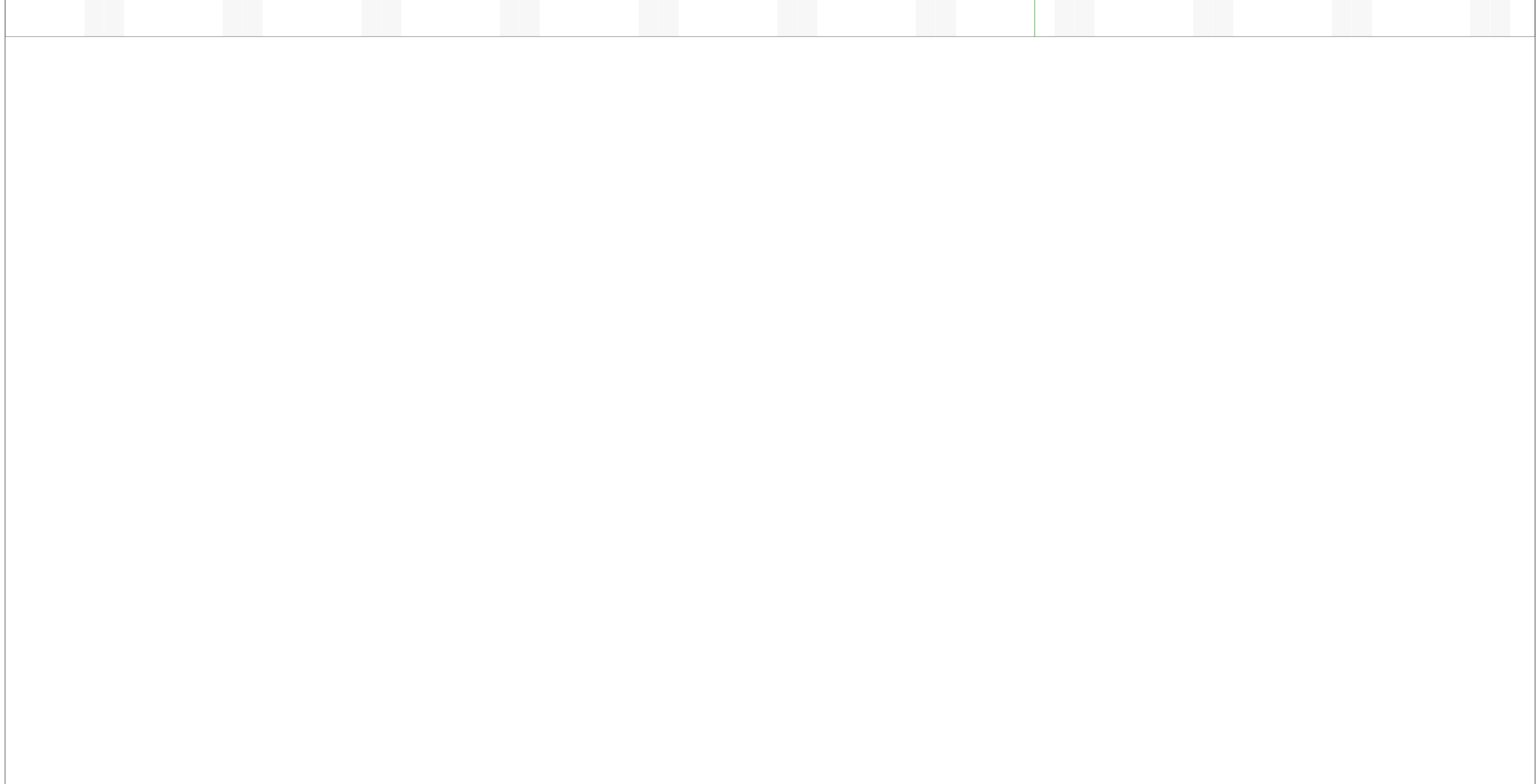
| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |

19 | T | W | T | F | S | May 19, '19 | S | M | T | W | T | F | S | May 26, '19 | S | M | T | W | T | F | S | Jun 2, '19 | S | M | T | W | T | F | S | Jun 9, '19 | S | M | T | W | T | F | S | Jun 16, '19 | S | M | T | W | T | F | S | Jun 23, '19 | S | M | T | W | T | F | S | Jun 30, '19 | S | M | T | W | T | F | S | Jul 7, '19 | S | M | T | W | T | F | S | Jul 14, '19 | S | M | T | W | T | F | S | Jul 21, '19 | S | M | T | W | T | F | S | Jul 28, '19 | S | M



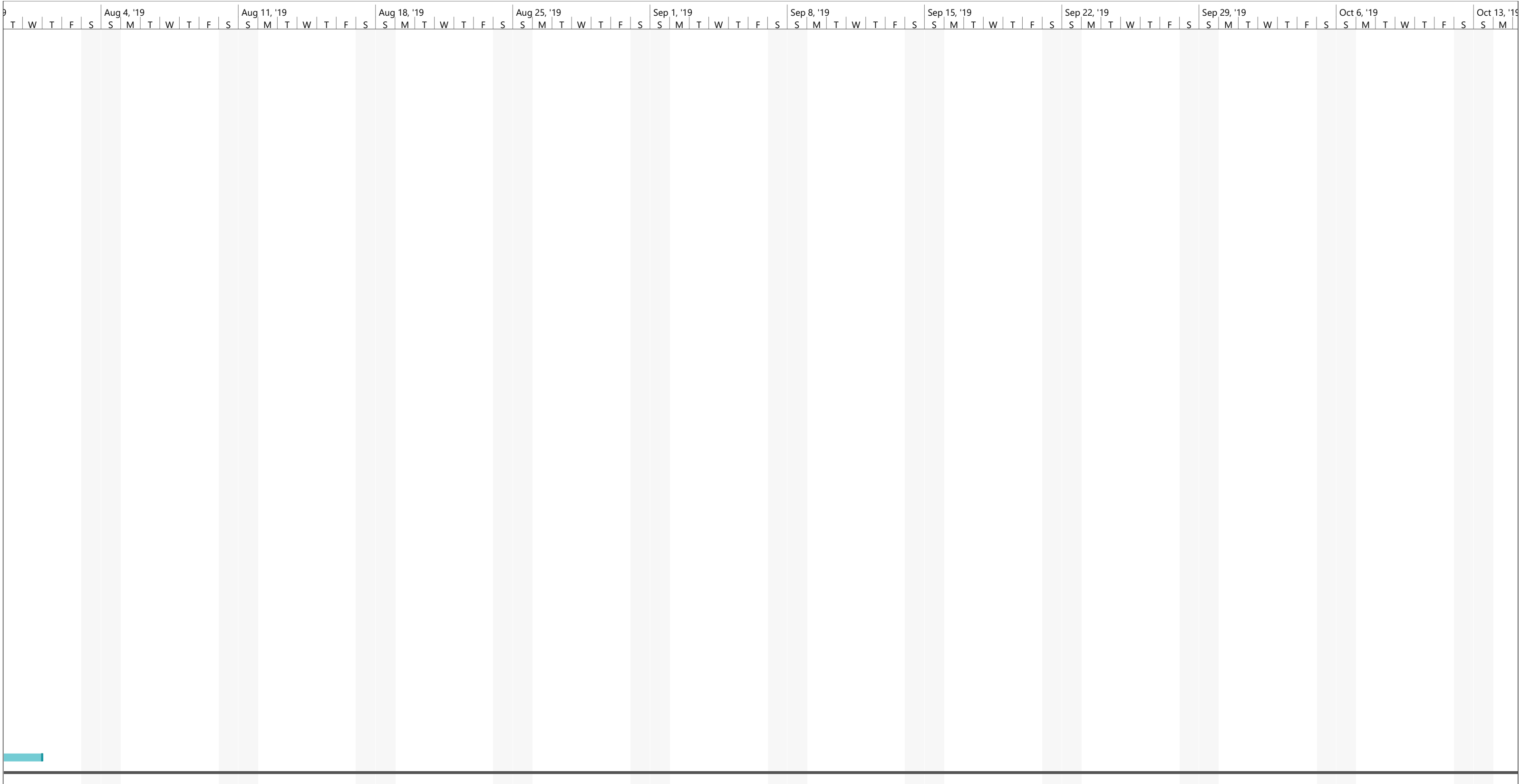
Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



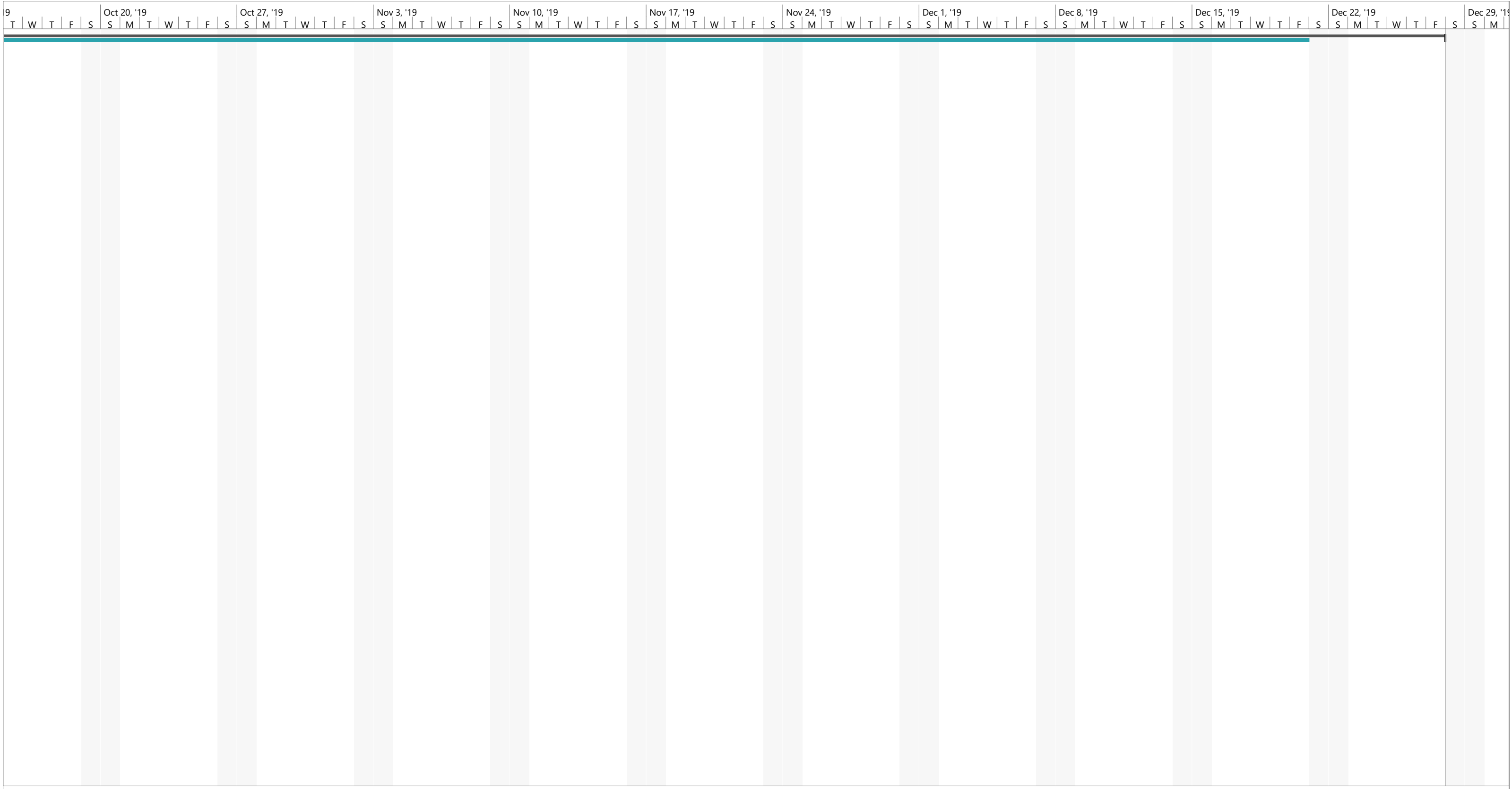
Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



Project: CFA CIM Program Plan
 Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |



Project: CFA CIM Program Plan
Date: Fri 7/5/19

| | | | | | | | | | |
|-----------|--|--------------------|--|-----------------------|--|--------------------|--|-----------------|--|
| Task | | Project Summary | | Manual Task | | Start-only | | Deadline | |
| Split | | Inactive Task | | Duration-only | | Finish-only | | Progress | |
| Milestone | | Inactive Milestone | | Manual Summary Rollup | | External Tasks | | Manual Progress | |
| Summary | | Inactive Summary | | Manual Summary | | External Milestone | | | |

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 - BAFO Submission - 8/28/2019 | | | | | | |
|--|----------------------------|----------------------------|----------------------------|--|---|--|
| 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 | Comments |
| 1.0 Security Operations Services | \$ 81,629.40 | \$ 81,629.40 | \$ 81,629.40 | \$ 81,629.40 | \$ 81,629.40 | |
| 1.1 Core Security Operations Services | \$ 17,220.00 | \$ 17,220.00 | \$ 17,220.00 | \$ 17,220.00 | \$ 17,220.00 | Plus non-recurring charge shown below. |
| 1.2 Analytics Platform Operations | \$ 6,420.00 | \$ 6,420.00 | \$ 6,420.00 | \$ 6,420.00 | \$ 6,420.00 | This item should not be considered an optional selection. It is required for effective Security Log Monitoring. MRC is based on 9,200 Users. |
| 1.3 Email Threat Monitoring and Analysis | \$ 5,078.40 | \$ 5,078.40 | \$ 5,078.40 | \$ 5,078.40 | \$ 5,078.40 | |
| 1.4 Cyber Intelligence Support | \$ 10,800.00 | \$ 10,800.00 | \$ 10,800.00 | \$ 10,800.00 | \$ 10,800.00 | |
| 1.5 Security System Support | \$ 42,984.01 | \$ 42,984.01 | \$ 42,984.01 | \$ 42,984.01 | \$ 42,984.01 | Security System Support can be satisfied by the same staff providing Onsite Services (1.6). |
| 1.6 Onsite Services | | | | | | Either 1.5 or 1.6 should be selected. |
| 1.6.1 Onsite Tier 3 Infrastructure Security Engineer | \$ 20,278.00 | \$ 20,278.00 | \$ 20,278.00 | \$ 20,278.00 | \$ 20,278.00 | 160 Hours/month |
| 1.6.2 Onsite Tier 3 Cyber Security Analyst | \$ 15,290.00 | \$ 15,290.00 | \$ 15,290.00 | \$ 15,290.00 | \$ 15,290.00 | 160 Hours/month |
| 1.6.3 16 hours/month onsite information security engineering support | \$ 2,043.00 | \$ 2,043.00 | \$ 2,043.00 | \$ 2,043.00 | \$ 2,043.00 | 16 Hours/month |
| 1.7 Threat Hunting | \$ 4,500.00 | \$ 4,500.00 | \$ 4,500.00 | \$ 4,500.00 | \$ 4,500.00 | |
| 1.8 Compromise Assessment | \$ - | \$ - | \$ - | \$ - | \$ - | Plus non-recurring charge shown below. |
| DESCRIPTION | Year 1- Non-Recurring Cost | Year 2- Non-Recurring Cost | Year 3- Non-Recurring Cost | Optional Renewal Year 1 Non-Recurring Cost | Optional Renewal Year 2- Non-Recurring Cost | |
| 1.1 Core Security Operations Services | \$ 35,400.00 | \$ 35,400.00 | \$ 35,400.00 | \$ 35,400.00 | \$ 35,400.00 | Non-recurring charges are billed once at beginning of year. CenturyLink may consider amortizing the NRCs upon further discussion. |
| 1.8 Compromise Assessment | \$ 23,600.00 | \$ 23,600.00 | \$ 23,600.00 | \$ 23,600.00 | \$ 23,600.00 | Non-recurring charges are billed once at beginning of year. CenturyLink may consider amortizing the NRCs upon further discussion. |

Notes:

In the initial solution, we assumed an aggressive rate of compression for data ingestion (200 GB to 25 GB). Without changing price, we have adjusted to a much more conservative assumption of data compression (200 GB to 180GB) to be attained at CenturyLink's risk. We believe your actual compression rate will exceed this, thereby providing the City plenty of headroom for growth.

We worked hard to provide our best pricing in the initial proposal; however, as a demonstration of our commitment to the City, we were able to further reduce the price by more than \$5000 per month.

In addition, we are pleased to offer, at no additional charge, planning assistance to the City of approximately 40-80 hours in preparation for the Republican National Convention. This planning assistance will be provided by CenturyLink Client Engagement Manager(s) and other SMEs.

| Part One- Security Operations Services - Reductions Between BAFO Submission and RFP Response | | | | | | |
|--|----------------------------|----------------------------|----------------------------|--|---|--|
| 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 | \$ 5,373.01 | \$ 5,373.01 | \$ 5,373.01 | \$ 5,373.01 | \$ 5,373.01 | |
| 1.1 Core Security Operations Services | \$ - | \$ - | \$ - | \$ - | \$ - | |
| 1.2 Analytics Platform Operations | \$ - | \$ - | \$ - | \$ - | \$ - | |
| 1.3 Email Threat Monitoring and Analysis | \$ - | \$ - | \$ - | \$ - | \$ - | |
| 1.4 Cyber Intelligence Support | \$ - | \$ - | \$ - | \$ - | \$ - | |
| 1.5 Security System Support | \$ - | \$ - | \$ - | \$ - | \$ - | |
| 1.6 Onsite Services | \$ - | \$ - | \$ - | \$ - | \$ - | |
| 1.6.1 Onsite Tier 3 Infrastructure Security Engineer | \$ 2,896.86 | \$ 2,896.86 | \$ 2,896.86 | \$ 2,896.86 | \$ 2,896.86 | |
| 1.6.2 Onsite Tier 3 Cyber Security Analyst | \$ 2,184.29 | \$ 2,184.29 | \$ 2,184.29 | \$ 2,184.29 | \$ 2,184.29 | |
| 1.6.3 16 hours/month onsite information security engineering support | \$ 291.86 | \$ 291.86 | \$ 291.86 | \$ 291.86 | \$ 291.86 | |
| 1.7 Threat Hunting | \$ - | \$ - | \$ - | \$ - | \$ - | |
| 1.8 Compromise Assessment | \$ - | \$ - | \$ - | \$ - | \$ - | |
| DESCRIPTION | Year 1- Non-Recurring Cost | Year 2- Non-Recurring Cost | Year 3- Non-Recurring Cost | Optional Renewal Year 1 Non-Recurring Cost | Optional Renewal Year 2- Non-Recurring Cost | |
| 1.1 Core Security Operations Services | \$ - | \$ - | \$ - | \$ - | \$ - | |
| 1.8 Compromise Assessment | \$ - | \$ - | \$ - | \$ - | \$ - | |

| Part One- Security Operations Services - RFP Response - 7/15/2019 | | | | | | |
|--|----------------------------|----------------------------|----------------------------|--|---|--|
| 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 | \$ 87,002.41 | \$ 87,002.41 | \$ 87,002.41 | \$ 87,002.41 | \$ 87,002.41 | |
| 1.1 Core Security Operations Services | \$ 17,220.00 | \$ 17,220.00 | \$ 17,220.00 | \$ 17,220.00 | \$ 17,220.00 | |
| 1.2 Analytics Platform Operations | \$ 6,420.00 | \$ 6,420.00 | \$ 6,420.00 | \$ 6,420.00 | \$ 6,420.00 | |
| 1.3 Email Threat Monitoring and Analysis | \$ 5,078.40 | \$ 5,078.40 | \$ 5,078.40 | \$ 5,078.40 | \$ 5,078.40 | |
| 1.4 Cyber Intelligence Support | \$ 10,800.00 | \$ 10,800.00 | \$ 10,800.00 | \$ 10,800.00 | \$ 10,800.00 | |
| 1.5 Security System Support | \$ 42,984.01 | \$ 42,984.01 | \$ 42,984.01 | \$ 42,984.01 | \$ 42,984.01 | |
| 1.6 Onsite Services | | | | | | |
| 1.6.1 Onsite Tier 3 Infrastructure Security Engineer | \$ 23,174.86 | \$ 23,174.86 | \$ 23,174.86 | \$ 23,174.86 | \$ 23,174.86 | |
| 1.6.2 Onsite Tier 3 Cyber Security Analyst | \$ 17,474.29 | \$ 17,474.29 | \$ 17,474.29 | \$ 17,474.29 | \$ 17,474.29 | |
| 1.6.3 16 hours/month onsite information security engineering support | \$ 2,334.86 | \$ 2,334.86 | \$ 2,334.86 | \$ 2,334.86 | \$ 2,334.86 | |
| 1.7 Threat Hunting | \$ 4,500.00 | \$ 4,500.00 | \$ 4,500.00 | \$ 4,500.00 | \$ 4,500.00 | |
| 1.8 Compromise Assessment | \$ - | \$ - | \$ - | \$ - | \$ - | |
| DESCRIPTION | Year 1- Non-Recurring Cost | Year 2- Non-Recurring Cost | Year 3- Non-Recurring Cost | Optional Renewal Year 1 Non-Recurring Cost | Optional Renewal Year 2- Non-Recurring Cost | |
| 1.1 Core Security Operations Services | \$ 35,400.00 | \$ 35,400.00 | \$ 35,400.00 | \$ 35,400.00 | \$ 35,400.00 | |
| 1.8 Compromise Assessment | \$ 23,600.00 | \$ 23,600.00 | \$ 23,600.00 | \$ 23,600.00 | \$ 23,600.00 | |

| | | | |
|------------------------------------|---------------------------|----|----------|
| Company Name: | Alphanumeric Systems, Inc | | |
| RFP Checklist | | | |
| | YES | NO | Comments |
| Cover Letter | x | | |
| 3 Copies | x | | |
| Electronic Copy | x | | |
| Form 1 - RFP Acknowledgement | x | | |
| Form 2 - Addenda Receipt Ack | x | | |
| Form 3 - Proposal Submission | x | | |
| Form 4 - Pricing Worksheet | x | | |
| Form 5 - MWSBE Utilization | x | | |
| Form 6- Company Background | x | | |
| form 7- References | | | |
| Form 8- Additional Comp. Questions | | | |
| Form 9- Debarment Certification | | | |
| Form 10- Byrd Anti-Lobbying | | | |
| Execeptions | | | |
| Notes | | | |

| | | | |
|---|--------------|----|----------|
| Company Name: | Century Link | | |
| RFP Checklist | | | |
| | YES | NO | Comments |
| Cover Letter | x | | |
| 3 Copies | x | | |
| Electronic Copy | x | | |
| Form 1 - RFP Acknowledgement | | | |
| Form 2 - Addenda Receipt Ack | x | | |
| Form 3 - Proposal Submission | x | | |
| Form 4 - Pricing Worksheet | x | | |
| Form 5 - MWSBE Utilization | x | | MBE. WBE |
| Form 6- Company Background | x | | |
| form 7- References | x | | |
| Form 8- Additional Comp. Questions | x | | |
| Form 9- Debarment Certification | x | | |
| Form 10- Byrd Anti-Lobbying | x | | |
| Execeptions | x | | |
| Notes: Marked as confidential- Century would like to be notified prior to release | | | |

| | | | |
|------------------------------------|-------------|----|----------|
| Company Name: | Root9B, LLC | | |
| RFP Checklist | | | |
| | YES | NO | Comments |
| Cover Letter | x | | |
| 3 Copies | x | | |
| Electronic Copy | x | | |
| Form 1 - RFP Acknowledgement | x | | |
| Form 2 - Addenda Receipt Ack | x | | |
| Form 3 - Proposal Submission | x | | |
| Form 4 - Pricing Worksheet | x | | |
| Form 5 - MWSBE Utilization | x | | |
| Form 6- Company Background | x | | |
| form 7- References | x | | |
| Form 8- Additional Comp. Questions | x | | |
| Form 9- Debarment Certification | x | | |
| Form 10- Byrd Anti-Lobbying | x | | |
| Execeptions | | | |

| Alphanumeric | | | | | |
|--|---|---------|--|----------|--|
| Strengths | | Neutral | | Concerns | |
| Qualifications & Experience | | | | | |
| page # | | page # | | page # | |
| 6 | Tier 3 analyst are well trained and cert | | partnership between Alpha and Delta Six | 6 | Tier 1 analyst are not required to have s sec cert |
| 24 | Company has been around for 40 years | 24 | Recently started with public sector | | SOC analysts don't have a training plan |
| 26 | 10 successful public sector engagements | Q&A | Will comply with CJIS requirements | | |
| Project Approach/ Proposed Solution | | | | | |
| 8 | Encrypt data at rest and transit | | | 15 | Only perform maintenance on security equipment with onsite resource |
| 3 | SOC's within CONUS | | | 15 | No backup for system support |
| 5 | Simple to deploy SaaS solution | | | 8 | Two factor is SMS |
| 14 | Analytics platform provides searchable for 90 days/store 365 | | IR is responsibility of customer unless other agreement is reached | | |
| 5 | Proactive threat hunting, penetration testing and cyber training | | | | |
| 4 | Have dedicated analysts assigned to the Charlotte account and will recruit more resources as needed to ensure | | | | |
| Cost Effectiveness and Value | | | | | |
| | Offers the Alien Vault USMTM at no additional cost. | 21 | Higher end of Cost | | |
| MWSBE Subcontractor Utilization | | | | | |
| Acceptance to the Terms of the Contract | | | | | |
| | No Exceptions to the contract | | | | |
| Demonstration | | | | | |
| | Standards and procedures reviewed every 6 - 12 months. Monthly audit as part of SOC 2. | | Dependency on Virtual Analyst that is based on AI. | | Alphanumeric provides NOC (which seems to include some security system support) as professional services time and materials. Company does not show a remote support option for security systems support through third-party SOC. |

| Century Link | | | | |
|--|---|---------|---|--|
| Strengths | | Neutral | | Concerns |
| Qualifications & Experience | | | | |
| page # | | page # | | page # |
| 7 | 400 certified security team members | 1 | 45,000 employees | |
| 7 | SOC in Santa Clara, CA and St Louis, MO | 62 | In business for over 50 Years | |
| 8 | 100% of SOC staff have security certifications | 75 | State of South Carolina as a reference | Q&A Will not manage SentinelOne console directly |
| 62 | 500 State and Local government customers | Q&A | Will comply with CJIS requirements | Q&A Lack of detail regarding how threat intel is integrated into systems/processes |
| 1 | Company Has the Resources to Do the Job | | | |
| 4 | Experienced Staff | | | |
| Q&A | Has PCI DSS Report of Compliance (ROC) | | | |
| Project Approach/ Proposed Solution | | | | |
| 7 | 400K+ cyber-attacks halted each month | 9 | CenturyLink uses proprietary software | 4,5 Analytics platform is proprietary, which could limit our ability to integrate it with other platforms. |
| 9 | SOC analysts will follow escalation procedures | 4 | on-premise Log Collector Appliance | 5 Proposal appears to indicate that logs are only stored for 90 days. |
| 5 | Monitoring Portal has mobile application | 10 | CenturyLink will utilize MWSBE subcontractors for onsite services | 10 Lack of clarity about company's ability to take action to mitigate threats based on alerts |
| 7,8 | Recommends the use of Dynatrace which is the 2019 Gartner leader for Application Performance Monitoring | | | |
| 9 | Monitoring Portal has mobile application | 10 | CenturyLink proposes 15 Min IR notification | 26 Changes will not be performed by offsite personnel. |
| | | 11 | Use of the Adaptive Service Desk for APM, NOC and Reporting | |
| Cost Effectiveness and Value | | | | |
| | | | | \$350k-\$400k/year software license + \$50/mth monitoring for Application Performance Monitoring Cost of Noc Service on the higher end. |
| MWSBE Subcontractor Utilization | | | | |
| | | | | |
| Acceptance to the Terms of the Contract | | | | |
| | | | | Provided own Master Service Agreement to Use |
| Demonstration | | | | |
| | Role of Service Account Manager as a technical lead in support of other on-site resources. | | SIEM service based on compressed storage count of 25GB. | Company unable to complete the demonstration. Security System Support does not show a remote option included in pricing. |

| Root9b | | | | | |
|--|--|---------|--|----------|---|
| Strengths | | Neutral | | Concerns | |
| Qualifications & Experience | | | | | |
| page # | | page # | | page # | |
| 10 | Highest concentration of DOD master operators Strong development capabilities | Q&A | Will comply with CJIS requirements | Q&A | No required certifications for SOC analysts |
| Project Approach/ Proposed Solution | | | | | |
| 11 | Use Slack for out of band communication | | | | Lack of detail surrounding custom developed security tools. |
| 12 | The IR process was well defined and explained how they will respond | | | | |
| 14 | The data will stay in the USA. | | | | |
| 11 | The City will have access to their ticketing system | | | Q&A | Backup SOC takes four hours to activate |
| 11 | The ticketing system is available from mobile device. | | | Q&A | Lack of clarity about how Elastic Stack is configured to provide SIEM capabilities. |
| 14 | The City is familiar with the platform Elastic | | | | |
| 16 | They can provide vendor agnostic to any system | | | | |
| 16 | They support devsecops | | | | |
| 16 | Comply with the dedicated on-site staff. | | | | |
| 11 | They provide on-site quarterly business reviews and weekly calls. | | | | |
| | They Establish Virtual Private Network (VPN) (Internet Protocol Security [IPSec]) services for the personnel and/or services | | | | |
| Cost Effectiveness and Value | | | | | |
| | | | | | Pricing is on the higher end. |
| MWSBE Subcontractor Utilization | | | | | |
| | | | | | |
| Acceptance to the Terms of the Contract | | | | | |
| | No exceptions to the contract | | | | |
| Demonstration | | | | | |
| | Automation for routine security system tasks supported remotely and on-site. Excellent training program for their employees. Security Operations Automation includes large number of pre-defined playbooks. Security System support included in remote offering MSS and MDR. | | While clear on various other services within the SOC APC, company did not clarify which team or service area would be doing security system support. | | |

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 24th day of October 2019 (the "Effective Date"), by and between root9b, LLC, a limited liability company 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 root9b, LLC 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.

Acceptance: Refers to receipt and approval by the City of a Deliverable or Service in accordance with the acceptance process and criteria in the Contract.

Affiliates: Refers to all departments or units of the City and all other governmental units, boards, committees or municipalities for which the City processes data or performs services.

Biodegradable: Refers to the ability of an item to be decomposed by bacteria or other living organisms.

Charlotte Business Inclusion (CBI): Refers to the Charlotte Business Inclusion office of the City of Charlotte.

Charlotte Combined

- Statistical Area (CSA):* Refers to the consisting of the North Carolina counties of Anson, Cabarrus, Cleveland, Gaston, Iredell, Lincoln, Mecklenburg, Rowan, Stanly, and Union, and the South Carolina counties of Chester, Lancaster, and York; a criteria used by Charlotte Business INCLUSION to determine eligibility to participate in the program.
- City:* Refers to the City of Charlotte, North Carolina.
- City Project Manager:* Refers to a specified City employee representing the City's best interests in this Project.
- Company:* Refers to Root9b, LLC.
- Company Project Manager:* Refers to a specified Company employee representing the best interests of the Company for this Project.
- Contract:* Refers to a written agreement executed by the City and the Company for all or part of the Services.
- Deliverables:* Refers to all tasks, reports, information, designs, plans, and other items that the Company is required to deliver to the City in connection with the Contract.
- Department:* Refers to a department within the City of Charlotte.
- Documentation:* Refers to all written, electronic, or recorded works that describe the use, functions, features, or purpose of the Deliverables or Services or any component thereof, and which are provided to the City by the Company or its subcontractors, including without limitation all end user manuals, training manuals, guides, program listings, data models, flow charts, and logic diagrams.
- Environmentally Preferable Products:* Refers to products that have a lesser or reduced effect on human health and the environment when compared with competing products that serve the same purpose. This comparison may consider raw materials acquisition, production, manufacturing, packaging, distribution, reuse, operation, maintenance, or disposal of the product.
- Minority Business Enterprise/MBE:* Refers to a business enterprise that: (i) is certified by the State of North Carolina as a Historically Underutilized Business (HUB) within the meaning of N.C. Gen. Stat. § 143-128.4; (ii) is at least fifty-one percent (51%) owned by one or more persons who are members of one of the following groups: African American or Black, Hispanic, Asian, Native American or American Indian; and (iii) has significant business presence in the Charlotte Combined Statistical Area.
- MWSBE:* Refers to SBEs, MBEs and WBEs, collectively.
- MWSBE Goal:* If an RFP or Contract has separate Subcontracting Goals for MBEs, WBEs, and/or SBEs, the term MWSBE is a shorthand way to refer collectively to all MBE, WBE, and SBE Goals set for the RFP. In some instances, the City may set one combined goal for MBEs, WBEs, and/or SBEs, in which event the term MWSBE Goal refers to that one, combined goal. In the latter instance, calculated as a percentage, the MWSBE Goal represents the total dollars spent with MBEs, WBEs, and SBEs as a portion of the total Proposal amount, including any contingency.

- Post-Consumer Recycled Material:* Refers to material and by-products which have served their intended end-use by a consumer and have been recovered or diverted from solid waste. It does not include those materials and by-products generated from, and commonly reused within, an original manufacturing process.
- Project:* Refers to the City's need for a company to provide Managed Security Services for the City.
- Project Plan:* Refers to the detailed plan for delivery of the Services as described in Section 3, in the form accepted in writing by the City in accordance with the terms of this RFP and resultant Contract.
- Proposal:* Refers to the proposal submitted by a Company for the Services as outlined in this RFP.
- Recyclability:* Refers to products or materials that can be collected, separated or otherwise recovered from the solid waste stream for reuse, or used in the manufacture or assembly of another package or product, through an established recycling program. For products that are made of both recyclable and non-recyclable components, the recyclable claim should be adequately qualified to avoid consumer deception about which portions or components are recyclable.
- Recycled Material:* Refers to material and by-products which have been recovered or diverted from solid waste for the purpose of recycling. It does not include those materials and by-products generated from, and commonly reused within, an original manufacturing process.
- Services:* Refers to the Managed Security Services as requested in this RFP.
- Small Business Enterprise/SBE:* Refers to a business enterprise that is certified by the City of Charlotte under Part E of the CBI Policy as meeting all of the requirements for SBE certification.
- Specifications and Requirements:* Refers to all definitions, descriptions, requirements, criteria, warranties, and performance standards relating to the Deliverables and Services that are set forth or referenced in: (i) this RFP, including any addenda; (ii) the Documentation; and (iii) any functional and/or technical specifications that are published or provided by the Company or its licensors or suppliers from time to time with respect to all or any part of the Deliverables or Services.
- Subcontracting Goals:* Refers to the SBE, MBE, WBE, and MWSBE Goals established by the City for an RFP and resulting Contract.
- Trade Secrets:* 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. See N.C. Gen. Stat. § 66-152 et seq. 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.
- Women Business*

Enterprise (WBE): Refers to a business enterprise that: (i) is certified by the State of North Carolina as a Historically Underutilized Business (HUB) within the meaning of N.C. Gen. Stat. § 143-128.4; (ii) is at least fifty-one percent (51%) owned by one or more persons who are female; and (iii) has significant business presence in the Charlotte Combined Statistical Area.

Work Product: Refers to the Deliverables and all other programs, algorithms, reports, information, designs, plans and other items developed by the Company in connection with this Contract, and all partial, intermediate or preliminary versions of any of the foregoing.

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.

4. COMPENSATION.

- 4.1. TOTAL FEES AND CHARGES. The City agrees to pay the Company for the Services listed in Exhibit A at the rates shown in Exhibit A as full and complete consideration for the satisfactory performance of all the requirements of this Contract.
- 4.2. NO EXPENSES CHARGEABLE. 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.** The Company shall be responsible for keeping a record that accurately states the type of Service performed, and for time and materials services, the number of hours worked by the Company. 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.** 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.** The Company shall prepare and submit to the City 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.

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 two (2) consecutive one (1) year terms.
- 20.2. **TERMINATION FOR CONVENIENCE.** The City may terminate this Contract or any specific Service 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 or any specific Service 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 or the specific Service if the default is not cured within the specified period.

Notwithstanding anything contained herein to the contrary, upon termination of this Contract or any particular Service 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 or (ii) any designee of the City Manager.
 - 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 or a specific Service, 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 or specific Service, 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.

- 30. 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: |
|--|---|
| Tabatha Stimmel | Kay Elmore |
| Sr. Contracts Manager | City of Charlotte |
| root9B, LLC | City Procurement |
| 90 S. Cascade Avenue, Suite 800 | 600 East Fourth Street, 9 th Floor |
| Colorado Springs, CO 80903 | Charlotte, NC 28202 |
| Phone: 719-368-3698 | Phone: 704-336-2524 |
| Fax: N/A | Fax: 704-632-8252 |
| E-mail: contracts@root9b.com | 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: amjones@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 4.3 "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. **PCI COMPLIANCE.** Company acknowledges that the Services provided shall be within a Payment Card Industry Data Security Standards (PCI DSS) compliant environment. Company shall comply with and shall have a program to ensure Company's continued compliance, and its subcontractors' compliance, with the PCI DSS published by the PCI Security Standards Council, as the PCI DSS may be amended, supplemented, or replaced from time to time. Company shall report in writing to City, at a minimum annually, proof of such compliance with the PCI DSS. If Company becomes aware that Company or its subcontract is not, or will not likely be, in compliance with PCI DSS for any reason, Company will promptly report in writing to City the non-compliance or likely non-compliance and shall resolve such as soon as possible and in a manner acceptable to the City. The Company is responsible for the security of cardholder data the Company possesses or otherwise stores, processes or transmits on behalf of the City, or to the extent that Company could impact the security of the City's cardholder data environment.
- 31.21. **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.

ROOT9B, LLC

BY: [Signature]
(signature)

PRINT NAME: John Harbaugh

TITLE: Chief Operating Officer

DATE: October 16, 2019

CITY OF CHARLOTTE:
CITY MANAGER'S OFFICE

BY: [Signature: Sabrina Joy Hogg]
(signature)

PRINT NAME: Sabrina Joy Hogg

TITLE: Deputy City Manager

DATE: 10/28/19

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

BY: _____
(signature)

DATE: _____

This instrument has been preaudited in the manner required by the "Local Government Budget and Fiscal Control Act."

[Signature]
Finance Officer

[Signature: Dhawal Shah]
10/24/19

EXHIBIT A – PRICING SHEET

This Price Schedule is an Exhibit to and is incorporated into the Services Contract between the City of Charlotte and root9b, LLC (the “Contract”). Capitalized terms not defined in this Exhibit shall have the meanings assigned to such terms in the Contract.

The Company shall provide the Services listed below at the prices set forth below. The pricing indicated herein is all-inclusive and covers every aspect of the Services.

Line 1.0 (Security Operations Services) is the total monthly price for Services 1.1-1.8 in the chart below, if the City elects to purchase them all together. The City may at any time elect to purchase the services individually at the individual rates below in lieu of purchasing them as a bundle. Transition support services shall be provided at no additional cost.

| | | Year 1- Monthly Cost | Year 2- Monthly Cost | Year 3- Monthly Cost | Optional renewal year 1 Monthly Cost | Optional Renewal Year 2- Monthly Cost |
|--------------|--------------------------------------|---------------------------------|---------------------------------|---------------------------------|---|--|
| Total | Security Operations Services | \$65,214.03 | \$66,785.98 | \$68,396.53 | \$70,165.16 | \$71,981.51 |
| 1.1 | Core Security Operations Services | \$42,355.36 | \$43,414.25 | \$44,499.60 | \$45,612.09 | \$46,752.39 |
| 1.2 | *Analytics Platform Operations | \$11,060.04 | \$11,335.92 | \$11,619.36 | \$11,910.42 | \$12,208.02 |
| 1.3 | Email Threat Monitoring and Analysis | \$3,594.25 | \$3,656.65 | \$3,720.85 | \$3,841.24 | \$3,965.86 |
| 1.4 | Cyber Intelligence Support | \$5,007.80 | \$5,101.70 | \$5,198.00 | \$5,359.20 | \$5,526.23 |
| 1.5 | Security System Support | \$8,655.60 | \$8,872.20 | \$9,093.60 | \$9,321.00 | \$9,554.40 |
| 1.7 | Threat Hunting | \$4,327.80 | \$4,436.10 | \$4,546.80 | \$4,660.50 | \$4,777.20 |
| 1.8 | Compromise Assessment | \$1,273.22 | \$1,305.08 | \$1,337.68 | \$1,371.13 | \$1,405.43 |

*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 \$11,060.04

The following rates apply for additional work that may be needed under this scope:

| |
|--|
| Additional Hourly Labor Pricing |
| \$210.18 |

EXHIBIT B – SCOPE OF SERVICES**1.1. General Scope.**

The City of Charlotte requires Security Operations Services. Core required services include Security Operations Center (“SOC”), security event management, security event analysis, security incident response (“IR”) and management, analytics platform operations, email threat monitoring and analysis, security incident response and management.

1.2. Security Operations Services

The Company shall provide the following:

1. Transition Support
 - 1.1. Provide support for transition planning and transition plan execution associated with meeting agreed upon timeline for transition of Security Operations services from the incumbent contractor at no additional cost.
 - 1.2. Actively participate in the transition of Security Operations services from the incumbent contractor and develop a Security Operations Incoming Transition Plan that ensure that there is not degradation of Security Operations services during the transition at no additional cost.
 - 1.3. Develop and submit an Outgoing Transition Plan for transitioning work to a successor contractor or the City at no additional cost.
2. SOC Operations, Facilities, Personnel, and Communication
 - 2.1. The objectives of the SOC are to protect, detect, respond, and recover from cyber security threats to the City's enterprise and associated information systems.
 - 2.2. Provide a SOC, along with one or more secondary or backup SOCs in case of emergency, located within the continental United States. A tour of SOC facilities shall be provided upon request by the City.
 - 2.3. SOC services must be available 24 hours a day, seven days a week.
 - 2.4. The SOC must be staffed with personnel who have the required educational background and experience to meet the requirements of this SOW.
 - 2.5. Provide a Senior Security Engineer who will be available to consult on security matters and direct SOC actions based on the City's cyber security needs.
 - 2.6. Ability to comply with the current and future requirements of the Criminal Justice Information Services (“CJIS”) Security Policy including but not limited to mandatory background checks and training.
 - 2.7. Notify the City of onboarding and offboarding personnel to the City's account.
 - 2.8. A weekly conference call will be hosted by the Company to review the current state of Security Operations services. This call must include sufficient technical representation from the Company to discuss the details of security issues being worked, as well as sufficient management representation to execute corrective actions when necessary.
3. Systems Access
 - 3.1. Access to City information systems will be provided on a least-privilege basis. The Company will document and propose a tiered, role-based access management procedure for Security Operations personnel which takes into account the education, certification, and experience of the individual and provides the City an opportunity to review and approve/reject applications for access.
 - 3.2. The City reserves the right to interview personnel prior to granting elevated access to City information systems. If personnel are determined to be unqualified for elevated access, such access will be denied.
4. Reporting
 - 4.1. On a monthly, annual, and ad hoc basis, provide reporting on key performance indicators (“KPI”) and other metrics related to the City's information security

- posture. The requirements for these reports will vary, but monthly and annual reports are required.
- 4.2. These reports must also provide graphs comparing current metrics against previous months to identify trends in the direction of the City's information security landscape.
 - 4.3. Ad hoc reporting on indicators of attack such as Internet Protocol ("IP") addresses, hashes, etc., from information security system logs/events will be required to comply with federal and regulatory reporting requirements. Ad hoc reports must be provided within three business days of request.
5. Security Event Management and Communication
- 5.1. A centralized, secure method to track and communicate information and data related to security events must be provided to allow authorized City personnel to view information relating to ongoing and resolved security events. This may take the form of an incident management platform, a ticketing system, or some other system for tracking these events.
 - 5.2. This system must be secure, encrypted, authenticated, and allow for access by authorized City employees from their mobile devices.
 - 5.3. Encryption must be in place both at rest and in transit and must use the latest standards required by the City. The City's current standards are AES-256 at rest and TLS 1.2 in transit.
 - 5.4. The system must protect the City's data from access by unauthorized individuals, especially via segmentation from other customer data.
 - 5.5. The system must record, at a minimum, the following information below about each event in separate fields for reporting and trend analysis.
 - Event summary
 - Severity
 - Event date and time, including time zone (in UTC)
 - SOC point of contact
 - Current status
 - Attack vector
 - Indicators of attack (raw logs, hashes, file names, registry entries, etc.)
 - 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
 - Operating System, including version
 - Endpoint protection software versions
 - Impacted department
 - Identification method
 - References
 - Resolution
 - 5.6. Messaging communications regarding security events between the SOC and the City must take place over secure, encrypted methods. Such communication methods must be approved by the City prior to implementation or use.
6. Security Event Analysis
- 6.1. Review all security device data feeds, analytical systems, sensor platforms, output from other information security systems. This may be performed via an analytics platform.

- 6.2. If the analytics platform is not capable of properly ingesting, parsing, and indexing the output of a given security system, that system must be reviewed directly.
 - 6.3. Analyze and investigate any information security events that would pose a threat to the City's information systems.
 - 6.4. The analysis process will differ by event type, so procedures or playbooks should be developed by the SOC and approved by the City for each type of event.
 - 6.5. In addition to reviewing other events and logs from City information systems, analysis processes should include thorough searches of both open source and closed source intelligence sources, monitoring of possible attacker communication channels, sandboxing, manual malware analysis and any other tasks useful to enriching the context of the event.
 - 6.6. As events are analyzed and determined to be false positives, propose security system configuration changes to the City to tune out those events. Tuning of the analytics platform may also be performed on confirmed false positives.
 - 6.7. Any security event which, after analysis and investigation, is determined to be malicious and poses a threat to the security of the City's information systems would enter the Security IR process as further defined in Section 7 and shall follow the timeline for notification per the SLA.
7. Security IR
- Once a security event is identified as a threat to the City's information systems, that event must be tracked, managed, communicated about, and responded to by the SOC through all phases of the IR process. The City's incident response process consists of the following phases.
- 7.1. Preparation
 - 7.1.1. The SOC will be responsible for supporting and assisting the City in the development and maintenance of the City's overall IR capability. The SOC will also assist the City in ensuring that systems, networks, and applications are sufficiently secure.
 - 7.2. Identification
 - 7.2.1. This phase will be the primary focus of the SOC during typical daily operations. This will include the Security and Event Analysis, Email Threat Monitoring and Analysis, Threat Hunting, Cyber Intelligence Support as well as additional operations to enrich and further investigate events to provide clarity regarding the nature of a given event and its possible or actual impact on the City's information systems.
 - 7.2.2. Identification and validation of a possible threat should include investigation into the configuration of affected systems. This may include performing vulnerability assessments of affected systems such as port scanning, service and software identification, and configuration review. Port/vulnerability scanning will only be performed with the explicit approval of the City.
 - 7.3. Containment
 - 7.3.1. The SOC will make containment strategy recommendations to the City based on the knowledge gathered during the Identification phase. Recommendations should consider the potential damage to and theft of resources, need for evidence collection/preservation, potential impact to service availability, time and resources required to implement, effectiveness, and duration.
 - 7.3.2. In addition to making containment strategy recommendations, once a strategy is approved, the SOC may be responsible for executing all or part

of the strategy by making configuration changes to City information security systems.

7.4. Eradication

7.4.1. The SOC will make eradication strategy recommendations to the City based on the knowledge gathered during the Identification and Containment phases.

7.4.2. In addition to making eradication strategy recommendations, once a strategy is approved, the SOC may be responsible for executing all or part of the strategy by making configuration changes to City information security systems.

7.5. Recovery

7.5.1. The SOC will monitor recovery from information security incidents and provide status updates as the City brings affected systems back online.

7.6. Lessons Learned

7.6.1. The SOC will recommend changes to City policy, process, or technology to prevent or more quickly detect similar incidents in the future. Depending on the scope of the incident, the SOC may need to participate in a root cause or lessons learned meeting to provide information about the incident from their perspective.

8. Changes to Information Security Systems

8.1. Any changes to City information security systems must be approved by the City prior to the change taking place. Depending on the nature of the change, and at the City's discretion, the SOC may need to use the City's Change Management process to make the change.

8.2. Information security systems in which the SOC may be required to make configuration changes to secure the City's information systems are in the Current Environment section.

8.3. Capacity to make security-related changes (blacklist hash, block IP, tune Intrusion Detection Prevention Systems, etc.) to these systems must be available 24 hours a day, seven days a week. All such security-related changes will be made in accordance with the City's Change Management process.

9. Analytics Platform Operations

9.1. Provide a hosted or cloud-based security analytics platform (or security information and event management ["SIEM"]) system to ingest, parse, index, categorize, correlate, visualize, and alert on security logs.

9.2. This analytics platform must be hosted within the continental United States only.

9.3. The analytics platform must parse and index logs from all City information security systems and make those logs hot searchable for no less than 15 days.

9.4. All logs ingested by the analytics platform must be retained in their raw log format for a minimum of 365 days.

9.5. Current log volume is provided in the Current Environment section below. The analytics platform should have the ability to scale up as the City's volume increases.

9.6. Provide a secure, encrypted method for transmitting logs from the City's information security systems to the analytics platform.

9.7. Support for newly onboarded information security systems must be provided in a timely manner, with new log sources being added including parsing and indexing set up within 30 calendar days.

- 9.8. Notify the City via email of a silent or unavailable log source within 2 hours of the source's threshold being reached. Thresholds for silent log sources will be established on an individual basis.
- 9.9. There are some security events/logs within the City's environment that must be monitored directly by City personnel. To facilitate this, the analytics platform must have the capability to alert the City immediately via email, or other messaging methods approved by the City, based on custom search parameters.
- 9.10. Creation of custom alerts should be provided within 24 hours of request.
- 9.11. Provide training regarding how to conduct investigations and analysis in the analytics platform to up to 14 City personnel.
- 9.12. The analytics platform must provide for authentication via the City's on-prem Active Directory ("AD") or Security Assertion Markup Language ("SAML") via AD Federation Services ("AD FS").
- 9.13. Provide management, maintenance, and technical support for the analytics platform, with response to support issues provided within 24 hours of an issue being reported.
- 9.14. Must have at least two years of experience implementing similar solutions.
- 10. Email Threat Monitoring and Analysis
 - 10.1. Provide an email address to which suspected malicious emails may be sent by the City. Emails sent to this address must be analyzed with the same frequency and urgency as other security data feeds.
 - 10.2. Any email which, during analysis and investigation, is determined to be malicious and may pose a threat to the security of the City's information systems would be considered a security incident and enter the IR process.
- 11. Cyber Intelligence Support
 - 11.1. In support of Security Operations and the City's efforts to secure its information systems, provide analysis of cyber intelligence. Gather, ingest, and review cyber news feeds, signature updates, incident reports, threat briefs, and vulnerability alerts from external sources and determine their applicability to the City's environment.
 - 11.2. Interpret and compile the information received about emerging threats through data feeds from Internet security firms, Government organizations, and private industry into actionable monitoring either by developing custom content or by some other means.
 - 11.3. Analyze threat information, determine the risk to the City's environment, and develop mitigations and/or countermeasures.
 - 11.4. Provide situational awareness to the City through regular threat briefs and vulnerability alerts, communicate methods for detecting activities of specific threats, and plan operations to mitigate or disrupt the threat as part of the City's information security program.
 - 11.5. At the City's request, gather, analyze, and report on intelligence regarding specified risks to the City's information systems. Preliminary reports should be provided within 12 hours of request, with Final report provided within a reasonable timeframe mutually agreed to by the Parties.
- 12. Security System Support
 - 12.1. The Company will be responsible for the management, administration, and operation of any systems provisioned by the Company, even systems provisioned on City infrastructure.
 - 12.2. Additionally, the Company will be required to provide support for the systems listed in the Security System Changes section below. The Company will be responsible for supporting the City in routine maintenance, administration, and

operation of these systems as defined in 12.3 below. Management and administration of security systems shall include responding to, investigating, and correcting the root cause of system alerts generated by the security system itself or a separate monitoring system.

12.3. Support for all security appliances by completing policy tuning, auditing, moves, adds, or changes (“MAC”).

12.3.1. Layer 7 firewall support to include:

- 12.3.1.1. OS monitoring for common vulnerability exposures (“CVE”) with associated upgrades and patching.
- 12.3.1.2. Firewall policy MACs.
- 12.3.1.3. Ongoing IPS tuning based on CVE notices by threat intelligence providers when applicable to the City’s environment.
- 12.3.1.4. Anti-virus, anti-bot, and other threat blade tuning as needed to include exceptions and evaluation of false positives.
- 12.3.1.5. Content awareness and data loss prevention policy updates and tuning.
- 12.3.1.6. Virtual private networking (“VPN”) IPsec tunnel support as needed.
- 12.3.1.7. VPN client support as needed.
- 12.3.1.8. Coordinating with vendor support to prepare for custom signature creation in the event of a security incident.
- 12.3.1.9. Coordination with vendor support to solve software bugs, address incidents, and resolve problems.

12.3.2. Load balancer support for Local Traffic Manager (“LTM”), Application Security Manager (ASM), and Application Performance Manager (“APM”) configuration, to include:

- 12.3.2.1. OS monitoring for CVE with associated upgrades and patching.
- 12.3.2.2. Virtual IP (VIP) configuration, discrete node and service health monitoring, iRule configuration, iApp deployments, and web application firewall setup and tuning.
- 12.3.2.3. ASM updates, staging, and tuning for all VIPs.
- 12.3.2.4. APM web portal VPN support to include portal apps, single-sign on configuration, policy editing for access management.
- 12.3.2.5. Coordinating with vendor support to prepare for custom iRules in the event of a security incident.
- 12.3.2.6. Coordination with vendor support to solve software bugs, address incidents, and resolve problems.

12.3.3. Distributed Denial of Service (“DDoS”) protection appliance support to include:

- 12.3.3.1. OS monitoring for CVE with associated upgrades and patching.
- 12.3.3.2. Blacklisting of habitual offenders.
- 12.3.3.3. Coordinating with vendor support to prepare for custom signature creation in the event of a security incident.
- 12.3.3.4. Coordination with vendor support to solve software bugs, address incidents, and resolve problems.

12.3.4. Automation of routine processes and tasks on security appliances.

- 12.3.4.1. Assist City InfoSec as needed in the automation of routine security tasks related to the load balancing LTM, firewall demilitarization zone (“DMZ”) creation, firewall policy rule updates and installation, and DDoS blacklisting.

- 12.3.4.2. The automation of these components will be made through an automation platform such as Ansible or Tufin.
- 12.3.4.3. Ensure the monitoring of automation processes to report failures and successful implementations.

13. Threat Hunting

- 13.1. Provide advanced analysis and threat hunting support to security operations to proactively uncover evidence of adversary presence on City networks.
- 13.2. Focus on threat detection, geared toward attacks that have bypassed existing security controls.
- 13.3. Develop hunt use cases or playbooks to look for specific tactics, techniques, and procedures (“TTPs”) that indicate a threat is active in the City’s environment.
- 13.4. Use information and threat intelligence related to the City’s information systems to identify undiscovered attacks.
- 13.5. Investigate and analyze all relevant sensor data (network, endpoint, logs, etc.), reporting on any findings and making recommendations to improve hunt operations.
- 13.6. Provide recommendations on security architecture, instrumentation, and controls to make the City’s information systems more resilient.

14. Compromise Assessment

- 14.1. Provide, annually, an 80-hour engagement of dedicated compromise assessment services to evaluate the City for signs of successful intrusion or exfiltration of data.
- 14.2. This engagement must include not only analysis of information systems owned by the City, but also a search for indications that the City’s data has been compromised and/or is being sold or shared online.
- 14.3. Provide full briefing to technical and management teams on findings and impact of any discovered compromise, including actionable guidance on next steps to respond to and eradicate any threats.

1.3. Current Environment

1. Security System Changes

The table below details the security systems on which the SOC will perform changes, including the number of devices and the types of changes the SOC will need the capacity to execute.

| Quantity | Type | Changes/Actions Required by SOC |
|-----------------|--|--|
| 1 | SentinelOne Management Console | Blacklist hash, whitelist hash, resolve events, disconnect system from network |
| 1 | Carbon Black Cb Response Management Console | Blacklist hash, create watchlist, tune watchlist |
| 2 | Palo Alto and Checkpoint Firewall Management Servers (in HA) – IPS, Anti-Bot, Anti-Virus, Threat Emulation (24 Clusters) | Policy MACs, IPS/Threat signature tuning, block bad IP/Host/Country, OS updates as needed. |
| 35 | Palo Alto and Checkpoint Small Appliances | Policy MACs, appliance configuration and tuning, OS updates as needed. |
| 8 | F5 ASM/LTM/APM | ASM Policy MAC and signature tuning, LTM VIP MAC, APM and |

| | | |
|---|-------------------------|---|
| | | SSO updates, iRule creation, OS updates as needed |
| 2 | Radware DDoS Appliances | Block bad IP/Host/Country, OS updates as needed. |

2. Systems Sending Logs to Analytics Platform

The following systems will send logs to the analytics platform.

| Quantity | System |
|------------------------------|--|
| 24 clusters 35 standalone | Checkpoint firewalls (firewall, IPS, Anti-Bot, Anti-Virus, Threat Emulation) (via management server) |
| 3 clusters 3 standalone | Palo Alto firewalls (firewall, IPS, threat) (via management server) |
| 1 cluster | Radware DDoS |
| 45 | Active Directory Domain Controllers (security logs only) |
| 2 | Adaxes servers |
| 1 | Airwatch MDM server |
| 2 | Apache web servers |
| 3 | Bind DNS servers |
| 2 | Cb Response servers |
| 3 | Cisco ACS |
| 1 | Cisco ASA |
| 3 | Cisco Router |
| 3 clusters | F5 BIG-IP LTM, ASM, APM |
| 4 | Netmotion VPN |
| 1 | RedHat Syslog |
| 3 | Radware DefensePro |
| 1 | SentinelOne server (CEF) |
| 3 - 5 | Tufin servers |
| 1 cluster | SonicWALL |
| 14 | Windows file servers |
| 1 | Web server |
| 2 | RADIUS servers |
| 1 | Certificate Authority |

3. Total Log Volume

The current log volume that will need to be processed by the analytics platform is as follows:

- 7,000 events per second (“EPS”)

- 200 gigabytes (“GB”) per day (average, raw log volume)

1.4. Service Level Agreement

- The Company must notify the City of suspected security incidents in accordance with the tables below.
- Metrics will be reported on monthly by the Company for tracking and adherence to SLAs.

| PRIORITY | SEVERITY | DEFINITION | RESPONSE TIME AND ACTIONS | NOTIFICATION TO CITY WITHIN (upon recognition as an incident) |
|----------|-----------------------------------|---|--|---|
| 1 | Critical | Confirmed Compromise, Unauthorized Access, or failure of a critical security device or service. Likelihood that the event could stop operations, cause significant business/financial loss, or negatively affect the client brand. | ≤ 15 Minutes; Client phone call until answered, follow-up with email | 5 minutes |
| 2 | High | Urgent Threat, Denial of Service or issue regarding security device or service. Likelihood that the event could interrupt operations, cause some business/financial loss, or negatively affect the client brand. | ≤ 30 Minutes; Client phone call/voicemail, follow-up with email | 30 minutes |
| 3 | Moderate | An isolated event that could negatively affect the functions of the serviced device. There is no immediate negative effect on day-to-day business operations. Could cause isolated interruption to operations or could be a chained progression of malicious activities to perform more disruptive attacks. | ≤ 2 Hours; Email to Client | 60 minutes |
| 4 | Low | A benign event, but should be addressed in future remediation planning. There is no immediate negative effect on day-to-day business operations. | ≤ 4 Hours; Reported in appropriate report | 24 hours |
| 5 | Informative | Scans/Probes/Attempted Access which existing rules prevented compromise. This event does not pose an immediate risk of damage to the client, but should be noted for inclusion in remediation planning and best practices for security. | ≤ 24 Hours; Reported in appropriate report | n/a |
| 6 | Investigation / Off-Line Analysis | Events generated due to Incident Response Investigative activities, during the first phase of a new system deployment, or major changes in the network. | Reported in separate Incident Response Recommendations Report | n/a |

Company must notify the City of suspected security incidents in accordance with the City’s change management process and the table below.

| Type Change | R9B Change Submission | Completion of Change | Definition |
|-------------|--|--|---|
| Emergency | Within 2 hours of confirmation of need for change | As soon as possible | Related to high or critical Incident. Requires approval from City Service Area Manager “SAM”; |
| Normal | Within 48 hours of confirmation of need for change | Per change model and release plan; scheduled 5-days prior to implementation | Non-urgent, requires approval from City Change Advisory Board “CAB” |
| Standard | Within 12 hours of confirmation of need for change | Per change model for City standard change; City SAM approval to execute change | Non-urgent, follows established path, City CAB pre-authorized |
| Expedited | Within 4 hours of confirmation of need for change | As soon as possible | Requires City SAM and special CAB approval; too urgent for normal or standard change |

EXHIBIT C – FEDERAL CONTRACT TERMS AND CONDITIONS

This Exhibit is attached and incorporated into the Agreement to Provide Managed Security Services (the "Contract") between the City of Charlotte and root9b, LLC (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 9 – Vendor Debarment Certification is incorporated herein as Form C.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 10 –Byrd Anti-Lobbying Certification is incorporated herein as Form C.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.

Form- C.1 Vendor Debarment Certification

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.

X 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

Form C.2 Byrd Anti-Lobbying Certification

City of Charlotte Managed Security Services
269-2019-109
Form 10



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

[Signature]
Authorized Signature

07/11/19
Date

root9B, LLC (R9B)
Company Name

90 S. Cascade, Suite 800
Address

Colorado Springs, CO 80903
City/State/Zip