Public Records Request #3017

The following materials have been gathered in response to public records request #3017. These materials include:

- RFP #269-2017-042, Security Audit and Assessment Services – root9B Response

This information was provided as a response to a public records request on 11/9/19 and is current to that date. There is a possibility of more current information and/or documents related to the stated subject matter.

Further Information

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

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

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

City of Charlotte

SECURITY AUDIT AND ASSESSMENT SERVICES

PROPOSAL

RFP Number: 269-2017-042
12 April 2017

CONFIDENTIAL INFORMATION ENCLOSED

This proposal includes data that shall not be disclosed outside the client and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offer or as a result of – or in connection with – the submission of this data, the client will have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. The data subject to this restriction are contained in the following sheets of this proposal. © 2017 root9B, LLC.
Prepared by root9B for the specified client. Portions of this document and the templates used in its production are the property of root9B, and cannot be copied without permission. While precautions have been taken in the preparation of this document, root9B, the publisher, and the author(s) assume no responsibility for errors, omission, or for damages resulting from the use of the information contained herein. Use of root9B services does not guarantee the security of a system, or that computer intrusions will not occur.

Intentionally Left Blank

R9B

root9B
102 N. CASCADE AVENUE | SUITE 220
COLORADO SPRINGS | COLORADO | 80903
PHONE 330-4653

12 April 2017

Mr. Shaunne Thomas
Management and Financial Services
Charlotte-Mecklenburg Government Center (CMGC)
600 East Fourth Street
Charlotte, NC 28202

Dear Mr. Shaunne Thomas,

root9B, a small business with a local presence in Charlotte, is pleased to present our proposal for providing a comprehensive Security Audit and Assessment Service for the City of Charlotte ("City"). The attached Technical Proposal outlines how root9B's Attack Surface Baseline (ASB) will provide value-added benefits beyond traditional penetration testing and vulnerability assessments (PenTesting). Our approach and the results of our ASB differs significantly from those offered by other companies. root9B believes that a cyber defense protocol of active, Manned Information Security, informed by relevant and specific threat intelligence, is necessary to halt the adversary's current freedom of maneuver in the defender's networks. Our application of advanced tools and cyber defensive tradecraft empowers network defense teams to expose and predict network attack vectors that currently go undetected by purely automated and passive security technologies. We ensure our assessments are germane by combining an understanding of your unique Business Context, a "*Think like an Adversary*" mindset, and a City of Charlotte-tailored Threat Intelligence baseline to filter threats and vulnerabilities that may be irrelevant while focusing on those threat vectors most likely to impact the City's network integrity.

A further differentiator is that we apply adversary Tactics, Techniques, and Procedures (TTP) to attempt to penetrate, infiltrate, and exploit your cyber defenses in the same manner as a malicious actor would. Our Cybersecurity analysts apply a unique assessment approach that centers on viewing your enterprise through the lens of an advanced cyber adversary to focus on likely threats vectors to your operations. Our assessments incorporate risk, probability of exploitation, and potential business impact. This allows us to deliver a comprehensive evaluation of how the City's defensive stance stacks up against real world adversaries that our tailored threat intelligence has identified as the most likely threat vectors that the City is likely to face.

When these contextual and threat focused assessments are integrated with our cyber defense exploitation methodology, and a City of Charlotte-specific vulnerability assessment, root9B will be able effectively identify and aggregate pertinent vulnerabilities, enumerate the adversary attack surface, identify and prioritize exploitation risk and impact, and provide actionable remediation recommendations. Our services will broadly address the spectrum of network and system level testing and assessments across the requested domains of:

1. Payment Card Industry ("PCI") Data Security Standard ("DSS") Compliance Assessment;
2. Internal and External Penetration Test;
3. Web Application Penetration Test;
4. Wireless Security Assessment;

5. Microsoft Group Policy Security Assessment;
6. Microsoft Active Directory ("AD") Security Assessment;
7. Domain Name System ("DNS") Security Configuration Audit; and
8. Server Security Configuration Audit.

To supplement our capabilities, root9B is joining forces with one of the industry's best-of-breed audit and regulatory compliance specialists and another small business; NDB Accountants & Consultants, LLP (NDB). NDB will be charged with providing the specialized PCI Qualified Security Assessor (QSA) services. With years of knowledge and insight into the regulatory compliance arena, root9B selected NDB for the PCI portion of this engagement since they have has developed what many industry experts consider to be industry best-of-breed audit methodologies.

In summary, root9B proposes to apply a City of Charlotte-specific Business Context, tailored Threat Intelligence, a "Think Like the Adversary" mindset, along with specialized PCI QSA services to effectively assess the City's vulnerability to cyber threats. We will work with City leadership to develop a customer-focused program that is customized and scaled to your specific requirements without compromise to a basic tenet: identifying and protecting the most critical elements of the City of Charlotte's ecosystem (infrastructure, financial/PCI, proprietary, personally identifiable information (PII), and branding data) from the range of cyber threats. The resulting assessment will provide the foundation for an enduring, effective yet sustainable cyber barrier to the cyber menace.

Per the instructions in the Request For Proposal (RFP), root9B accepts the **RFP Section 3.8 Representations and Warranties** and attests to the accuracy of the information provided in this proposal.

If you have any questions, please contact:

John Harbaugh
Chief Operating Officer, root9B
Direct: 443-758-0538
E-mail: john.harbaugh@root9b.com
Colorado Springs Office: 102 N. Cascade Ave Suite 220 Colorado Springs CO 80903
Colorado Springs | San Antonio | Manhattan | San Diego | Boise | Honolulu

PROPOSED SOLUTION

This Page Intentionally Left Blank

TABLE OF CONTENTS

01 INTRODUCTION

root9B, a longtime member of the City of Charlotte's small business community, welcomes the opportunity to assist City of Charlotte ("City") conduct comprehensive Vulnerability Assessment and Penetration Testing of the City's network, systems, and applications as well as support mandated annual Payment Card Industry (PCI) reporting requirements.

We refer to our Cybersecurity Penetration Testing (PenTesting) and Vulnerability Assessment Program as an Attack Surface Baseline (ASB). Our ASB approach exceeds traditional PenTest engagements in several ways. We do this by addressing the expected technical, functional, and threat-driven aspects of a client's enterprise while also applying client-specific Business Context, tailored Threat Intelligence, and an aggressive adversarial mindset to enhance the assessment. The result is a comprehensive appraisal of the real-world vulnerabilities and threat exposure that the City is likely to face. By incorporating City of Charlotte-specific threat vectors, risk, probability of exploitation, and potential business impact we are able to view the enterprise through the lens of likely cyber adversaries. Observing and evaluating your enterprise from the attacker's perspective offers the benefit of analyzing City of Charlotte's defensive strengths and weaknesses relative to attacker capability vs. a "phonebook listing" of all possible risks. Furthermore, this allows us to make actionable recommendations that will help City of Charlotte apply corrective actions and resources where they will be most effective.

A key component of our ASB offering includes the PenTesting and Assessment activities that City of Charlotte needs to meet its Payment Card Industry Data Security Standard (PCI DSS) requirements. Employing a small business industry leader, NDB Accounting, our PCI assessment will focus on identifying exploitable vulnerabilities that may circumvent or defeat the Cardholder Data Environment (CDE) security features employed by City of Charlotte.

01.1 Engagement Objectives

The objectives of this effort are to accurately assess the City of Charlotte's overall network vulnerability while also addressing annual PCI compliance mandates. Both objectives are readily accomplished by conducting assessments that provide objective data on the robustness of City of Charlotte's network perimeter, or attack surface. Additionally, we will provide expert enhancement, mitigation, and remediation recommendations that your team can use immediately to improve the City's security posture.

Specific advantages of the root9B ASB include:

- Enhanced Vulnerability Assessment and PenTesting that includes Business Context, tailored Threat Intelligence, and a "*Think Like the Adversary*" mindset.
- PCI Compliance reporting that covers all PCI DSS mandated topics and is structured and formatted for easy integration with City of Charlotte's Annual PCI Assessment. By extension, root9B ASB results will

provide a fuller understanding of the threat needed to help City of Charlotte protect payment data before, during and after a payment or purchase.

- Verifying the perimeter security controls, identifying weaknesses and making recommendations strengthen City of Charlotte Cardholder Data Environment (CDE) security.
- Threat Intelligence-based determinations as to whether and how priority threat actors identified by root9B analysts can gain unauthorized access to City of Charlotte assets, associated networks and systems affecting cardholder data, system files, logs and other critical records.
- Customized, detailed, actionable environment safeguarding and remediation recommendations to strengthen the security level of the City of Charlotte's infrastructure (vs a 'data dump')
- All ASB activities will be performed by Department of Defense (DoD) and National Security Agency (NSA) trained cyber operators backed by national cyber Subject Matter Experts (SME).
- Manual analysis of vulnerabilities to eliminate false positives.
- Customer-focused flexibility, agility, and unbureaucratic management that only a small business can offer.

In summary, root9B's testing, analysis, and remediation recommendations will tangibly enhance the City's network and data sovereignty.

01.2 What Sets an Attack Surface Baseline (ASB) Apart

Every Information Technology (IT) enterprise, regardless of the precautions taken, is at risk. Misconfigurations, inherent system vulnerabilities, or malicious operations by way of an otherwise authenticated and authorized access point provide a multitude of avenues that an attacker can exploit. Helping Client's understand their exposure to potential attacks provides ample motivation and incentive for conducting Vulnerability Assessment and Penetration Testing (PenTesting). However, while many vendors offer PenTesting, the value of these operations is dependent upon considerations that go beyond a rote checklist and an automated scan of the network. The key to achieving a balanced, effective, and sustainable cyber defense requires a deeper understanding of the concept of the Attack Surface, creating the need to objectively assess the organization's vulnerabilities relative to its threat exposure. Achieving this understanding creates the foundation for achieving meaningful cybersecurity situational awareness and is the basis for root9B's Attack Surface Baseline (ASB).

Conceptually, the Attack Surface encompasses all available points of access and method of interaction with the outside world. Each access point along the network boundary presents varying degrees of risk; some of which are not technical in nature (e.g. Social Engineering). Another consideration is that your enterprise or IT ecosystem may not be the attacker's actual objective but instead, your enterprise may be used as gateway into other systems. Collectively, your risk is a function of the vulnerability of each component in your corporate ecosystem, the motivation for exploitation that your organization presents to an attacker, and the Tools, Techniques and Procedures (TTP) that an attacker is able to deploy to take advantage of your vulnerabilities.

Through our heritage in the US intelligence community we recognize that a checklist approach to Vulnerability Assessments and Penetration Tests that generates reams of raw data spewed from automated scans has little actionable value. Instead we ensure our assessments are germane by combining an understanding of Client-specific Business Context, our "*Think like an Adversary*" mindset, and a Client-specific Threat Intelligence baseline to filter threats and vulnerabilities that may be irrelevant. root9B Cybersecurity analysts apply a unique assessment approach that centers on viewing your enterprise through the lens of an advanced cyber adversary to focus on a likely threats vectors to your operations. Our assessments incorporate risk, probability of exploitation, and potential business impact. Finally, root9B's Attack Surface Baseline produces actionable reporting and readily applicable recommendations. This results in fact-based assessment of the relevant vulnerabilities and most likely threat vectors the City of Charlotte currently faces.

01.2.1 Client-Focused Business Context

All root9B's services invest in developing an awareness of the client's critical Business Context. This allows us to define the ecosystem that the security program is designed to protect. Through this process, we also develop insights into the client's environment, identify critical assets, and, learn what is normal, or what is not. By starting with the business-critical components, root9B focuses on validating the security posture of the systems that truly matter to the City of Charlotte and branch out to other components over time. root9B believes our emphasis on Business Context in the execution of an Attack Surface Baseline assessment is both critical and unique.

Key elements of root9B's Business Context are listed in the following table.

Business Context	Sample Assessment Categories
• What assets need to be protected	• Critical data, key users, applications, systems, networks
• Why do these assets need to be protected	• Revenue sustainment, brand impact, regulatory requirements, proprietary intellectual property
• How are these transactions identified	• Data fingerprints, business roles, access credentials
• Who is involved in these transactions	• Business groups, customers, administrators, vendors
• Where do these transactions occur	• Applications, systems, networks
• When do these transactions occur	• Busy season, product launch, acquisition

01.2.2 Tailored Threat Intelligence

The term "threat intelligence" is often misused and misrepresented for impact. Simple bulk propagation of threat data that has been identified and published on the internet is not threat intelligence. root9B's proactive approach to cyber threat intelligence begins with a risk assessment tailored to address the client's own Business Context and designed to identify the unique security vulnerabilities and threat profiles they face. Our approach applies a dedicated Threat Intelligence Team that is proactive and seeks to identify emerging and targeted threats pre-exploitation. Our cyber analysts will:

- Establish a baseline understanding of the City's threat exposure to identify likely threat actors, vectors and objectives specific to them.
- Develop threat profiles (e.g. nation-state sponsored threats, criminal elements, politically motivated, hacktivists, curious student, disgruntled employees) to identify threat actor motivations.
- Evaluate threat actor sophistication, capabilities, unique threat signatures, and recent or current tactics. We focus on the human behind the attack and the methodologies (aka Tactics, Techniques, and Procedures [TTP]) that they employ.

The result is truly actionable threat knowledge that City of Charlotte security professionals can use to defend against emergent threats before a breach takes place.

01.2.3 "*Think Like the Adversary*" Mindset

When conducting any cyber operation, root9B employs a "*Think like the Adversary*" mentality that considers an adversary's core motives, capability, and approach. This methodology embraces and recognizes that the greatest threat to any network is the sophisticated, Advanced Persistent Threat (APT) whose refined techniques shred standard automated cybersecurity solutions. Whereas traditional automated cybersecurity solutions are valuable and exceedingly necessary, they are incomplete, especially when pitted against a patient, well-resourced APT. These elite cyber actors find and exploit the gaps in defenses that rely solely on automated / passive tools. Firewalls, security sensors, telemetry tools, and post-incident response protocols are no match for them. As the cyber attacker adapts in real- or near real-time to the tools, techniques, and procedures employed by static defensive measures, the attacker will always prevail. It is inevitable that a malicious actor will eventually be successful if not countered in kind by a smart defender who assumes compromise and conducts an adaptive, defensive response.

To counter the thinking, adaptive manned threat, root9B employs a unique, active manned Intelligence feature that engages a live person to analyze and recognize intrusion vulnerabilities that are otherwise missed by automated systems. Cultivated and refined by real-world operations, this approach is proven and highly effective in both the Intelligence and Commercial sectors. Everything root9B does applies this "*Think like the Adversary*" active man-in-the-loop approach. By combining Business Context, Threat Intelligence and an adversary's mindset, root9B is able to proactively identify vulnerabilities and determine how an adversary is most likely to target and infiltrate a network. Knowing the potential adversary, their methodology, and their objectives allows us to direct our ASB operations to those portions of the City's network that are at greatest risk. It is this ability to anticipate the adversary and act decisively that uniquely sets root9B apart from all other Cybersecurity vendors.

01.2.4 Value Added Recommendations and Reporting

root9B provides value added reporting and results in the form of a comprehensive Attack Surface Baseline Report. This report is a genuine value added product. It is easy to understand and facilitates informed decisions as opposed to the standard automated tool "data dump" which leaves customers with too much data and little actionable intelligence or implementable recommendations. root9B's Attack Surface Baseline Report includes a cyberattack narrative based on threat analysis specific to the City of Charlotte's Business Context and network architecture. Additionally, we provide an executive summary (C-Suite), mid-level manager view, and a complete technical review for your Chief Information Systems Officer (CISO) and Security/System Administration staff. For a complete listing of our ASB deliverables, reference **Section 02.11**.

01.2.5 root9B Acumen and Experience

A significant differentiator of root9B's ASB is our security assessment team. root9B operators/analysts have the experience and insight to act as experts to review policies, configurations, and overall health of your network from a skilled network administrator and experienced cyber defender perspective. We start our assessments by measuring the components of the City's network against industry accepted standards and frameworks. Our security assessment team also evaluates the existing defensive solutions against those standards as well as analyzing their effectiveness in supporting the City of Charlotte's defensive strategies. Though our security assessments initially focus on a Client's Cybersecurity implementation against Government and industry standards (e.g., National Institute of Standards and Technology [NIST] SP 800 series publications, Defense Information System Agency [DISA] Security Technical Implementation Guide [STIG], Center for Internet Security [CIS] Security Benchmarks), we go well beyond meeting industry norms. Much as an adversary is not limited to a fixed set of attack techniques, our assessment will be tailored in such a way to exceed your security needs by considering far more than a fixed set of prescribed standards. This result adds network defense value in a sustainable defensive cyber program that is unique and tailored to the needs of the City.

01.2.6 Customer Service

root9B's management approach is focused on complete customer satisfaction with root9B's products, services, and performance. Our management approach emphasizes a qualified team performing according to a comprehensive project plan, maintaining flexibility in execution, responsiveness to customer needs, and close collaboration with the City of Charlotte to ensure that the products and services delivered provide value. We meet these objectives by applying best-practices, processes, and methods guided by disciplined systems engineering processes over the entire life cycle of the City's Security Audit and Assessment Services engagement. This includes precisely defining the task requirements, establishing relevant program/quality metrics, tracking performance, establishing open communications, and accurately reporting our results. City of Charlotte benefits from a customer-focused program that is unbureaucratic, responsive, and flexible.

01.2.7 Minimal Changes to the City's Systems

root9B's ASB engagement will have minimal impact the City of Charlottes existing infrastructure, systems, or operations. Operating on-site, or optionally from root9B's Adversary Pursuit Center (APC) in Colorado Springs, all that is needed is Virtual Privat Network (VPN) access. root9B does not require extensive proprietary hardware or software to be installed on the City's enterprise system to conduct its ASB engagement or support remote communications.

The one software platform that root9B proposes to install on the City of Charlotte's network is our credential assessment tool; ORKOS. Reference **Section 2.6.1** for details.

This Page Intentionally Left Blank

02 TECHNICAL APPROACH

root9B's Attack Surface Baseline (ASB) assessment incorporates traditional PenTesting and Vulnerability Assessments, yet extends the assessment beyond what is commonly offered by the industry. This ASB will specifically address the technical, functional, and information aspects unique to City of Charlotte's environment, as well as collect the assessment data needed to meet City of Charlotte's annual PCI mandates.

When conducting the ASB, root9B will ensure our assessments are germane by combining our understanding of City of Charlotte's Business Context, our "*Think like an Adversary*" mindset, and City of Charlotte specific threat intelligence baseline across each activity. We will use this information to filter irrelevant threats and vulnerabilities to ensure the assessment properly incorporates risk, probability of exploitation, and potential business impact to City of Charlotte.

02.1 PCI DSS Compliance Assessment (RFP Section 3.1 and 3.2.1)

To support City of Charlotte's annual PCI reporting requirements root9B will enlist the specialized services of our small business teammate, NDB LLP. NDP specializes in PCI DSS audits and will provide the City of Charlotte with industry best-of-breed audit methodologies through its use of licensed Qualified Security Assessors (QSA).

Employing a seven (7) phase PCI DSS roadmap, NDP will identify, assess, test, and document Cardholder Data Environment (CDE) controls mandated by PCI DSS v3.2. This will include the following:

1. PCI DSS Readiness Assessment and Gap Analysis
2. Policy & Procedure (P&P) Analysis and Development
3. Remediation Activities
4. Vulnerability Scanning Services
5. Penetration Services
6. Assessment | On-site Fieldwork
7. Issuance of "Report on Compliance" (ROC) and any other necessary reporting deliverables

The objective of the investigation will be to thoroughly assess whether or how a malicious user could gain unauthorized access to City of Charlotte PCI assets, associated networks and systems affecting cardholder data, system files, logs and other critical records. As with our ASB implementation (See **Section 2.2** for details), NDB's PCI compliance will result in actionable reporting, cybersecurity enhancement, mitigation, and remediation recommendations.

Following PCI DSS V3.2 industry standards and using a mix of automated tools and manual testing techniques, our testing and verification will assess the effectiveness of the City's in place PCI security measures. This will be achieved by assessing and verifying that the existing City of Charlotte's perimeter security controls adequately protect cardholder data. Where found, we will identify weaknesses and make recommendations strengthen these

PCI security measures. This will include verifying the security setup and configuration of internal City PCI controls to ensure confidentiality, integrity, availability, and authenticity of data and information systems.

To ensure compliance with DSS, our PCI assessment will focus on all PCI mandated topics to include people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data. Additionally, NDB will confirm that the applicable controls, such as scope, vulnerability management, methodology, and segmentation, required by PCI DSS are in place with the City of Charlotte. Finally where needed we will provide expertise and insight needed to complete Self-Assessment Questionnaires C and D.

Per the requirements of the City of Charlotte RFP, all PCI assessments will be conducted on-site in Charlotte.

At the conclusion of this investigation NDB will provide a PCI gap analysis along with detailed, actionable remediation recommendations to strengthen the security level of the City's PCI infrastructure. The content will be similar to what is provided in the ASB Summary report but will be formatted to support integration into PCI report. The final report will address PCI assessment details to include all applicable controls (e.g., scope, vulnerability management, methodology, and segmentation) required by PCI DSS v3.2.

02.1.1 PCI Assessment Deliverables

To ensure that NDB captures and generates the PCI Compliance Assessment Report in a format that readily integrates into City of Charlotte's PCI assessment, NDB will coordinate with City of Charlotte to ensure we properly capture the vulnerability management and methodologies needed to meet City of Charlotte's PCI reporting requirements. NDB will provide properly scoped and formatted material for integration into the required PCI report. For example, this may include PCI DSS 3.2 Self-Assessment Questionnaires (SAQ), Attestation of Compliance (AOC) forms, and Report on Compliance (ROC) templates.

The Payment Card Industry (PCI) Data Security Standard (DSS) Compliance Assessment Report will specifically include:

» Description of detected PCI vulnerabilities, and an assessment of the system and enterprise impacts of any detected vulnerabilities.

» Narrative description of the methods and tools used to exploit detected vulnerabilities.

» Recommendations on software updates (patching) policies and procedures.

» Actionable remediation and hardening recommendations addressing identified vulnerabilities and misconfigurations.

02.2 Internal and External Penetration Test (RFP Section 3.1 and 3.2.2)

Using City of Charlotte provided network configuration data which may range from full network disclosure to no prior network insight, we will conduct 'black-box', 'grey-box', or 'white-box' PenTesting of City of Charlotte's external (internet-facing) and internal (inside the City's network firewall) devices and information systems. Our security assessment will employ multiple techniques to include intelligence gathering, discovery & probing, vulnerability analysis, exploitation, and post exploitation analysis, and other methods of the to identify potential exploitation risks to City of Charlotte.

The following narrative describes the techniques we will employ when conducting the Vulnerability Assessment and Penetration Testing (collectively PenTesting.) Note: root9B combines our discussion of Internal and External PenTesting since both activities are similarly scoped, employ similar approaches, and result in a like set of deliverables.

Figure 1 illustrates the progression of root9B PenTesting activities.

root9B PenTesting uses a custom, systematic testing process based upon well-recognized frameworks such as the Penetration Testing Execution Standard (PTES) and the Open Source Security Testing Methodology Manual (OSSTMM). Additionally, root9B will apply a mix of automated tools and manual testing techniques to maximize the thoroughness of the test and to reduce the likelihood of false positives.

The PenTesting will include the following activities:

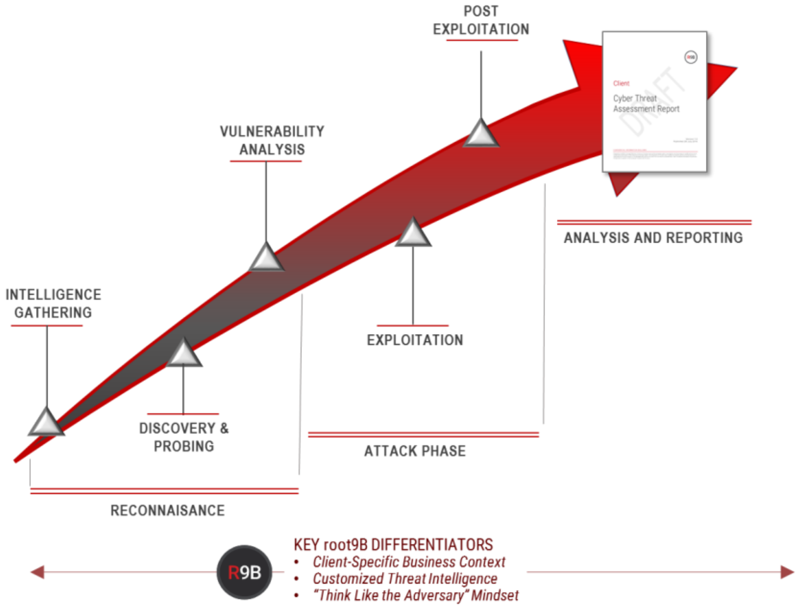

POST EXPLOITATION
VULNERABILITY ANALYSIS
INTELLIGENCE GATHERING
DISCOVERY & PROBING
EXPLOITATION
ANALYSIS AND REPORTING
ATTACK PHASE
RECONNAISANCE
Client
Cyber Threat Assessment Report
DRAFT
R9B
KEY root9B DIFFERENTIATORS
• Client-Specific Business Context
• Customized Threat Intelligence
• "Think Like the Adversary" Mindset

Figure 1 – root9B's Approach to Vulnerability Assessments and Penetration Testing

root9B's approach combines multiple stages and techniques that consider key issues of the targeted systems for a comprehensive assessment.

» **Intelligence Gathering** - root9B employs reconnaissance techniques for conducting predictive target analysis, identification, and discovery, typically using Open Source Intelligence (OSINT), commercial, or proprietary tools and techniques to identify/discover and anticipate elements of the City's network that an adversary is likely to attack. Using OSINT techniques and processes, we will locate publicly available information that may be valuable/useful towards the project scope and to a real-world potential attacker. Sources of information can include, web searches, corporate information searches, and public employee social media pages.

» **Discovery and Probing** - root9B will actively scan in-scope portions of the City's network using well-known automated tools on all TCP and UDP ports to identify any known vulnerabilities or issues. Our automated tests include checks for all common methods for exploiting targeted technologies, including but not limited to; patch audits for unpatched vulnerabilities, default credentials in third party products, SQL injections, cross-site scripting, and sensitive information leaks as defined by the City's Restricted Data Policy. root9B applies a scanning process that ingests data collected during the intelligence gathering phase to develop a detailed understanding of potential network targets that an adversary is likely to pursue. Since City of Charlotte has opted for a Gray-Box assessment, root9B will apply the limited network details provided.

» **Vulnerability Analysis** – We will search for exploitable vulnerabilities that may exist in exposed services (or APIs, applications, firmware, or through social engineering). Where possible, root9B will extrapolate the data collected during Intelligence Gathering and Discovery & Probing, and condense the collected data into 'target profiles' that mimic a hostile adversary's offensive cyber operations Tactics, Techniques and Procedures (TTP). During this phase root9B identifies possible entry points and system vulnerabilities into targeted systems. Once these target profiles have been established, we will gather more detailed information on the target network and/or devices including operating-specific information, application-level information, user and/or group information, and other metadata regarding internal City operations. root9B will conduct Vulnerability Analysis to provide insight into the value of each target to a hostile cyber adversary, including how the device may be used to pivot deeper into the network.

  Results from the scan(s) are further analyzed to ensure the validity of the findings. Validation of the results may involve manual testing or the use of additional automated tools. (False positives are not included in the final report.) Our Cyber Threat Analysts use the results of the scanning to generate an initial target profile for subsequent steps.

» **Exploitation** - During the Exploitation phase root9B will use a custom manual and automated testing process that systematically inspects select systems to exploit identified vulnerabilities. Customized for each targeted system, root9B will employ any number of attack techniques. Our analysts skillfully employ apply a combination of publicly available exploitation code, commercial PenTesting tools, as well as root9B unique exploitation techniques, software, and tools to maximize the thoroughness of the test and to reduce the likelihood of false positives. Our penetration testing tools and techniques employ the latest threat vector TTPs and tools to simulate realistic attack conditions. Specific to each desired exploitation outcome root9B may employ malicious agents such as implants, call-backs, and other payloads. All discovered vulnerabilities that are potentially exploitable may be manually explored and exploited, provided that there is a high confidence that the exploit will not result in a Denial of Service (DoS) or other disruption in the City's operations. Vulnerabilities that if exploited may impact the City of Charlotte systems or operations will *not* be tested and will be noted in the final report.

  During this phase root9B's ability to apply an adversary mindset becomes a significant discriminator. Rather than employ client provided credentials, root9B conducts penetration testing and exploitation (and subsequent post exploitation) in the same manner as likely adversaries will do. Using the same threat actor tools and TTPs, we will attempt to gain access privileges to the highest value segments and systems on the City's network. Using an adversary mindset and approach provides a far more accurate and meaningful gauge of the City of Charlotte's vulnerability than would be realized through automated scans alone.

» **Post Exploitation -** These are activities conducted on a system after having achieved access. Where access is gained through an exploited vulnerability, root9B will then attempt to gain escalated privileges, execute code on exploitable services to gain further escalated privileges, find additional vulnerabilities, gather access information (passwords, keys, documents, etc.) and/or move laterally within the project's scope. root9B documents all evidence of successful penetrations by way of screen captures. This evidentiary material is later included in the summary Attack Surface Baseline Report.

root9B will focus its PenTesting on the IP addresses provided during scoping discussions. We will exclude City of Charlotte's blacklist of unapproved or regulated IP addresses from the security assessment. Furthermore, all tools will be configured to reduce risk to business operations, software, and services. To preclude any disruptions to City of Charlotte operations, root9B will not attempt to perform any exploitation without prior approval from City of Charlotte staff. All assessments will be preceded with adequate notification and approval from City of Charlotte's technical staff. root9B is prepared to limit penetration testing to off-peak hours (7 PM-4 AM Standard Scanning and 10PM-4PM) for intrusive scanning to reduce impact on its business operations.

02.3 Web Application Penetration Test (RFP Section 3.1 and 3.2.3)

root9B will conduct a thorough assessment of designated City of Charlotte and third party (Oracle PeopleSoft), and City developed (.Net, Java) web applications to identify, assess, and propose mitigations to any identified vulnerabilities. root9B web application testing uses a custom, systematic testing process based upon well-recognized frameworks such as the Open Web Application Security Project (OWASP) Testing Guide, OWASP Application Security Verification Standard (ASVS), and the Open Source Security Testing Methodology Manual (OSSTMM).

During an initial Discovery and Exploration phase, root9B will manually explore the designated website(s) hosted on Linux (RedHat, CentOS, Ubuntu) and Windows (Server 2008 R2+) to include a software and associated database review to become familiar with the functionality, purpose, workflow, and content. Using a combination of manual analysis and a static source code analysis tool root9B will identify weaknesses (if any) in the applications' logic. By combining manual and automated analysis techniques we can increase the speed of the analysis while leveraging the experience and training of senior root9B Cybersecurity Engineers to identify potential weaknesses in the software. root9B's static review will employ functional analysis, residual data analysis, and static analysis tools to examine:

- Local application data
- Application configuration
- Mobile application functionality
- Application interactions with external services

Next, root9B will conduct an automated vulnerability analysis employing well-known vulnerability identification tools to actively scan the City of Charlotte's web application(s) and identify any known vulnerabilities or issues. Our scans can include un-authenticated scans simulating an anonymous user, authenticated (per access roles) scans simulating a logged in user, and infrastructure scans to discover server configuration issues. Results from the scan(s) will be manually analyzed to ensure the validity of the results. Validation of the results may include manual testing or the use of additional tools. False positives will not be included in the final report.

During a manual testing and exploitation phase, root9B will use a custom testing process that thoroughly and systematically inspect all aspects of the website application. The process covers all major aspects of web application security including, but not limited to: Authentication, Authorization, Session Management, Input/Output Validation, Injection, Misconfiguration, Privilege Escalation, and Sensitive Data Handling/Exposure.

root9B will perform fuzzing, cross-site scripting/exploit, and specialized Vulnerability Assessments against the web applications identified by the City of Charlotte. Commonly used cyber actor attack surfaces (e.g. public facing assets) will be explored and customized techniques or tools may be written and used to probe for vulnerabilities in the application frameworks. All raw data will be analyzed by root9B Cyber Threat Analysts and included in the ASB report. In the report, root9B will highlight the types of cyberattacks that may be deployed during an offensive cyber operation through the City's websites and web application products.

Where appropriate, discovered vulnerabilities that are potentially exploitable may be manually explored and exploited if there is a high confidence that the exploit will *not* result in a DoS or other negative condition. Those vulnerabilities that if exploited may negatively impact the City of Charlotte systems or operations will not be tested and will be noted in the final Assessment Report.

If further access is gained through an exploited vulnerability, root9B will then attempt to gain escalated privileges, identify additional vulnerabilities, gather access information (passwords, keys, documents, etc.) and move laterally within the project scope. With the exception of access/system/security logs, any artifacts (files, accounts, etc.) generated by root9B will be documented and removed (primarily through timer "self-destruction") from the affected system(s) prior to the end of the engagement. If we cannot remove the residual files or if removal could affect the City of Charlotte's systems, we will ask the City to remove them.

All discovered vulnerabilities and exploits, associated evidentiary data, and cursory remediation advice for each vulnerability will be included in the ASB report. If "Critical" severity vulnerabilities are discovered during testing, root9B will immediately notify the City.

02.4 Wireless Security Assessment (RFP Section 3.1 and 3.2.4)

root9B's wireless network security assessment and penetration testing will utilize a risk-based approach to identify critical vulnerabilities that exist in the City's wireless infrastructure. The data collected during this assessment will highlight the use of wireless network points as a means for cyberattack and the risk this dynamic medium may present to City of Charlotte's critical business assets. Assessment and testing objectives include:

- Providing City of Charlotte with an understanding of the level of risk from wireless infrastructure.
- Providing recommendations for a cost-effective and targeted mitigation approach.
- Creating a basis for future decisions regarding information security strategy.

Using an on-site "War-walk" approach that employs a wireless-enabled notebook computer or device to map wireless hotspots, root9B will assess whether remote access points can be compromised and exploited by an attacker to gain access to internal City of Charlotte domains, or expose sensitive data such as authentication credentials or potentially deny/degrade services.

root9B will initially attempt to identify the types of wireless services in use through a combination of on-site "War-walk" testing and open source research. Open source research will include conducting web-based searches to gather publicly available information on a client, potential device types, and technologies in use. root9B will also attempt to determine if any client components are remotely accessible via external access vectors to include internet availability, proximity of broadcast signals, or deployed bridging devices. Detailed attributes collected during device reconnaissance can include: SSID, WEP/WPA status, EAP status, Channel, device type, AP Name, Latitude and Longitude, Vendor, MAC address. Once the wireless services types have been identified and enumerated, root9B will attempt to identify vulnerabilities and compromise the discovered wireless services and access points. root9B's wireless assessment methodology will include, but is not limited to testing the following:

- Access Control, Integrity, Confidentiality, Availability
- Authentication attacks.
- Radio Frequency (RF) Analysis.
- Authentication and Authorization.
- Unauthorized Access Points and Unauthorized Vendor Devices.
- Access Range and Exterior Signal Bleed.
- Cryptographic strength of keys.
- Man-in-the-middle attack determinations.

To simulate a real-world attack on your networks, wireless penetration testing will begin with limited knowledge and no credentials ("Black-Box" or "Grey-Box" testing). While this exercise is not designed to test the effectiveness of each implemented control individually (depending on scope), City of Charlotte will learn what vulnerabilities exist and the overall information security risk the wireless infrastructure introduces to the client's IT environment. However, if "Critical" severity vulnerabilities are discovered during testing, root9B will immediately notify the City of Charlotte.

02.5 Microsoft Group Policy Security Assessment (RFP Section 3.1 and 3.2.5)

root9B recognizes that although Group Policies do not provide complete domain protection, they still function as a key security component in the defense of City of Charlotte's network infrastructure. Our approach to reviewing the City of Charlotte's Group Policy Security settings applies a two-step process that begins by assessing whether the MS Group Policies are configured in accordance with industry best practices, Microsoft recommendations, and other regulatory standards. We follow this initial assessment with a check of endpoint configurations to ensure that City of Charlotte endpoints have received and are properly configured in accordance with the prescribed standards. root9B will work with the City to identity which systems will be included in the scope assessment through a series of interviews. This will ensure that root9B focuses their efforts on only targets most valued by the City.

root9B will conduct Group Policy setting assessments using the Microsoft Security Compliance Manager as a baseline. This tool readily supports centralized security baselines audits for Windows workstations and server operating systems, and Microsoft applications. Through this tool root9B staff will have a security compliance verification capability as well as access to the complete database of Microsoft recommended security settings. Examination of Group Policy Objects (GPO) and the Organizational Units (OU) structure will map existing City of Charlotte Group policy settings to industry best practices, updated security guides, attack surface reference workbooks, Microsoft recommended security settings, and deep security expertise and experience. As appropriate, root9B can expand its assessment to include regulatory guides such as the Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), and other standards.

Specifically, our assessment will examine the following GPO settings:

- Security Settings (Account Policies, User Rights Assignments, Event Log, Restricted Groups, System Services, Applications Control Policies (AppLocker), IP Security Policies, etc.)
- Kerberos and Password Settings
- Group Policy Preferences (Registry Settings, Local Users and Groups, Scheduled Tasks, etc.)
- City of Charlotte specific needs or configurations

Following our assessment of City of Charlotte Group Policies and configuration settings, root9B will validate that domain clients are receiving and are configured in accordance with these policies/settings. Using Group Policy Results, we will generate a random or City-specified sampling of devices to ensure that configuration settings are installed and operating correctly. Finally, root9B will provide recommendations for effective mechanisms and approaches for on-going maintenance of Group Policies.

Our MS Group Policy Assessment support will culminate with a two-part final report. The report will reflect shortfalls (against industry standards, analyst experience, etc.,) in Group Policy configurations. Secondly, we will report on the success rate of City of Charlotte endpoints in applying these configuration settings.

02.6 Microsoft Active Directory (“AD”) Security Assessment (RFP Section 3.1 and 3.2.6)

Using both technical and non-technical audits, root9B will gather detailed information about the configuration of the City of Charlotte’s AD directory, privileged accounts, security settings, and domain controller configurations. Interviews with City of Charlotte administrator will supplement automated information-gathering scripts and custom analysis tools to identify gaps in process or governance that may expose the City to cyber risk. The preceding Group Policy assessment will assist in this endeavor by providing associated AD policy and configuration details.

Using Microsoft recommendations, industry best practices, and root9B experience, root9B will assess the Domain Controller’s health and susceptibility to cyber threats. We will specifically address the following security aspects for the AD Domain Controllers:

- Host-based defenses (Host-based firewall and Antivirus, Microsoft EMET, Application Whitelisting)
- Investigate if the Domain Controllers can access the internet by any means
- Reveal if the Domain Controllers function for anything other than AD and DNS

- Operating system of the Domain Controllers and last time security patches were installed
- Account management to include DSRM accounts, KRBTGT service account, and Administrative account lifecycle and controls
- Define how administrators remotely access the Domain Controllers

Additionally, root9B will review the City of Charlette's privileged account delegation model to review how permissions have been defined and where. This review includes interviews with the AD administrators, an audit of Group Policies Objects for Restricted Group configurations, and a random sampling of accounts to see if users have been assigned appropriate levels of administrative powers.

root9B applies the Microsoft privilege tiered approach that calls for organizations to have logical administrative boundaries. This isolates accounts and privileges found in one tier from assets found in another tier. (For example, a server administrator should not have permissions to administrate workstations or the domain. While a domain administrator should not have elevated powers over servers or workstations.) root9B will measure the City of Charlette against this Microsoft standard. root9B will also review how privileged accounts are controlled in the domain and what tools the City of Charlette has employed. As a number of different solutions exist to help manage privileged accounts (Microsoft FIM/MIM, CyberArk, RSA tokens, Thycotic Secret Server, native AD tools/ organization policies, etc.), this review will be customized to whatever solutions the City of Charlette has employed.

02.6.1 root9B's Unique Credential Assessment Platform: ORKOS

root9B alone offers ORKOS: a state-of-the-art credential assessment and remediation product. ORKOS identifies exposed credentials that lead to major network breaches when attackers steal and use those credentials to move laterally through an enterprise network. ORKOS combines comprehensive data collection, advanced logic, and cutting-edge credential analysis to identify the critical links attackers will exploit during a breach. It characterizes both the immediate risks and higher-order effects to show the total impact of credential theft within a network. ORKOS can also simulate a client's network environment to support pre-exploitation remediation and mitigation actions.

ORKOS highlights include:

- Comprehensive data collection.
- Advanced risk analysis and logic engine.

- Generates detailed findings and remediation recommendation report.

root9B uniquely offers ORKOS to help identify City of Charlotte credential risks that enable attackers to pivot (move laterally) from system-to-system once they have breached the City's network. Through the deeper analysis that ORKOS provides, our Operator/Analysts will have a better understanding of credential-related vulnerabilities and will be better able to highlight associated critical risks. ORKOS identifies exposed credentials to include passwords with the highest system privileges, passwords that are reused, and passwords that have domain equivalent permissions. ORKOS employs advanced logic to identify vulnerable links and presents this information in easily understood visualizations showing individual as well as aggregate risk. ORKOS collects data on the following credential-based topics to:

- Identify credentials found on the network
- Identify all user accounts on each system
- Record all relevant privilege assignments
- Record relevant system configuration details
- Identify all security group memberships

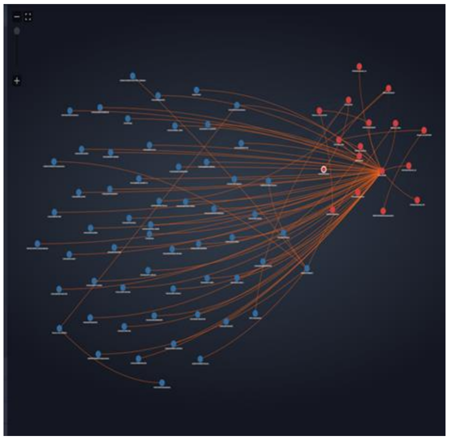


Figure 2 - ORKOS

ORKOS characterizes both the immediate credential risks and subsequent credential access risks to show the total impact of credential theft within a network. ORKOS discovers a Client's critical links that are at risk of credential exposure. It enables analysts to analyze the myriad conditions, privileges, and configurations and quickly visualize potential lateral and vertical exploitation that a Cyber attacker could exploit to gain greater system access and control.

Using ORKOS we will assess the City of Charlotte's network for credential risk and identify to City system administrators how to remediate any credential-based problems found. The resulting credential assessment will specifically:

- Identify credential dissemination
- Identify re-used credentials
- Identify direct and indirect impact of credentials, constructing attack chains for maximal impact
- Determine mechanisms to break credential-based attack chains
- Determine changes to prevent it from happening in the future

On completion of an AD Security Assessment, root9B will present the City of Charlotte with a comprehensive analysis of both technical and non-technical risks. In addition, it presents a prescriptive guidance and prioritization to provide an organization a roadmap to a more secure directory

02.7 Domain Name System ("DNS") Security Configuration Audit (RFP Section 3.1 and 3.2.7)

root9B DNS security configuration audit services will help provide secure name and address resolution functionality for the City of Charlette. root9B's DNS Security Configuration Audit will provide a clear view into the City's current configuration along with any discrepancies relating to DNS zones configurations or DNS permission levels. For speed and efficiency, root9B will employ automated DNS auditing scripts to specifically interrogate

DNS Server and Zone configurations. This reduces the time and cost associated with security testing while providing repeatable test results utilizing the latest configuration benchmarks. Follow-up manual checks will validate and supplement automated findings.

Department of Defense (DoD) DNS Security Requirements Guide (SRG) and Security Technical Implementation Guidelines (STIG) provide a foundation for our evaluation. Paired with extensive DNS experience, this will deliver the full range of DNS compliance validation/verification. Areas of focus will include:

- Existence and configuration of a Microsoft Domain Name System Security Extensions (DNSSEC)
- DNS aging and scavenging mechanisms for cleanup and removal of stale resource records, which can accumulate over time
- DNS lock down to include Secure Dynamic Update, DNS logging, Zone transfer permissions, and other configuration settings
- Conditional Forwarders and DNS resolution forwarding configurations
- Placement of the DNS server in network and if proper configuration of perimeter devices exist to protect internal DNS servers

02.8 Server Security Configuraiton Audit (RFP Section 3.1 and 3.2.8)

root9B recognizes that there is no one way to secure a server. Everything depends upon City of Charlotte's business context, the server environment and the unique requirements of each City server. root9B's approach treats Server Security Configuration audits as one element in a larger overall security strategy for the City of Charlotte. We will synchronize our server analysis and audit activities with the preceding Group Policy, AD, DNS assessments.

In addition to DISA STIG, CIS, and industry best practice assessments, root9B audits will focus on ensuring that basic tenets in system security are followed. This will include:

- Install only what is needed for the server to operate
- Ensuring that the City of Charlotte employs a robust software and security patching program
- Ensuring that Antivirus and Host-Based protections configurations are current
- Ensuring that the server administrative delegation model is configured correctly
- Reviewing City's end-of-life program and does is adequately address legacy vulnerabilities

Our investigation will meet both internal and externally mandated auditing inspection and regulatory analysis mandates. Additionally, this assessment can be used for a variety of purposes, including forensic analysis, regulatory compliance, monitoring user activity, and troubleshooting.

02.9 Compliance with City's Information Security Manual and other Standards

root9B will conduct all cybersecurity assessments and audits in accordance with the City of Charlottes' Security Manual (To be provided upon contract award) and. as appropriate, industry best practices and applicable regulatory frameworks. This could include:

- SANS Critical Security Controls
- Federal Information Processing Standard (FIPS) Standards
- National Institute of Standards and Technology (NIST) Guidelines
- International Organization for Standardization (ISO) 27002
- Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG)
- Center for Internet Security (CIS) Security Benchmarks
- Other State Laws and Standards as applicable to the assessment

root9B will, in conjunction with the City of Charlotte, develop a detailed scoping document that identifies any specific regulatory guidelines or legal standards that need to be applied prior to each service engagement.

02.10 On-Site and Off-Site Engagment Support

Per the desires of the City of Charlotte, root9B is proposing to provide all services on-site in City facilities.

02.10.1 Alternative Approach to On-Site Services

To save our clients significant time and money root9B also offers a mixed range of on-site and off-site services. Since Remote Cybersecurity operations are the norm for root9B, we are accomplished providers of providing a complete range of services from our state-of-art Adversary Pursuit Center (APC). This approach saves our client's both time and money while providing secure access to the full range of root9B's powerful suite of tools. Nearly all root9B cybersecurity services can be conducted from our Colorado Springs, CO APC, with back-up provided from a secondary APC in San Antonio, TX.

Based on equivalent engagements, root9B is able to provide an alternative approach that mixes both on-site and off-site engagement. For this cost-saving approach, root9B proposes to confine on-site (in Charlotte) ASB activities to a project kickoff meeting, PCI assessments, internal and wireless penetration testing and vulnerability assessments, and as required program management reviews. Interchange meetings would generally be limited to one day events. Internal PenTest activities would be conducted by fly-out teams with on-the-ground

root9B conducts cyber operations remotely from its state of the art Adversary Pursuit Centers (APC). The APCs serve as the nerve centers for our manned cyber security HUNT operations. They are always-on environments where highly-trained security operators actively monitor clients' networks, searching for malicious activity.

engagements. External PenTests could alternatively be performed remotely from root9B's APC, saving up to $5,000.00 in the initial engagement for **WBS 1.4**.

Pricing for the requested **all-on-site** approach is reflected in the City provided **Form 4** of **RFP Section 06**.

02.10.2 Communications Between On-Site and Off-Site Teams.

On-site and off-site root9B teams will communicate via telephone and email, text, Skype, and security tool embedded communications links as needed. Communications between root9B engagement teams and City of Charlotte staff will be in accordance with the Communication Plan outlined in **Section 03.5**.

02.11 Deliverables

root9B will generate a comprehensive report that addresses all sections of the proposed City of Charlotte Attack Surface Baseline. The ASB report will consist of the appropriate specific ASB engagement summaries to include:

- Payment Card Industry (PCI) Data Security Standard (DSS) Compliance Assessment Report;
- Internal and External Penetration Test Report;
- Web Application Penetration Test Report;
- Wireless Security Assessment Report;
- Microsoft Group Policy Security Assessment Report;
- Microsoft Active Directory (AD) Security Assessment Report; 7. Domain Name System (DNS) Security Configuration Audit Report; and
- Server Security Configuration Audit Report.

The resulting report will be easy to understand and facilitates informed cyber defensive response decisions and provides clear, guidance and recommendations to correct any vulnerabilities discovered. The Attack Surface Baseline Report includes separate sections designed specifically for the City's Executive Staff (C-Suite), Mid-Level Managers, and a detailed technical review for your CISO and Security/System Administration staff.

Included in the report is a cyberattack narrative based on threat analysis specific to a City of Charlotte's business context security architecture. The following provides an overview of the components within the ASB report:

- **Executive Summary**
  - Provides a senior management view into the engagement scope, approach, critical findings and root9B's remediation recommendations.
- **Preliminary Report (draft of Detailed Technical Report)**
  - root9B will make a preliminary report draft available to City personnel for review and feedback.
- **Detailed Technical Report**

- Assessment and testing methodology details for PCI DSS, Internal, External, Web Application, Wireless, MS Group Policy, MS AD, DNS, and Server Security assessments
- List of all assets evaluated by IP address and host name.
- Uniquely identified collection and detailed technical description of any detected vulnerabilities from each assessment and test section.
  - IP address and host name of the vulnerable system.
  - Assessment of the severity of the findings to include a narrative of system and enterprise impact.
  - Client specific risk rating as a function of vulnerability impact and ease of exploitation.
  - Narrative description of attacker methods to exploit detected vulnerabilities.
  - Supporting detailed exhibits and evidence.
  - Detailed remediation recommendations.
- Positive security controls that were identified.
- Detailed References.
- Raw tool output.

To help meet PCI reporting requirements, the final ASB report will include detailed discussion of the tools used, steps performed, vectors, and any vulnerabilities exploited during testing.

Formal written submission of our ASB repost will be followed with a verbal presentation that highlights the findings of the assessment, reviews remediation recommendations, and addresses any questions. Verbal presentations may be performed on-site in Charlotte or remotely via telephone or video teleconference (VVTC) from root9B's Colorado facilities.

Finally, all root9B documentation will provide sufficient detail to address the requirements specified in the **RFP Section 3.14.5**.

03. MANAGEMENT APPROACH

03.1 Customer Service (RFP Section 3.4)

Our management approach is to focus on complete City of Charlotte satisfaction with root9B's products, services, and performance. Customer service is a central tenet with our staff. We carefully select the staff assigned not just for their technical skills but also for their customer service orientation. As such, all staff members understand the need for genuine customer orientation. As individual representatives of root9B, our team knows that we must provide prompt, courteous service. This customer orientation extends to the responses we provide to all inquiries and products we generate. To the degree possible, we will also assist in directly resolving, or identifying other root9b and non-root9B resources capable of resolving technical issues and concerns.

To meet this aim, we implement several management features that guarantee that root9B provides City of Charlotte with full satisfaction while minimizing any performance risk. Key features of our management approach include:

- Assignment on Day One of a strong, effective, Delivery Lead/Project Manager (DL/PM) supported by individual Task Leads each having the right credentials on Day One of any engagement;
- Assignment of highly qualified staff with technical experience, certifications, and on-keyboard experience needed to perform the services proposed. Allocating the correct skill sets and numbers of personnel as well as associated equipment and infrastructure support.
- A proven Program Management Plan (PMP) that offers timely and thorough contract and project status reporting based on agreed Service Level Agreements (SLA) and Key Performance Indicators (KPI) that accurately and objectively measure root9B performance.
- Placing task management authority and accountability as close to the customer as possible, while maintaining strong corporate visibility and oversight.
- Solid corporate credentials backed by deep individual experience across the range of cybersecurity engagements and operational capabilities offered.
- Providing prompt and accurate status updates and reports to City of Charlotte and its members through informal reporting when needed, and via required Monthly Program Status and Financial Reports.
- Engagement support performed without delay to meet City of Charlotte needs.
- A strong corporate commitment to meeting customer needs by way of unbureaucratic management and direct and continuous program monitoring by our Chief Executive Officer (CEO) and his senior staff.

We keep overall customer service satisfaction high via project performance control procedures consistent with proven industry program management practices. We ensure DL/PM's receive the highest quality technical and analytical support, and ensure project performance through aggressive monitoring, strict compliance to company quality standards, and active reporting. This includes daily monitoring of scheduled tasks by the DL/PM, and regular communications with City of Charlotte and their leadership on cost, schedule, and project performance status. The result is a program management approach able to rapidly respond to the needs of the City.

Central to our approach are the establishment of Service Level Agreements (SLA) and Key Performance Indicators (KPI) that define measures to accurately and objectively root9B performance managing schedule, resources, mission milestones, staff, and the assessment and mitigation of program risk.

03.1.1 ASB Service Level Agreement (SLA)

Service Level Agreements (SLAs) will be tailored to the requirements of individual City of Charlotte tasks. As an example, **Table 1** illustrates how root9B prioritizes and defines security alerts, and response times and actions for the corresponding priority levels assigned for our ASB service.

Priority Level (Category)	Severity	Activity / Event / Condition	Response Time and Actions
1	Critical	Discovery during ASB testing of a critical vulnerability that presents an immediate threat to the Client systems and/or operations	≤ 15 Minutes; (Customer Phone call until answered, follow- up with e-mail) Remediation Suggestion (Both immediate and long term)
2	High	Discovery during ASB testing of a serious vulnerability that presents a threat to the Client systems and/or operations	≤ 30 Minutes; (Customer phone call / voicemail, follow-up with e- mail) Remediation Suggestion (Both immediate and long term)
2	High	Critical customer inquiry	Critical customer inquiries acknowledged within 2 hours (Monday-Friday 8:00 am – 5:30 PM) and response provided within 24 hours
3	Normal	Routine customer inquiry	Customer inquiries acknowledged within 24 hours (Monday-Friday 8:00 am – 5:30 PM) and initial response provided within one (1) business day.
3	Normal	Conduct ASB Penetration Testing and Vulnerability Assessment	• ASB Engagement begins on agreed schedule date (Assumes that all requisite PenTest data and conditions are met) • Completed assessment of all in-scope systems on or before scheduled date • Every reason effort made to ensure that the ASB does not result in a negative impact to City of Charleston systems or operations. root9B will notify the client and seek guidance for any ASB that may impact client operations • Evidence provided for all identified vulnerabilities • Provide remediation recommendations for vulnerabilities discovered
3	Normal	Delivery of ASB Report(s)	Delivery on or before scheduled delivery date
3	Normal	ASB Report(s) Quality	ASB report accepted as final after client edits have been incorporated into the draft version

Table 1. Example ASB Program SLAs.

root9B manages cybersecurity services along specific business SLAs mutually agreed upon with City of Charlotte member.

03.1.2 Customer Service Goals

Customer services goals will be measured using Key Performance Indicators (KPI). This tracking performance enables the DL/PM to accurately measure and control the technical, schedule, fiscal performance of each City of

Charlotte engagement. **Table 2** offers examples from similar projects of KPIs that we have tracked to ensure on time and on cost delivery of contracted services.

Metrics Category	Focus	Purpose	Measure of Success
Customer Satisfaction	• Customer satisfaction rating	• Assess customer's perception of how we are doing	• Overall rating of "Very Good" or better during customer surveys
	• Products and services that meet customer's needs	• Measure how well customer needs are being met	• Positive trend in customer satisfaction surveys
Schedule and Performance	• Cybersecurity responsiveness	• Ensure that cyber engagements are timely	• Mean Time to Response (MTTR) • Performance against stated SLAs
	• Tasks completed vs. tasks planned at given point in time (monthly)	• Assess task progress • Apply resources	• 100% of planned tasks completed on time
	• Major milestones met vs. planned at given point in time (quarterly)	• Assess task progress • Apply program resources	• 100% of major milestones met
	• Changes to task requirements	• Understand and manage scope and schedule of task	• All changes to task requirements managed and controlled
	• Timely submission of Products and Deliverables	• Assess task progress • Apply resources	• 100% of Products and Deliverables submitted on or before due date
	• Number of errors identified and removed prior to delivery	• Track effectiveness of QA reviews	• No reported errors after delivery
	• Time to implement corrective actions once identified	• Assess efficiency and effectiveness of corrective action process	• 100% of problems addressed within 48 hours
Management of Key Personnel	• Retention rate of proposed key personnel	• Assess ability to retain quality and quantity of personnel proposed	• Replace vacated positions with qualified individuals within 21 days

Table 2. Example Program KPIs.

root9B measures and tracks program performance to ensure delivery of quality goods and services, customer satisfaction, and that program requirements are met

03.2 Program Structure

Our management approach is focused on complete City of Charlotte customer satisfaction with root9B's products, services, and performance. To meet this objective, we will be implementing several key management features that will guarantee that root9B provides City of Charlotte with full satisfaction while minimizing any performance risk. The features of our management approach include:

- **A strong, effective, Service Delivery Lead** (aka Project Manager) having the right credentials.
- **Assigning the Right Resources** - Allocating the correct skill sets and numbers of personnel as well as associated equipment and infrastructure support.

- **Qualified senior-level cybersecurity staff** backed by a deep staffing pool of available qualified Cybersecurity Operator/Analyst professionals ready to support starting on Day One of operations.
- **Timely and Accurate Reporting** - Provide precise status updates and reports to City of Charlotte through formal status reporting and continuous informal dialog.
- **Continuous, on-going dialog and status reporting** for early problem identification and early resolution.

The organizational structure for this program was selected since it retains management flexibility to meet emerging requirements and efficiently adjust/supplement team capabilities and manning as required.

03.2.1 Management Roles and Responsibilities

To ensure that root9B's organization remains flat and lean, we have intentionally limited the levels of management and overhead administration. The result is an agile, highly responsive management construct with no bureaucracy. **Figure 3** illustrates root9B's simple organizational structure applied to this effort. We strive to bring the right balance of oversight and control without burdening the task with excessive layers of management. This lean organizational framework will be used to manage overall task execution. It provides engaged program control, open customer access, and support reach-back into the root9B's significant pool of qualified expertise. The organizational structure also ensures appropriate program controls and management flexibility to meet emerging or modified requirements.

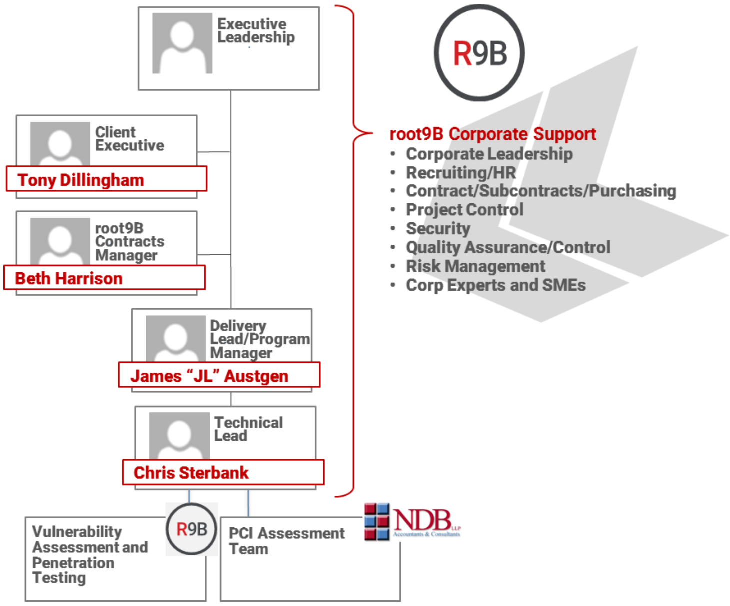


Figure 3 – **root9B's Team**

Our lean organization structure provides non-bureaucratic lines of communication and easy deep reach-back to corporate resources and expertise.

03.2.2 Service Delivery Lead/Program Manager

After careful consideration, root9B selected Mr. James "JL" Austgen as the Service Delivery Lead / Project Manager for the City of Charlotte project. Mr. Austgen is a seasoned technical account manager and support engineer with 14 years of technical management and service experience. He was selected for this project since he is a skilled leader in managing complex root9B cybersecurity programs and strengthening security and reliability of enterprise endpoint offerings. As an experienced technical project lead he will be responsible for scoping the project, managing the effort, and working closely with City of Charlotte to ensure the successful delivery of all products and services.

As the DL/PM he is accountable for both customer satisfaction and the overall success of the program. The DL/PM will also be responsible for contract management, technical execution, cost/budget, and schedules of the City of Charlotte engagement and to interface with City of Charlotte to ensure responsive task performance. The DL/PM remains accountable to Mr. John Harbaugh, root9B's Chief Operating Officer (COO), and reports progress and issues weekly (staff meetings), and monthly (internal program reviews) with root9B management and with City of Charlotte Leadership. He has oversight and approval authority for all project deliverables. The DL/PM is additionally responsible for developing and implementing corrective action plans to address any issues that may arise. He has the authority to make the changes and decisions required to ensure rapid reaction to customer needs and contractual issues. Specific responsibilities assigned to the DL/PM are presented in the table below**.**

Project Elements	Delivery Lead Responsibilities
Program and Performance	▪ Promulgate and enforce root9B management plans, policies, processes, and procedures ▪ Control and report technical, cost, and schedule performance ▪ Manage collection, analysis, and reporting of performance metrics
Cost Control	▪ Approve all cost estimates ▪ Monitor and control all contract expenditures
Staffing and Personnel Assignments	▪ Coordinate and vet candidates with City of Charlotte leadership ▪ Approve all personnel selected and proposed for contract performance
Project Communication	▪ Acts as the primary point of contact for all engagement communication between City of Charlotte and root9B ▪ Coordinates all scheduled and as-needed status updates

03.2.3 Supporting Management Staff Roles and Responsibilities

root9B has implemented a structured organization with clear, standardized lines of communication, responsibility, and corresponding authority to meet City of Charlotte requirements. Each role is defined and is integral to facilitating successful program execution. The following table summarizes the roles and responsibilities of each management position.

Position	General Description	Specific Duties
Executive Corporate Management *(Provided at No Direct Additional Cost to the Contract)*	▪ Responsible for ensuring access to all corporate resources for successful implementation and execution of the City of Charlotte Program	▪ Ensures the program has appropriate visibility and priority within the corporate structure of each Team member ▪ Ensures receipt of all required resources in a timely manner ▪ Participates in senior management reviews ▪ Ensures QA/QC objectivity and compliance ▪ Reviews corrective action issues or plans
Contracts Manager *(Provided at No Direct Additional Cost to the Contract)*	▪ Single point of contact with contracting officer for contractual matters and negotiation ▪ Formal interface to the City of Charlotte Contracting Officer/	▪ Manages all contract and subcontract development and negotiations ▪ Ensuring timely processing of all contact modifications, ▪ Acts as the single root9B interface with City of Charlotte Contracting Office ▪ Submits invoices, cost reports, and formal contract submissions

Position	General Description	Specific Duties
	Representative for all contractual matters	
Program Control Manager *(Provided at No Direct Additional Cost to the Contract)*	▪ Dedicated Project Control specialist who will monitor the day-to-day financials with root9B accounting methods ▪ Provide the necessary program controls for budgeting and expenditures of this contract	▪ Responsible for tracking the monthly expenditures and preparing contract status documentation ▪ Conducts cost control planning, monitoring, and reporting ▪ Takes positive action to correct negative variances
Recruiting/HR Manager *(Provided at No Direct Additional Cost to the Contract)*	▪ Assists the root9B program with recruiting, hiring, and personnel issues	▪ Responsible for new candidate identification, screening, and capture ▪ Responsible for all hiring, orientation, and recruiting activities (e.g., applications, pre-screens, offer letters, drug screening, benefits packages, and benefits orientation)
Quality Control Manager *(Provided at No Direct Additional Cost to the Contract)*	▪ Responsible for implementation of root9B quality assurance system across all elements and subcontractors ▪ Provides leadership and guidance to the program team as it relates to quality assurance	▪ Develops the Quality Assurance Plan ▪ Establishes processes and practices focused on the quality of end products ▪ Assists in determination of formalized processes/tools ▪ Reviews all deliverables and ensures they are of high quality and on schedule ▪ Supports additional process audits as needed

03.3 Corporate Leadership and Support

root9B's executive leadership, while not participating in the day-to-day operations and decision making of our Service DL/PM, will be engaged and actively involved in the oversight of the City of Charlotte contract. root9B leadership will meet monthly with the program management team to monitor and assess the programmatic and financial health of the contract to ensure that contract needs are being met. By keeping abreast of project status, our leadership will be able to address and resolve concerns as they arise and will make sure that the necessary resources are accessible to the team performing this work. In addition, as City of Charlotte 's needs evolve and requirements change under the contract, corporate leadership will help to quickly identify and tap into the wealth of resources and expertise available throughout our company.

03.4 Management Tools and Processes.

root9B will use a variety of project management tools to aid in conducting performance, cost, and schedule tracking and control. These include MS Project for tracking project scheduled tasks and deliverables. Our management approach leverages proven, disciplined best practices to provide structured, repeatable methods for tracking and evaluating performance, controlling the schedule, managing cost and ensuring customer satisfaction. root9B will work with the City of Charlotte's Program Manager to evaluate our program roadmap to identify and assignment priorities, develop project milestones and track analysis, assessment, development, and test objectives to completion. We will incorporate these efforts in an integrated schedule to plan for the appropriate allocation of the correct resources for each task to meet project milestones and deliverables ensuring completeness and a low-risk solution. Our engagement team will monitor work completed versus costs incurred and adjust resource allocation and spending to ensure on-time delivery of required support and products. We will report and deliver the status of our accomplishments, technical performance, travel, costs, issues, and recommendations in Status Reports.

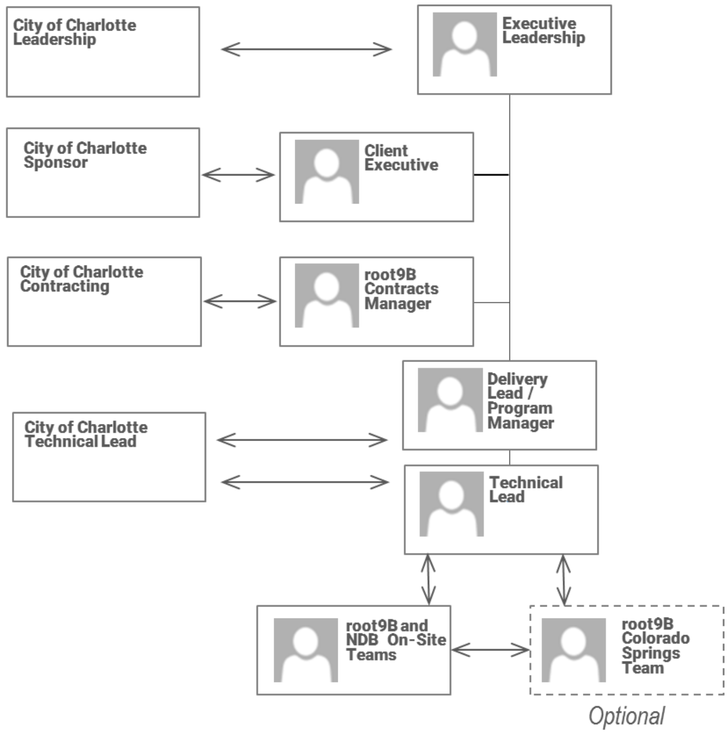

City of Charlotte Leadership
Executive Leadership
City of Charlotte Sponsor
Client Executive
City of Charlotte Contracting
root9B Contracts Manager
Delivery Lead / Program Manager
City of Charlotte Technical Lead
Technical Lead
root9B and NDB On-Site Teams
root9B Colorado Springs Team
Optional

Figure 4 – **root9B's Communications Plan**

root9B will establish timely and open communications and dialog with all key organizational elements within City of Charlotte 's hierarchy.

03.5 Communications Plan

root9B will employ a number of effective communication techniques and approaches to ensure the City of Charlotte counterparts are provided with current, accurate, and complete information on all key aspects of the engagement to include engagement performance, services delivered, cost and schedule details, quality and performance metrics, as well as any problems or risk and the activities associated with their mitigation. As shown in **Figure 4**, the primary lines of communication will be between the DL/PM and the City of Charlotte Project Manager or designated point of contact and between our technical lead(s) and the City of Charlotte technical point of contact. Through active and continuing telephone email, and, as applicable, face-to-face contact, we can confidently provide the on-going dialog and communications that is critical to engagement performance and customer satisfaction. root9B will conduct a formal Project Kick-off meeting and Status Reports with City of Charlotte stakeholders and the root9B Team. Informal interactions will supplement formal status reporting and meetings and will afford City of Charlotte leadership ample opportunity to review the overall effort to ensure resources are being used effectively and managed efficiently. Finally, root9B will host a final out-briefing of the results of our testing. These venues will also provide City of Charlotte opportunities to assess the degree to which root9B services meet or exceed contractual requirements.

root9B will conduct immediate, as-needed notifications and reviews with the City of Charlotte PM and/or technical POCs should we uncover any critical vulnerabilities that puts the City of Charlotte IT environment at significant risk.

root9B will employ communication techniques and approaches to ensure the City of Charlotte counterparts are provided with current, accurate, and complete information on all aspects of the engagement as summarized in the table below:

Event	Purpose	Responsible	Target	When/Frequency	Communication Method
Kickoff Call	Orient all project stakeholders to the Project	Led by root9B SDL, assisted by City of Charlotte Sponsor and Project Manager	City of Charlotte Stakeholders; root9B Engagement Team	Prior to start of work. Used for all new work	Online Meeting
Executive Review Sessions	Provide Senior City of Charlotte leadership with project status	Scheduled by root9B SDL	Sr City of Charlotte leadership	At program start and at program close-out	Online Meeting
Weekly Status / Review Reports and Status Calls	Update stakeholders on progress of the project. • ID any tasks that have fallen behind schedule and reason • Summarize all risks and possible impacts – ID mitigation POC and approach • ID all changes to Project Plan	Scheduled by root9B SDL	City of Charlotte Project Manager & Sponsor; root9B SDL and Security & Technical Lead/s as required	Weekly, Bi-weekly or as needed; frequency of reporting and meetings may decrease as engagement matures	Weekly written report and Online Meeting
Technical Team Meetings	To review detailed plans (tasks, assignments, and action items).	Led by root9B Operations Lead/s; coordinated with root9B SDL	root9B and City of Charlotte Security & Technical Team;	As needed	Online
Program Status Review	Identify improvement plans, lessons learned, what worked and what could have gone better. Review accomplishments.	Led by root9B SDL	City of Charlotte Sponsor and Project Manager	Quarterly and end of major project phases as appropriate	Onsite Meeting, if possible, otherwise Online
Deliverables Meeting	To establish with the City of Charlotte that the project or project phase has completed, review the report, discuss next steps and how to work with root9B technical teams as appropriate.	Led by root9B SDL	root9B Sales account executive, SDL, City of Charlotte Sponsor, City of Charlotte Project Manager, City of Charlotte Stakeholders; Engagement Team	Upon delivery of report or other deliverable	Online and/or Onsite as appropriate

03.6 Staff Qualifications

root9B is comprised of subject matter experts in the field of advanced offensive and defensive cyber operations. Our personnel are routinely tasked with the most advanced and challenging operations within critical mission areas. root9B combines cutting edge technology, tactics development, and vast mission experience with a focus on emerging threats to continuously position us ahead of the adversary. As a result, root9B is able to offer clients premier cybersecurity consulting services, advanced cyber operations and forensics training, cyber threat and risk detection assessments, and complex cyberspace range operations. With thousands of “real-world” operational experiences in the cyberspace domain, root9B professionals continue to perfect cyber operations tradecraft and routinely solve complex problem sets for the dynamically charged world of cybersecurity.

Recognized by their peers across the cybersecurity community, root9b staff are respected as subject matter experts in the field of advanced defensive network operations. While avoiding public recognition, our corporate and individual cyber defense successes are never-the-less nationally recognized. root9b staff members have garnered numerous awards including citations from President Obama, President Bush and other notable leaders both in the public and private sector. With thousands of real-world operations, root9b professionals have perfected their capabilities allowing them to anticpate, find, and neutralize even the most advanced cyber threats.

04 SUMMARY

As a trusted incumbent provider of cybersecurity services to major Corporations and the US Government, root9B has delivered on our promise of ensuring each Client's' network and data sovereignty, protection of their critical brand and customer trust, and meeting regulatory requirements. Our on-going Cybersecurity efforts can provide a key element in maintaining City of Charlotte customer trust as well as reducing operational liability, sustaining revenue, and protecting brand and proprietary information for City of Charlotte.

For this project, we will conduct a thorough ASB assessment of City of Charlotte network and support mandated annual PCI Cybersecurity PenTesting requirements. The resulting ASB will accurately identify and help remediate any discovered vulnerabilities by integrating Business Context, Tailored Threat Intelligence, and a "*Think Like the Adversary*" mindset. root9B will tailor all its activities to meet the objectives, priorities, requirements, and network configurations needed to maintain confidence in City of Charlotte network security and satisfy PCI DSS reporting requirements.

04.1 Point of Contact

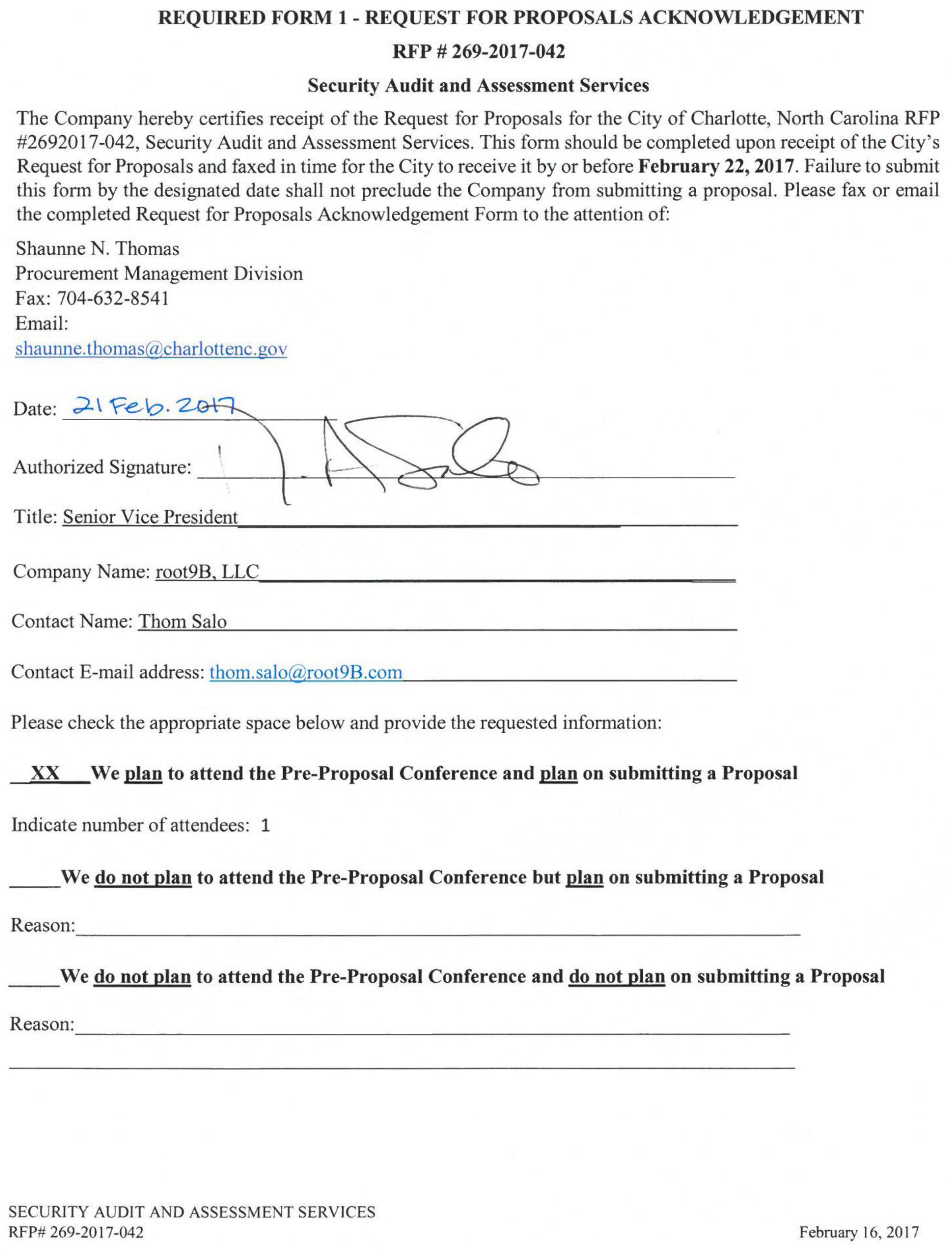
If you have any questions, please contact:

Tony C. Dillingham
Client Executive, root9B
Direct: 704-227-3872
E-mail: Tony.Dillingham@root9b.com
Colorado Springs | San Antonio | Manhattan | Charlotte | Annapolis Junction | Honolulu | Boise

SECTION 6
REQUIRED FORMS

Intentionally Left Blank

Required Form 1 – REQUEST FOR PROPOSALS ACKNOWLEDGEMENT



REQUIRED FORM 1 - REQUEST FOR PROPOSALS ACKNOWLEDGEMENT

RFP # 269-2017-042

Security Audit and Assessment Services

The Company hereby certifies receipt of the Request for Proposals for the City of Charlotte, North Carolina RFP #2692017-042, Security Audit and Assessment Services. This form should be completed upon receipt of the City's Request for Proposals and faxed in time for the City to receive it by or before **February 22, 2017**. Failure to submit this form by the designated date shall not preclude the Company from submitting a proposal. Please fax or email the completed Request for Proposals Acknowledgement Form to the attention of:

Shaunne N. Thomas
Procurement Management Division
Fax: 704-632-8541
Email:
shaunne.thomas@charlottenc.gov

Date: 21 Feb. 2017

Authorized Signature: ______________________________

Title: Senior Vice President

Company Name: root9B, LLC

Contact Name: Thom Salo

Contact E-mail address: thom.salo@root9B.com

Please check the appropriate space below and provide the requested information:

__XX__ **We plan to attend the Pre-Proposal Conference and plan on submitting a Proposal**

Indicate number of attendees: 1

_____ **We do not plan to attend the Pre-Proposal Conference but plan on submitting a Proposal**

Reason: ______________________________

_____ **We do not plan to attend the Pre-Proposal Conference and do not plan on submitting a Proposal**

Reason: ______________________________

____

Section 6
Required Forms

Required Form 2 - ADDENDA RECEIPT CONFIRMATION

RFP # 269-2017-042

Security Audit and Assessment 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.

ADDENDUM #:	DATE ADDENDUM DOWNLOADED FROM NC IPS:
#1	6 March 2017
#2	27 March 2017

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)

10 April 2017
Date

Authorized Signature

COO
Title

root9B, LLC
Company Name

Section 6
Required Forms

Required Form 3 - PROPOSAL SUBMISSION FORM

RFP # 269-2017-042

Security Audit and Assessment Services

This Proposal is submitted by:

Company Name: root9B LLC

Representative (printed): John Harbaugh, Chief Operating Officer (COO)

Address: 102 North Cascade, Suite 220.

City/State/Zip: Colorado Springs, CO, 80903

Email address: John.Harbaugh@root9B.com

Telephone: 443-758-0538
(Area Code) Telephone Number

Facsimile: None
(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. 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, religion, national origin, marital status, familial status, sexual orientation, gender identity, gender expression 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*.
2. 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 bid submitted by the Bidder on this Project and to terminate any contract awarded based on such bid.
3. 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 bid.
4. 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 Company in a legal or administrative proceeding alleging that Company discriminated against its subcontractors, vendors or suppliers, and a description of the status or resolution of that complaint, including any remedial action taken.

5. 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.

6. 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 re-bid this RFP.

7. 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 Terms as included herein as Exhibit A. As such, I have elected to do the following:

___ Include exceptions to the sample contract in the following section of my

Proposal:_______ __x_ Not include any exceptions to the Sample Terms.

Representative (signed): ____

Required Form 4 - PRICING WORKSHEET

RFP # 269-2017-042

Security Audit and Assessment 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 rounded to the nearest quarter of a dollar. **If there are additional costs associated with the Services, please add to this chart. Your Price Proposal must reflect all costs that the City will be responsible for.**

Security Audit and Assessment: Milestone Pricing Plan			
Milestone			**Cost**
1.0		**Initial Engagement**	
1.1		**Deliver assessment report on PCI DSS SAQ D environment**	$ 39,112.50
1.2		**Deliver assessment report on two PCI DSS SAQ C environments**	$ 28,875.00
1.3		**Deliver internal penetration testing report on 150 active IP addresses**	$ 18,134.50
1.4		**Deliver external penetration testing report on 100 active IP addresses**	$ 18,134.50
1.5		**Deliver penetration testing report on 100 web applications**	$ 1,383,096.00
1.6		**Deliver group policy security assessment report on 150 Group Policy Objects (GPO)**	$ 22,668.00
1.7		**Deliver Active Directory (AD) security assessment report on 10 domains and 500 groups**	$ 104,073.50
1.8		**Deliver Domain Name System (DNS) security configuration audit report on 10 DNS servers**	$ 16,498.25
		TOTAL COST:	**$ 1,630,592.25**
2.0		**Annual Services**	**Period = 1 Year**
2.1		**Deliver assessment report on PCI DSS SAQ D environment**	$ 39,112.50 / year
2.2		**Deliver assessment report on two PCI DSS SAQ C environments**	$ 28,875.00 /year
2.3		**Deliver internal penetration testing report on 150 active IP addresses**	$ 18,134.50 /year
2.4		**Deliver external penetration testing report on 100 active IP addresses**	$ 18,134.50 /year
		TOTAL COST:	**$ 104,256.50 /year – assumes one service each per year**

3.0		Ad-hoc Services	COST per Engagement
3.1		Deliver assessment report on PCI DSS SAQ D environment	$ 39,112.50 /engagement
3.2		Deliver assessment report on PCI DSS SAQ C environment	$ 28,875.00 /engagement
3.3		Deliver internal penetration testing report on 100 active IP addresses	$ 18,134.50 /engagement
3.4		Deliver internal penetration testing report on 500 active IP addresses	$ 27,201.50 /engagement
3.5		Deliver internal penetration testing report on 2,500 active IP addresses	$ 31,735.25 /engagement
3.6		Deliver internal penetration testing report on 5,000 active IP addresses	$ 40,802.50 /engagement
3.7		Deliver external penetration testing report on 1 active IP address	$ 8,226.50 /engagement
3.8		Deliver external penetration testing report on 25 active IP addresses	$ 8,226.50 /engagement
3.9		Deliver external penetration testing report on 100 active IP addresses	$ 24,724.50 /engagement
3.10		Deliver penetration testing report on 1 web application	$ 19,350.25 /engagement
3.11		Deliver penetration testing report on 25 web applications	$ 376,887.50 /engagement
3.12		Deliver penetration testing report on 100 web applications	$ 1,498,970.00 /engagement
3.13		Deliver wireless security assessment report on 1 physical location (site) with 10 access points	$ 16,498.25 /engagement
3.14		Deliver wireless security assessment report on 1 physical location (site) with 150 access points	$ 24,724.75 /engagement
3.15		Deliver group policy security assessment report on 150 Group Policy Objects (GPO)	$ 16,498.25 /engagement
3.16		Deliver Active Directory (AD) security assessment report on 10 domains and 500 groups	$ 106,713.50 /engagement
3.17		Deliver Domain Name System (DNS) security configuration audit report on 10 DNS servers	$ 16,498.25 /engagement
3.18		Deliver server security configuration audit report on 100 servers	$ 16,498.25 /engagement
TOTAL			**$2,319,677.75 / all engagements (Assumes 1 service each)**

Required Form 5 – M/W/SBE UTILIZATION

RFP # 269-2017-042

Security Audit and Assessment 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 LLC

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

____ MBE ____WBE ____SBE __X__ 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: The U.S. Small Business Administration, SBC_000890731 Effective Date: 19 February 2016 Expiration Date: N/A

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):

root9B conducted an exhaustive search of small businesses (of any type) to identify potential partners offering equal or superior cybersecurity services or technologies to root9B. With the exception of NDB, a small business who will provide niche PCI QSA support, root9B 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):

root9B 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 root9B. 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 #
TBD	MWSBE companies providing equal or better cybersecurity services to root9B or who provide niche cyber services not available through root9B may be assessed and added to the root9B Team	TBD	TBD

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

Representative (signed): ______________________

16 April 2017
Date

John Harbaugh
Representative Name

Required Form 6 – COMPANY'S BACKGROUND RESPONSE

RFP # 269-2017-042

Security Audit and Assessment 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).	Colorado Springs, CO
How many years has your company been in business? How long has your company been providing the Services as described in Section 3?	root9B was founded in July 2011. We have been providing equivalent cybersecurity services six (6) 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).	root9B in conjunction with CISCO conducted a fourteen (14) day (1-14 Aug 2014) Proof of Value (POV) for Bedford County, VA to demonstrate our ability to identify and effectively eradicate already present, previously unidentified threats to Bedford County and thwart potential future malicious activity. During the POV root9B sent specialized cyber operators into Bedford County's network to hunt, identify, stop, and remove intruders that existing passive security solutions did not detect. Real-time HUNT operations identified signs of planned and active attacks and took action to neutralize them. root9B helped the customer identify two critical city services that were believed to be entirely separate and impenetrable for an outside malicious attack. Our Penetration Testing provided evidence that these essential services were vulnerable. Our analysts provided remediation recommendations designed to harden these and other Bedford Country networks. Additional citations are provided in **Section 6 Required Form #7 References**
List any projects or services terminated by a government entity. Please disclose the government entity that terminated and explain the reason for the termination.	None
List any litigation that your company has been involved with during the past five (5) years for Services similar to those in this RFP.	None
Provide an overview and history of your company.	Started in 2011 root9B has become is an industry-changing provider of advanced Cybersecurity products and services for the U.S. Government and Fortune 500 retail, banking, financial, utility, higher education, and medical Clients. Using credentials established supporting

	the Pentagon and U.S. Intelligence Community, root9B has become a "pure play" provider of advanced Cybersecurity operations, training, consulting services, and associated technologies. root9B stands in defiance of the unwanted human presence within our clients' networks by attacking the root of the problem—the adversary's ability to gain entry and remain undetected. root9B's application of advanced technology developed through cutting-edge Research and Development (R&D) and engineering and leveraging intelligence-community cyber tradecraft is revolutionary. This unique application of technology, tactics development, specialty tools, and deep mission experience to effectively locate, identify, track and defeat Cyber threats has led the company's successful climb to its current position as the #1 company on Cybersecurity 500's world's hottest and most innovative Cybersecurity firms for 2016. (http://Cybersecurityventures.com/Cybersecurity-500/)
If your company is a subsidiary, identify the number of employees in your company or division and the revenues of proposing company or division.	root9B LLC is a subsidiary of root9B Holdings. root9B LLC currently has 85 employees with an annual revenue for 2016 of approximately $5M.
Describe your company's complete corporate structure, including any parent companies, subsidiaries, affiliates and other related entities.	root9B LLC is a subsidiary of root9B Holdings. root9B LLC's sister company is IPSA International. IPSA specializes in consulting and investigations related to complex financial crime and intellectual property. root9B Holding oversees both root9B LLC and IPSA.
Provide a management organization chart of your company's overall organization, including director and officer positions and names and the reporting structure.	root9B's organizational structure, listing all directors and officer positions including names is provided in **Attachment 1.**
Describe the key individuals along with their qualifications, professional certifications and experience that would comprise your company's team for providing the Services.	A summary of key personnel available to support this effort are listed in **Attachment 2**
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.	N/A – With the exception of PCI QSA services, root9B anticipates providing all services required to support the City of Charlotte. Specialized niche services such as as PCI QSA will be provided by our partner NDB Accounting. Should additional services beyond the operational or technical capacity of root9B be required, we will leverage our extensive outreach within the cyber community to provide these services.

Explain how your organization ensures that personnel performing the Services are qualified and proficient.	root9B is committed to ensuring team members are trained and qualified to excel within their respective areas of responsibility. root9B's standard practice is to continually evaluate employee skills and provide necessary mentoring and training to ensure they are proficient with the latest Cybersecurity capabilities and approaches. We place equal emphasis on who the current threat actors may be, their motivations, sophistication, unique threat signatures, and recent or current Tactics, Techniques, and Procedures (TTPs). We steadfastly support ongoing professional development and training of all staff members. Finally, root9B regularly schedules Cybersecurity roundtables and workshops to share new developments and changes in the ever-evolving, ever-changing arena of Cybersecurity.
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.	root9B and NDB Accounting anticipate providing the bulk of our services remotely from our facilities in Colorado Spring, CO, and Atlanta, GA respectively. On-site (in Charlotte) activities will be limited to PCI assessment, internal and wireless testing. Staffing levels for both on-site and off-site will be commensurate with the specific requirements and scope of the associated activity
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.	Our physical security posture is deployed with an industry standard 'defense-in-depth' practices. This starts at our front door, where regular employee access is controlled through electronic locking system and a token to access the door. Areas that receive non-employees, visitors, shipping, etc., are on a scheduled timer that will provide access to a manned reception area during normal working hours. Spaces inside the company that are restricted due to equipment or data processing sensitivities are also protected by a swipe and further restricted for all but authorized personnel (such as system administrators or forensic analysts). Data wiring is installed in accordance with NEC code in conduit or J-hooks in our plenum areas, where it is easily inspect-able. Ingress/egress to all root 9B areas are monitored 24 hours by video recording systems that capture and offsite all accesses for review if needed. The offsite is a third party capture service that we have under contract for our video processing requirements

Section 6
Required Forms

Required Form 7 – REFERENCES

RFP # 269-2017-042

Security Audit and Assessment 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: VF Corp* **Phone:** (336)-424-7762

(* *VF Corporation is a $12B+ Fortune 500 corporation whose portfolio of brands includes such iconic names as: Rustler, Wrangler, Lee, Vans, Northface, Timberland, Jansport, Riders, EastaPak, Nautica, Ella Moss, Majestic, Smartwool, Eagle Creek, Kipling, Reef, Red Kap, Bulwark'FR, Horace Small, Splendid, Lucy, 7 for All Mankind, and Napapijri)*

Address: 105 Corporate Center Drive Boulevard Greensboro, NC

Primary Contact: Ed Harris **Title:** Manager of Security Operations

Phone: (336)-424-7762 **E-mail address:** ed_harris@vfc.com

Service Dates: 1 Oct 2014 – 30 Sept 2017

Summary & Scope of Project

root9B provides comprehensive ASB services accompanied by Active Adversary Pursuit (HUNT) and Incident Response (IR) operations to identify, stop, and remove intruders attempt to access the multiple integrated company networks that comprise VF Corporation's (VF Corp) extensive corporate network infrastructure.

Operating within the client's networks, root9B continuously and actively hunts for, detects, and remediates intrusions by advanced attackers that might otherwise go undetected by traditional network defense solutions. This is achieved by conducting full spectrum Defense Cyber Operations that provide assessment, analysis, design, and monitoring of the client's current and proposed infrastructure. The driving objective of this program is to identify all vulnerabilities, enumerate adversary attack surface, estimate exploitation risk and impact, and provide remediation services for affected devices, or autonomous information systems. The work includes client requested support to cyber defense planning, as well as incident response. Specific program service elements include:

» Attack Surface Baseline (ASB) – root9B delivers full spectrum network penetration testing, vulnerability assessments, and comprehensive cybersecurity program assessment, analysis, design, and monitoring of current and proposed infrastructure VF Corp. We identify pertinent vulnerabilities, enumerate adversary attack surfaces, estimate exploitation risk and impact, and provide remediation recommendations for information systems and affected end point devices.

  During the initial phases of the program we conducted a deep-dive analysis of VF Corp's networks, created the threat intelligence baseline that provides a foundation for all subsequent cybersecurity activities. PenTesting focused on Password Cracking, Router Testing, Denial of Service (DOS) Testing, and Distributed DOS testing. The results of the ASB effort included: actionable reporting, Cybersecurity enhancement, mitigation, and remediation recommendations. The resulting ASB report included a discussion of the tools used, steps performed, vectors, and exploited vulnerabilities that may lead to penetration, as well as vulnerabilities that were not exploitable but which are deemed to pose a potential risk to VFC operations

- Remote Active Adversary Pursuit (HUNT) – Direct HUNT support to VF Corp focuses on enterprise vulnerability identification and mitigation, and active pursuit of adversaries and discovery of adversary movement artifacts within the VF Corp network missed by their automated enterprise cyber defense suite.

  root9B conducted operations and a detailed forensic investigation for VF culminating with the discovery of a compromised host being used to spearfish clients. Operations in another segment of the network discovered two pieces of malware, which were undetected by current anti-virus and network monitoring tools.

- Incident Response (IR) Retainer - root9B analysts have been called to address multiple VF IR incidents. Our engagement, often within minutes of an indicator of an IR event, ensured that thousands of VF systems in its network remain healthy and productive.

Operating together, root9B's ASB, HUNT, and IR services recorded many successful engagements to include stopping malware not identified by McAfee, an advanced spearfishing campaign, a compromised web server in Southeast Asia, and multiple Point of Sale (POS) attack vectors affecting thousands of POS devices.

REFERENCE 2:

Name of Client: XPO Logistics **Phone:** 336-447-2795

Address: Five American Lane, Greenwich, CT 06831

Primary Contact: Lateek Wille **Title:** Executive Dir IT Security Engineering & Operations, XPO Logistics Supply Chain

Phone: 336-447-2795 **E-mail address:** Lateek.Willie@xposc.com

Service Dates: 2 Nov 2015 – 16 Dec 2015

Summary & Scope of Project

root9B performed Attack Surface Baseline (ASB) External and Internal Vulnerability Assessment and Penetration Testing. root9B conducted penetration testing consisting of External Network Penetration Test(s) and Internal Network Penetration Test(s). We incorporated industry standard and tailored penetration techniques designed to methodically test XPO LOGISTICS cybersecurity posture. Through these methods, root9B evaluated the current network-operating environment and ascertained the need for additional network defense mechanisms including remediation and additional network monitoring capabilities.

Our external network penetration tests were conducted without any access assistance from XPO LOGISITICS to validate perimeter security controls. Subsequent External Network Penetration testing included limited remote access into its customer environment to simulate a customer's attempt to gain unauthorized network access. Our Internal Penetration testing included simple LAN access, valid user account access, guest wireless access, and system access to validate the effectiveness of user account, file/directory, and access control safeguards. Additionally, our penetration testers attempted to gain access to targeted systems and critical network segments by circumventing existing XPO LOGISTICS safeguards.

REFERENCE 3:

Name of Client: Duke Energy **Phone**: 980-373-3555

Address: 550 South Tryon Street, Charlotte, NC 28202

Primary Contact: Hafid Elabdellaoui **Title:** Managing Director IT Security & Compliance

Phone: 704-382-0350 **E-mail address:** Hafid.Elabdellaoui@duke-energy.com

Service Dates: 31 August 31, 2015 through March 29, 2016

Summary & Scope of Project

oot9B was awarded a contract to provide cybersecurity Penetration Testing and Vulnerability Assessments for one of the largest electric and nuclear power holding companies in the United States. The primary testing objective is to identify all pertinent vulnerabilities, enumerate the adversary attack surface, estimate exploitation risk and impact, and provide remediation services for affected devices, or autonomous information systems. Our analysis is conducted using various threat models to emulate financially motivated cybercriminals and state-sponsored 'Advanced Persistent Threat' attackers.

root9B conducts a broad range of technical and "non-technical" cybersecurity assessment services to Duke Energy to include:

» Cybersecurity Infrastructure Design Assessment - root9B conducted a full spectrum Network Defense and Enterprise Security Infrastructure Assessment to analyze the overarching security posture of the Utility's current cybersecurity infrastructure design, implementation, and procedures. This analysis assessed the overall security posture of the organization's deployed Cybersecurity capabilities, processes and procedures, and network security architecture. The primary objective was to provide a tabletop cybersecurity network design analysis to fully evaluate the architecture and implementation of HP Security Voltage.

» Threat Intel and Vulnerability Baselining – root9B initially identified the Utility's external attack surface by performing Open Source Intelligence (OSINT), social media analysis, Footprinting, Scanning, and Enumeration activities. Together with the Infrastructure Design Assessment root9B identified enterprise-level cybersecurity infrastructure and design vulnerabilities, adversary attack surfaces, estimated exploitation risks and impact, and provided recommendations for affected devices, security infrastructure design, or autonomous information systems.

» Penetration Testing – root9B tested the effectiveness of the Utility's external security posture and control. Our operators also tested the effectiveness of the network from an isolation and segmentation standpoint. Where root9B was able to penetrate the Utility's defenses, we simulated activities to compromise systems and attempt to obtain confidential or sensitive data. As part of the scanning process, root9B provided information relating to all identified vulnerabilities (to include open TCP/UDP ports) on each of the new production network internal devices. Each identified machine having an exploitable vulnerability was thoroughly analyzed and documented in a full remediation plan, which was part or root9B's Cyber Threat Assessment report.

» Social Engineering – root9B conducted operations to obtain system credentials by using non-technical social engineering techniques such as targeted calls, creation of fake users through LinkedIn or other social media and directed these attacks to help desk and other high profile employees. root9B also employed other techniques to include spearfishing, and manipulation to create targeted and realistic attack environments.

root9B continues to provide cybersecurity services to include ongoing vulnerability assessments and recommendations on how to fix any identified weakness of improve the Utility's overall security posture.

REFERENCE 4:

Name of Client: University of Washington **Phone:** 206-685-5145

Address: Brooklyn Ave, University of Washington Tower Building C (UWTC), Seattle WA

Primary Contact: Brandon Vinroe **Title:** Info Security Consulting Manager Office of The CISO

Phone: 206-685-5145 **E-mail address:** vinroeb@uw.edu

Service Dates: 1 Oct 2015 through 31 Sept 2019

Summary & Scope of Project

root9B is providing the University of Washington with security assessments primarily in the form of Task Order driven Penetration Testing and Vulnerability Assessments. On this and our other Penetration Testing and Vulnerability Assessment programs, root9B's approach is unique. By initially determining the Business Context that the University of Washington's security we are able to establish a security baseline for their critical components.

Recent individual task orders being conducted under this contract include:

- To help University of Washington protect its $15M annual donations program, root9B is conducting web application testing of two University of Washington donor websites to expose security vulnerabilities that may make a donor or potential donor susceptible to a breach of Personal Identifiable Information (PII) or credit card information theft.
- root9B is conducting a security assessment of the university's new parking system. This assessment will evaluate the newly implemented gated facilities and associated software for security vulnerabilities and implementation problems. The proposed assessment includes a best practices review focused on governance, an overall security architecture review, an optional threat assessment, as well as recommendations for improved system implementation planned for later implementation phases.
- root9B will conduct Website Penetration Testing and Vulnerability Assessment identifying and mitigating security vulnerabilities in applications and websites used by the University of Washington Division of Enrollment Management.

root9B's post assessment and test "Cyber Threat Assessment Report" provides the University of Washington with a detailed adversary attack narrative based on identified vulnerabilities, network misconfigurations, anomalous activity, network maps, and application security. The report includes guidance and recommendations for remediation and hardening of network infrastructure as well as identifying regulatory compliance or architectural best practice weaknesses

REFERENCE 5:

Name of Client: Orlando Longwood Auto Auctions (OLAA) **Phone:** 407-491-4433

Address: x

Primary Contact: Joe Weinstein **Title:** Director of Information Technology

Phone: 407-491-4433 **E-mail address:** Jweingstein105@me.com

Service Dates: 18 – 21 Jan 2017

Summary & Scope of Project

Orlando Longwood Auto Auctions (OLAA) was hit with a virulent strain of CRYSIS ransomware that encrypted key operational systems and supporting databases. The Client attempted to recover using backups of these components only to see their systems become re-infected immediately after each restoration attempt.

OLAA then contacted root9B and within 72 hours, we identified the malware and the associated attack vector. We provided the Client with a remediation strategy to fully restore their operations and ensure that the malware was permanently removed. Using the proposed strategy, we worked with OLAA to help verify that all systems were on-line and operational.

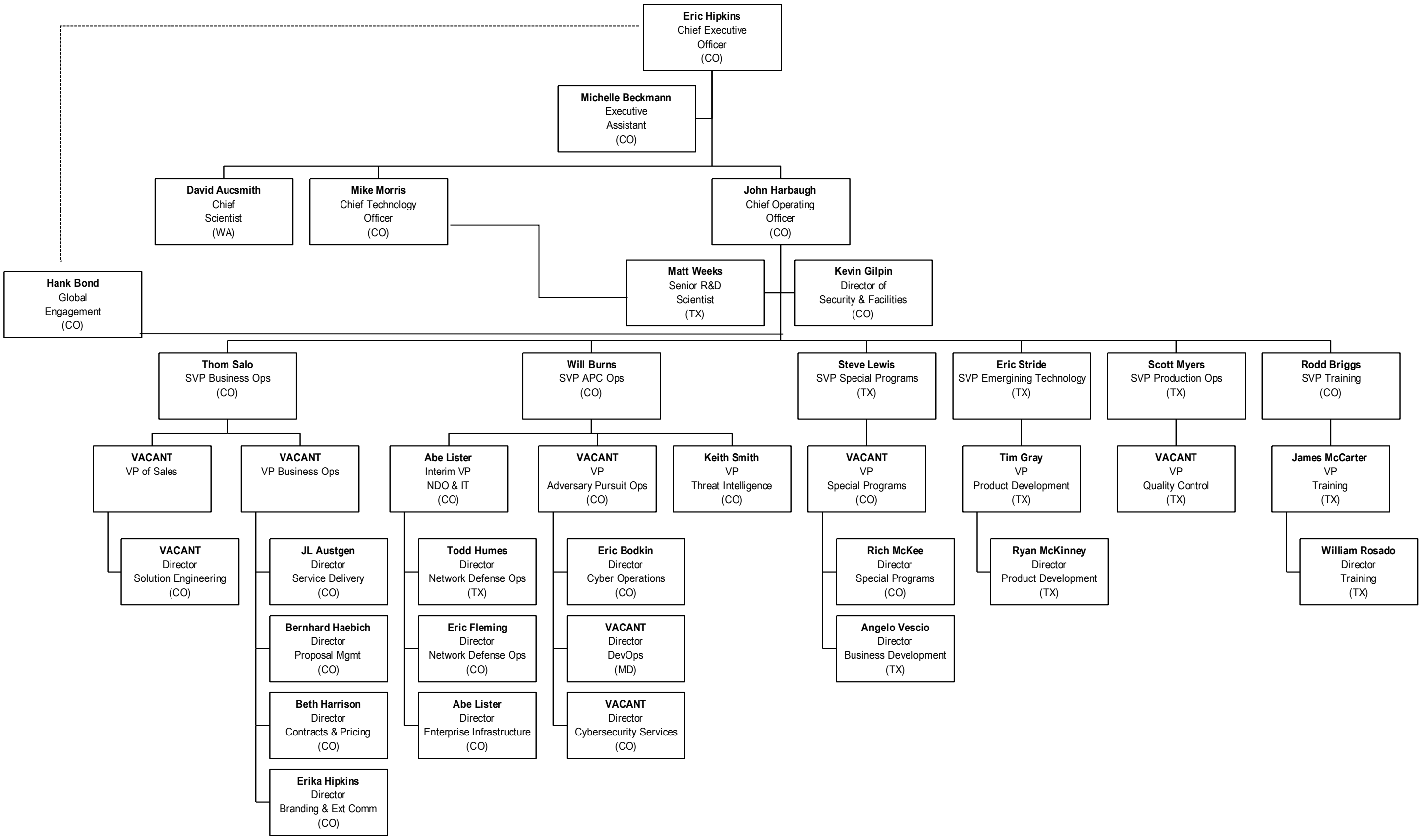
The rapid resolution of this attack allowed OLAA to conduct a scheduled sales event valued at $16M three days after initial contact with root9B.

Section 6
Required Forms

ATTACHMENTS

Intentionally Left Blank

Attachment 1 - root9B's organization structure



Intentionally Left Blank

Attachment 2 – Key root9B Staff

Recognized and respected by peers across the Intelligence Community, root9B is comprised of subject matter experts in the field of advanced offensive and defensive cyber operations. Our personnel are routinely tasked with the most advanced and challenging operations within critical mission areas. root9B combines cutting edge technology, tactics development, and vast mission experience with a focus on emerging threats to continuously position us ahead of the adversary. As a result, root9B is able to offer clients premier cybersecurity consulting services, advanced cyber operations and forensics training, cyber threat and risk detection assessments, and complex cyberspace range operations. With thousands of "real-world" operational experiences in the cyberspace domain, root9B professionals continue to perfect cyber operations tradecraft and routinely solve complex problem sets for the dynamically charged world of cybersecurity.

William Burns – Senior Vice President and Director of Operations

Years of Applicable Professional Experience	• 20 Years
Education	• Easter Michigan University, Masters Of Science MSTA/LA Offensive Computer Security Program - 15 Of 31 Credit Hours Completed
Certifications	• Certified GIAC Intrusion Detection Analyst – 08/2006 • Certified Information Systems Security Professional (CISSP) 2005 • Cisco Certified Network Associate –/2003 • Microsoft Certified Systems Engineer –1997
Security Clearance	• Top Secret/SCI Clearance with Polygraph – 03/2015

Will Burns leads root9B's Adversary Pursuit Center and Threat Intelligence operations. He is an expert in the cyber security field with over 20 years of information technology experience. For the Marine Corps, and the National Security Agency (NSA) Mr. Burns was the Technical Team Lead for Red Team Assessments. He conducted Red Team Assessments against every major Department of Defense (DoD), and Combat Command network. Mr. Burns was the originator of the Master Operator Program at the NSA. He was also the Technical Director and Mission Director of their Remote Operations Center with oversight and risk management of all cyber operations. He has been certified as a Microsoft Certified Software Engineer (MCSE), Cisco Certified Network Associate (CCNA), Certified Information Systems Security Professional (CISSP), and GIAC Intrusion Detection Analyst. He has developed Graduate level content for the University of Eastern Michigan Masters of Science Offensive Computer Security Program, and awarded the AFCEA Copernicus Award for advancements in the field of Cyber Operations.

Eric Bodkin - Director of Cyber Operations

Years of Applicable Professional Experience	12 Years
Education	• Bachelor of Arts – Finance, Southern Methodist University, 2015
Certifications	• GIAC Certified Forensic Examiner (GCFE) • GIAC Certified Forensic Analyst (GCFA)

Years of Applicable Professional Experience	12 Years
	• Certified Information Systems Security Professional (CISSP)
Security Clearance	• Top Secret SCI

As the Director of root9B's Cyber Operations Eric applies his 12 years of experience to lead the technical execution of Active Adversary Pursuit (HUNT) and traditional network defense services. He directs and conducts full-scope penetration tests, advanced adversarial pursuit (HUNT) operations, and incident response and remediation efforts for root9B clients. He is also the key developer and instructor for multiple industry leading Offensive and Defensive Cyber Operations courses focused on preparing and mission qualifying U.S. Government and Military units for Computer Network Operations (CNO). Prior to joining root9B, was a senior operator at the National Security Agency (NSA). He was also a Technical Lead for NSA's Computer Network Operations (CNO) operator training pipeline and spent time conducting malware analysis and intelligence reporting. Since joining root9B in 2014, he has led full-scope penetration tests, adversary pursuit (HUNT) operations, and incident response and remediation efforts across some of the most sensitive and targeted networks globally, including Fortune 500 clients, the US Government, major utilities, higher education institutions, and the Department of Defense. Eric is the primary technical contributor to all company products.

Eric Flemming - Technical Director

Years of Applicable Professional Experience	18 Years	
Education	• BS, Computer Science, Colorado Technical University, 2014	
Certifications	• RHCE • CTT+ • Security+	• Network+ • Linux+ • CEH
Security Clearance	• Top Secret SCI clearance with CI	

Accomplished intelligence professional with 17 years of experience in cyber warfare serving as a Senior Army Information Operations Intelligence Professional and Senior Cyber Security Engineer. Skilled penetration tester, security researcher, developer and trainer of advanced cyber courses. Seasoned cybersecurity operator and capability developer having performing numerous assessments and developed sophisticated exploits to some of the Nation's most challenging problems. Army career as Signals Intelligence Analyst primarily spent under the NSA/CSS umbrella. Currently the Director of Adaptive Network Defense Operations and Technical Director for root9B in Colorado Springs, CO. Responsible for providing Threat Intelligence, Detection and Response services. Leads technology innovation and research. Directed the company's strategic direction, development and future growth. Member of IEEE Computer Society (IEEE), Association for Computing Machinery (ACM), InfraGard National Members Alliance(INMA), Association of Information Technology Professionals (AITP), Internet Engineering Task Force (IETF).

Todd Humes - Director of Information Technology / Director - Network Defense Operations (NDO)

Years of Applicable Professional Experience	16 Years
Education	• Bachelors of Applied Science, Wayland Baptist University, Cum Laude, 2013
Certifications	• VMware Certified Associate – Data Center Virtualization (VCA-DCV), Oct 2013 • Information Technology Infrastructure Library (ITIL) v3 Foundation, Oct 2011 • Red Hat Certified Systems Administrator (RHCSA), Sep 2011 • CompTIA Security + (SYO-201), Dec 2010
Security Clearance	• Top Secret SCI Full Scope Polygraph

Sixteen years of information technology experience, supporting various multi-architecture mission platforms for the intelligence community and the Department of Defense. Currently leads root9B IT system security architecture, and oversight of all IT systems; handles requirements towards the planning, installation, configuration, integration, management, and documentation of on-site and geographically dispersed systems. Company lead for all NDO/MSS engagements. Extensive experience formulating and implementing complex information system solutions with an emphasis on security, virtualization, administrative automation, and cost savings. Extensive experience with establishing, configuring, and maintaining various virtualization infrastructures (VMware/OpenStack), Operating Systems (Windows/Linux/UNIX), underlying GOTS/COTS applications, networking components (Cisco/Juniper/HP/Dell/F5 Networks), Storage Arrays (EMC/NetApp), and clustered computing environments. Experience constructing various scripting-language programs (UNIX shells, Windows PowerShell, Python, Perl, Tcl). Experience in computer system and network analysis, utilizing various security products, to include but not limited to: (Nessus, Retina, Statseeker, Cisco FirePOWER Intrusion Prevention System (IPS) / Intrusion Detection System (IDS), Cisco Prime Network Analysis Module (NAM), Snort, Splunk, Logstash, Snare/Epilog, Nmap, Ziften, Nagios, Wireshark, R-Studio, Kali, CAINE). Understands and applies commonly known security practices and possess a working knowledge of applicable industry controls such as NIST 800-53, ISO 27002, PCI, SSAE 16, and CIS.

Chris Sterbank - Cyber Threat Analyst / Vulnerability and Penetration Testing Lead

Years of Applicable Experience	12 Years
Certifications	CISSP - Certified Information Systems Security Professional, 2011 GIAC Penetration Tester (GPEN) Certification, 2011 GIAC Security Essentials (GSEC) Certification, 2010 CompTIA Security+ Certification, 2008
Professional Training	Intermediate Network Warfare Training, Hurlburt Field, FL 2011 Undergraduate Network Warfare Training, Hurlburt Field, FL, 2010
Security Clearance	Top Secret/SCI

Information Systems and Network Security Specialist with 12 years of professional experience. Key member of root9B operations team responsible for multiple areas of expertise, including host based forensics/analysis, penetration testing, and holistic network security reviews. Performs vulnerability analysis, penetration testing, and provides remediation recommendations for Fortune 500 customers against industry standards/frameworks such as NIST 800-

53 and OWASP Top 10. Proficient in log and packet capture analysis, penetration testing methods and network defense. Advanced knowledge of protocols and operating systems invaluable to intrusion analysis. Exceptional ability to develop, analyze and deploy standardized network security policies. Subject matter expert with proven ability to effectively train others on information technology

James Krainock - Senior Forensics Investigator

Years of Applicable Experience	• 12 Years
Education	• BA Computer Science, Mesa Community College, 1993
Certifications	• Forensic Computer Examiner • Private Investigator
Security Clearance	• None

Digital Forensics Specialist and Licensed Private Investigator with extensive experience in the fields of digital investigations and computer forensics working with law enforcement at the international, federal, state and local levels, and in the private sector. Manages root9B's in-house digital forensics capabilities and is the creator of processes and procedures to ensure customer forensic readiness throughout root9b's cyber security product offering. Architect of integrated forensic capture and analysis capabilities in root9b's proprietary cyber HUNT program allowing its cyber security analysts to forensically capture remote system artifacts to more efficiently identify and respond to cyber threats and incidents. Has worked in development of specialized digital forensic hardware, software and training for law enforcement engaged in child exploitation investigations, and has trained hundreds of forensic examiners and investigators in optical media forensics and image/video analysis. As a private sector partner Mr. Krainock has worked closely with government and law enforcement officials on international projects and initiatives to advance the capability of international child exploitation investigation. A member of the International Association of Computer Investigative Specialists, an internationally accredited forensic training and certification organization. Licensed Private Investigator by the State of Colorado.

James McCarter – VP for Training /Senior Threat Analyst

Years of Applicable Experience	• 12 Years
Security Clearance	• Top Secret
Education	• BS Liberal Arts, Excelsior College, 2014 (Cum Laude) • AS Engineering Track, Pikes Peak Community College, 2011 • AA, Korean, Defense Language Institute, 2006
Certifications	• Cellebrite Certified Instructor • ADF Triage-G2 Instructor • Computer Forensics & Digital Investigations Certificate, Champlain College, 2014 • Cybersecurity Certificate, Champlain College, 2015 • Security Fundamentals Certificate, Champlain College, 2015

Years of Applicable Experience	• 12 Years
	• Sensitive Site Exploitation (SSE) • Field Forensics EL100, EL230 Explosive Residue Detection

Talented security professional as a Marine Corps Signals Intelligence NCO and Mobile Technologies Technician and Instructor with twelve (12) years of leadership experience and security expertise in support of the Intelligence Cycle. Certified Cellebrite UFED Ultimate Mobile Forensics Instructor and certifying authority having taught hundreds of students. Regarded by prior colleagues and managers to be critical to support operations and to be tremendously adaptive and tenacious in strategic planning, creative problem solving and team building. Developed a successful track record and reputation for dealing with customers with the utmost professionalism while continuously working to find cost effective but top quality solutions

From: Beth Harrison
To: Thomas, Shaunne
Cc: Beonde, Amelia; Jones, Adam; John Harbaugh; Thomas Salo
Subject: RE: 269-2017-042 Security Audit and Assessment Services - Confidentiality Disclaimer
Date: Friday, May 19, 2017 11:58:55 AM

Shaunne–

root9B confirms that it has no objections to a release of the subject proposal in response to any public records request the City may receive. The company therefore does not intend to submit any redactions to its proposal.

We appreciate your inquiry. Please let me know if you have any additional questions.

Beth

Beth Harrison

Director, Contracts and Pricing

Direct: 719-600-8033

E-mail: beth.harrison@root9b.com

Web: www.root9B.com

***Please note I have a new work cell phone 719-660-8033. Please update your records accordingly.**

Colorado Springs Office: 102 N. Cascade Ave Suite 220 Colorado Springs CO 80903
Colorado Springs | San Antonio | Manhattan | Boise | Honolulu

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity named. If you are not the named addressee you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited. Please notify the sender immediately by email if you received this email in error and delete this email from your system. Any views or opinions presented in this e-mail are solely those of the author and do not necessarily represent those of root9B, LLC.

> **From:** "Thomas, Shaunne" <Shaunne.Thomas@ci.charlotte.nc.us>
> **Date:** May 19, 2017 at 04:59:34 MDT
> **To:** "john.harbaugh@root9b.com" <john.harbaugh@root9b.com>
> **Cc:** "Jones, Adam" <amjones@ci.charlotte.nc.us>, "Beonde, Amelia" <abeonde@ci.charlotte.nc.us>

Subject: 269-2017-042 Security Audit and Assessment Services - Confidentiality Disclaimer

Dear Mr. Harbaugh,

I am writing for clarification regarding a confidentiality statement on Root9B's proposal. Please note that the City is statutorily required to provide copies of proposals in response to public records requests unless materials are specifically marked as trade secrets by the proposer per section 1.6.2. (Trade Secrets and Personal Identification Information /Confidentiality of the RFP). It is not an acceptable practice for a vendor to mark its entire proposal trade secret.

Root9B has not provided a redacted version of the proposal, nor marked specific section(s) as confidential or trade secret. If it is your intent to redact specific portions of the proposal, please provide section or page references as soon as possible, bearing in mind that pricing cannot be marked as confidential. If you do not intend to redact any portion of the proposal, please confirm that you have no objections to a release of your proposal in response to any public records request the City may receive. If your intent is to mark either your entire proposal or your Form 4 Pricing Worksheet as trade secret or confidential, the City will need to consider whether it is able to continue with the evaluation of root9B's proposal.

Shaunne N. Thomas
Procurement Officer

City of Charlotte
Management & Financial Services
Finance Office – Procurement Management
600 East Fourth Street, CMGC – 9th Floor
Charlotte, North Carolina 28202-2850

shaunne.thomas@charlottenc.gov
Phone: 704.336.2933
Fax: 704.632.8541