

EMBARQ® ASSESSMENT SERVICES ANNEX

The following terms and conditions, including Exhibit A, together with the applicable Embarq cover agreement, end-user license agreement, and the Embarq Standard Terms and Conditions for Communication Services (collectively, the “Agreement”) govern Embarq’s provisioning and Customer’s use of the IP-protocol network or device security assessment services (“Services”) specified in the Agreement.

1. SERVICE OVERVIEW.

1.1. Services include security assessment and testing services described in this Annex. Embarq only provides Services on network or devices running the IP protocol. Network and devices that run non-IP protocols are excluded from the Services. Services are provided by United Teleservices, Inc., in coordination with Embarq’s third-party agent, TekSecure Labs.

1.2. Following initial discussions with Customer, Embarq will develop a statement of work (“Customer SOW”) that describes the specific Services to be performed by Embarq and applicable prices for the Services. The Customer SOW is incorporated by reference into the Agreement, and the form of the Customer SOW is attached as Exhibit A to this Annex. Embarq will provide information related to the Services on the Embarq-provided, secure web portal (“Embarq Web Portal”). Services not specifically provided for in the Customer SOW are outside the scope of the Services and will not be provided.

2. ORDER TERM. Services are provided on a one-time basis without a specific term or duration commitment. Each Customer SOW will define the scope and period in which Services are provided. Following completion of the Services described in the Customer SOW and the Agreement, any further Services must be described and agreed upon by Customer and Embarq under a separate Customer SOW and Agreement. Upon termination or expiration of the Customer SOW and Agreement, Customer agrees to return to Embarq any hardware and software (other than if Customer has purchased such hardware and software from Embarq) which Embarq has provided to Customer in connection with the Services.

3. SERVICE DESCRIPTIONS

3.1. External Target Identification. This Service is the scanning of Internet accessible host IP addresses to identify the number of targets for a specific vulnerability scan or in-depth ethical hacking. Embarq will scan IP addresses and identify active hosts on the network. This information will be used in conjunction with the Vulnerability Scanning or Ethical Hacking Services. The timeframe for delivery of all reports for these services is dependent on the scope and number of services ordered. The timeframe for delivery of all reports will be discussed with Embarq and Customer as part of the Customer SOW and implementation planning meeting.

3.2. External Vulnerability Scanning. This Service is the vulnerability scanning of IP addresses relying on the use of automated tools.

A. Scanning with Engineering Analysis

(1) After the set of Customer Internet accessible addresses is defined in the External Target Identification phase, or as defined by the Customer, Embarq will meet with Customer to determine which addresses will be included in the full vulnerability scan and in-depth ethical hacking. Vulnerability scanning identifies information about the operating system, network services, applications, and versions of those items that are active on targeted systems. After the configuration of the systems and networks is defined in more detail, exploitable vulnerabilities known to exist in those configurations are identified and documented. In addition, data collected by the tools may allow the test team to identify operating systems in use on those systems, and network service applications that are available (SMTP, DNS, HTTP, etc). External scanning (i.e. performed across the Internet) will reveal the services that are available on targeted systems from outside the Customer environment. Any vulnerabilities will be identified and documented, but will not be exploited by the Embarq team.

(2) The next phase of the vulnerability scanning process utilizes medium intensity probes to identify the versions of service applications that are in use. Identification of service application version information is useful because many vulnerabilities

contained in network applications are version specific, and knowing the version number allows specific problems to be targeted. Embarq will develop a report that recaps the vulnerability scanning process and identifies the prioritized security findings and risks with risk mitigating recommendations. The vulnerabilities and risk levels are clearly listed for the overall test, and by system. The report also includes a listing of each active system identified during the scan, and all vulnerabilities that may be found on each system. Each vulnerability listing includes a description and recommendation for corrective action.

- (3) A full vulnerability scanning report will be delivered for the entire set of systems that were included in the vulnerability scan.

B. Scanning with Automated Raw Results

- (1) After the set of Customer Internet accessible addresses is defined in the reconnaissance phase, Embarq will meet with Customer to determine which addresses will be included in the automated vulnerability scan. Automated Vulnerability scanning identifies information about the operating system, network services, applications, and versions of those items that are active on targeted systems. After the configuration of the systems and networks is defined in more detail, exploitable vulnerabilities known to exist in those configurations are identified and documented. In addition, data collected by the tools may allow the test team to identify operating systems in use on those systems, and network service applications that are available (SMTP, DNS, HTTP, etc). External scanning (i.e. performed across the Internet) will reveal the services that are available on targeted systems from outside the Customer environment.
- (2) A vulnerability scanning report will be delivered for the entire set of systems that were included in the automated vulnerability scan.

3.3. PCI Scanning. This Service is the scanning of IP addresses and reporting based on the requirements of an approved scanning vendor per the payment card industries (“PCI”) security council.

- A.** Embarq will provide a vulnerability scanning service certified as PCI compliant by the PCI Security Council, which is also recognized by MasterCard, Visa, American Express, and Discover.
- B.** Customer provides an initial list of Internet accessible IP addresses targeted for vulnerability scanning. Embarq will verify that the list is comprehensive using PCI compliant network discovery techniques. The scans identify IP addresses that are active on the network, and information about the operating system, network services, applications, and versions of those items that are active on targeted systems. After the configuration of the systems and networks is defined in more detail, exploitable vulnerabilities known to exist in those configurations are identified and documented. In addition, data collected by the tools may allow the test team to identify operating systems in use on those systems, and network service applications that are available (SMTP, DNS, HTTP, etc). External scanning (i.e. performed across the Internet) will reveal the services that are available on targeted systems from outside the Customer’s environment. Any vulnerabilities will be identified and documented, but will not be exploited by the Embarq team.
- C.** The next phase of the vulnerability scanning process utilizes medium intensity probes to identify the vulnerabilities and the recommended remediation procedures for eliminating these vulnerabilities.
- D.** Embarq will develop a report that recaps the vulnerability scanning process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides a PCI standard “Pass” or “Fail” status for the network, based on the vulnerabilities identified and the risks associated with those vulnerabilities. The

vulnerabilities and risks levels are clearly listed for the overall test, and by system. The report also includes a listing of each active system identified during the scan, and all vulnerabilities that may be found on each system. Each vulnerability listing includes a description and any recommendation for corrective action.

- E. A report will be delivered in electronic format after the completion of each vulnerability scan on a date agreed upon during the engagement kickoff meeting.

3.4. External Ethical Hacking. This Service is an in-depth network-based security assessment of Internet accessible host IP addresses.

- A. Embarq will employ what are commonly known as “soft” reconnaissance techniques to collect information from public information sources, such as newsgroups, web sites, and registration databases. Embarq will use this information to determine user email addresses, job functions, and current projects. This information will help Embarq determine the technology that is deployed in Customer’s environment, allowing the testing team to focus and tune its attacks to specific types of platforms.
- B. This initial step will also help identify and confirm the ownership of the networks and systems the Customer has submitted for testing, as well as the identities of service providers and systems that are active on a network. Service port numbers that are open on the systems identified, as well as traffic filtering that may be in place anywhere between the attacking and targeted systems. The information obtained during this process helps to verify the set of systems defined for testing, and provides a framework for more in-depth testing that occurs during the next phase.
- C. During this phase of testing, the provided list of targets (from as identified above) is used for more in-depth scans that attempt to identify the operating system, network services, applications, and versions of those items that are active on target systems. After the configuration of the systems and networks is defined in more detail, exploitable vulnerabilities known to exist in those configurations are identified and documented. In addition, data collected by the tools may allow the test team to identify operating systems in use on those systems, and network service applications that are available (SMTP, DNS, HTTP, etc). Scanning will reveal the services that are available on routers, firewalls, and servers from outside the Customer environment.
- D. During this phase, medium intensity probes are used to identify the versions of service applications that are in use. Identification of service application version information is useful because specific vulnerabilities contained in network applications are version specific, and knowing the version number allows specific problems to be targeted. These types of tests typically involve use of telnet and DNS probes by the test team from the keyboard or via customized scripts that collect information about services in use. The information about systems behind the firewall that is collected during these tests can also help illustrate the effectiveness and implementation of the firewall’s filtering rules and configuration.
- E. Once the operating system and application versions have been identified, specific exploits can be identified for the ensuing attack plan. Embarq will work closely with the Customer to determine whether specific vulnerabilities are approved to be exploited. Customer may determine that leaving a specific vulnerability open for exploit is too risky, and it should be immediately corrected rather than being allowed to remain open for even for short duration during testing. In some cases a specific vulnerability can be “partially” exploited to verify it exists, but no action is taken to actually enter a system, or expand access or privileges. Embarq will provide expert advice on vulnerability assessment and testing plan procedures, but in all cases the Customer has the final word on how exploit testing will be performed.
- F. Finally Embarq will try to exploit the vulnerabilities identified during previous tests in an effort to confirm the vulnerability itself, and to leverage any access gained to other

systems on the targeted network. Exploit scripts and procedures obtained from the Internet and other sources are used to exploit identified vulnerabilities. After initial access is gained to a single system on the network, trust relationships between systems and networks can often be used to access other systems on the network.

- G. Password files that can be obtained will have password cracking tools run against them. Network sniffers will be installed where possible to monitor the network for other user account and password information. This will help illustrate the extent to which the network can be compromised, if even a single system with a vulnerable configuration is available online. Since this type of activity involves exploitation of trust relationships from valid accounts on the internal network, it is unlikely that an intrusion detection system will identify these types of tests.
- H. Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides a methodology of the testing process, vulnerabilities found, recommendations for corrections, and an analysis of strengths and weaknesses. The security risks will be risk-ranked so that the most critical risks can be addressed first.
- I. As part of this phase Embarq will provide knowledge transfer with Customer staff to help promote an understanding of how potential problems were identified, corrective actions that can be taken, and the impact of corrective actions on business operations and security. The Internet based testing will be performed remotely from a Embarq facility.
- J. The Ethical Hacking team will not use the access or privileges gained on any system to intentionally modify data, delete files, or cause any other type of damage or service interruptions during phase II.
- K. External Ethical Hacking will be performed on Internet accessible IP addresses for in-depth ethical hacking. The ethical hacking will be performed remotely from Embarq designated facilities. Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides: methodology of the testing process, vulnerabilities found, recommendations for corrections, analysis of strengths and weaknesses, and ranking of security risks so that the most critical risks can be addressed first.

3.5. Ethical Hacking Remote Denial of Service (DOS) Attacks. This Service is the in-depth network-based security assessment of an Internet accessible host using denial of service attacks.

- A. Embarq will perform denial of service attacks Internet facing IP addresses designated for this type of testing from the ethical hacking target list. The tests will be performed using publicly available tools and techniques. Two types of denial of service testing will be performed, resource based and vulnerability based. Resource based involves attempting to send large amounts of data connection requests to the targeted systems in an attempt to overwhelm the processing or bandwidth resources and make the system or network unavailable. Vulnerability based involves attempting to exploit vulnerabilities on a system to make a service or the system itself unavailable. A vulnerability scan will be performed on targeted systems to help identify vulnerable systems and applications that could be targeted for DOS. The specific vulnerabilities that may be available for exploit would be identified after the vulnerability scan is completed, so specific scenarios cannot be provided until that phase has been performed.
- B. The testing on each IP address will consist of a maximum of three (3) different attack scenarios, with each scenario being one type of attack against one IP. The specific set of scenarios will be defined in coordination with the Customer at the appropriate time within the External Ethical Hacking process. Resource based attacks can be performed on any IP that is reachable from the Internet, and vulnerability based attacks can be performed based on vulnerability information obtained during previous testing. The denial of

service testing is coordinated with the Customer, to be conducted on a day during the testing period designated by the Customer. This allows any systems that are affected by the testing to be returned to normal operations at the completion of the testing. The scenarios used and results of the denial of service testing will be documented in a report accessible to Embarq and the Customer. Note that denial of service testing is designed to disrupt and disable systems and networks, and may temporarily have an impact on business operations during testing.

3.6. Web Application Security Testing. This Service is the security testing of the components of external (Internet accessible) IP addresses to include the operating system platform, web server, middleware, and associated databases.

- A. The Web Application Security Testing process consists of an in-depth evaluation of all the major components of a typical web application to include the operating system, web server platform, middleware, and associated databases as accessible from the Internet. The test can be performed from the perspective of an internal or external user of an application, and attempts to determine what type of access an attacker could gain using publicly available hacking tools and techniques. Playing the role of an attacker, the objectives of the test team would be to gain access to the network with the intent to steal or manipulate data that resides there, or to deface the web site. The team will not actually perform any of these malicious acts during the testing process, but will attempt to identify ways an attacker with those objectives could find entry to the network and its systems.
- B. The web applications that are targeted will be evaluated for vulnerabilities in the operating system, web server, middleware, and any associated databases that are accessible. Vulnerabilities that can affect the platform include those that could allow unauthorized access to the system, modification of web site content, viewing and modifying other users' data, or access to entire databases. If possible and applicable, the team will also attempt to gain elevated privileges and expand access to other systems on the network. Any attempt to gain elevated privileges or expand access to other systems would only be done after gaining explicit approval from the Customer. System logs and screenshots collected during the testing process can help illustrate the presence and risk of certain vulnerabilities without performing an exploit, and Embarq will use these resources to document and support findings in the reports.
- C. For applications that allow user logins, five (5) temporary test accounts per role are required to be set up on the application for testing purposes. Additional accounts may be required depending on the number and types of roles (up to three (3) different roles) that are defined by the application. For applications with more than three (3) different roles, custom pricing will be provided. The test accounts are used in determining whether an authorized user or Customer of the application could break out of their defined security role to access and manipulate other users' data, or databases associated with the application. The team will provide a report at the end of the testing process that includes a list of vulnerabilities with associated corrective actions for the tested application. The team will provide immediate verbal notification of all high priority vulnerabilities identified in the web-based application during the testing process. Web Application Security Tests are performed the process defined in six (6) task steps that are summarized below.
 - (1) Task 1: Verification of target information and basic scanning and identification procedures used to identify operational systems and service.
 - (2) Task 2: Probing the identified systems for known vulnerabilities.
 - (a) In depth scans of all 65,535 ports to identify the operating system, network services, applications, and versions of those items that are active on target systems.
 - (b) Identify the versions of service applications that are in use.
 - (c) Identify candidate exploits, and develop an attack plan.

-
- (3) Task 3: Exploiting of web server vulnerabilities in a manner to identify what an attacker would be capable of.
 - (a) Active scans are performed using commercial, public, and custom tools designed to identify and/or exploit specific vulnerabilities.
 - (b) Scans for default material.
 - (4) Task 4: Exploiting of database vulnerabilities, if accessible, in a manner to identify what an attacker would be capable of.
 - (a) Active scans are performed using commercial, public, and custom tools designed to identify and/or exploit specific vulnerabilities.
 - (b) Attempt connections with default usernames and passwords.
 - (5) Task 5: Exploiting of middleware vulnerabilities in a manner to identify what an attacker would be capable of.
 - (a) Use proxy to intercept and change data transmissions to determine effect on application.
 - (b) Up to twenty five (25) web pages with no more than twenty five (25) forms will be tested. This testing assumes that there are no more than twenty (20) user input fields per form. Applications exceeding these limits will require custom pricing.
 - (6) Task 6: Exploiting of the application to identify what an attacker would be capable of.
 - (a) Active scans are performed using commercial, public, and custom tools designed to identify and/or exploit specific vulnerabilities.
 - (b) The following items are tested for potential weaknesses: authentication, account lockout, buffer overflows, error messages, -password policy, session tracking, session hi-jacking, IP hopping, concurrency, proper cookie usage, session timeouts, encryption, and username harvesting

D. Web Application Security Testing will be performed on Internet accessible web-based application owned by the Customer . The testing of the Internet accessible web-based application will be performed remotely from Embarq designated facilities. Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides:

- (1) Methodology of the testing process
- (2) Vulnerabilities found
- (3) Recommendations for corrections,
- (4) Analysis of strengths and weaknesses:
- (5) Ranking of security risks so that the most critical risks can be addressed first.

3.7. Internal Target Identification. This Service is the scanning of Internet accessible host IP addresses to identify the number targets for specific vulnerability scan or in-depth ethical hacking.

- A.** Embarq performs broad scans of large network segments to identify active systems for a specific vulnerability scan or in-depth ethical hack.
- B.** Embarq will scan network ranges and identify active hosts on the network. This information will be used in conjunction with the internal Vulnerability Scanning or internal Ethical Hacking services.

3.8. Internal Vulnerability Scanning. This Service is the scanning of Intranet accessible host IP addresses.

- A.** After the set of Customer intranet accessible addresses is defined in the reconnaissance phase, Embarq will meet with Customer to determine which addresses will be included in the full vulnerability scan and in-depth ethical hacking. Vulnerability scanning identifies IP addresses that are active on the network, and information about the operating system,

network services, applications, and versions of those items that are active on targeted systems. After the configuration of the systems and networks is defined in more detail, exploitable vulnerabilities known to exist in those configurations are identified and documented. In addition, data collected by the tools may allow the test team to identify operating systems in use on those systems, and network service applications that are available (SMTP, DNS, HTTP, etc). Internal scanning (i.e. performed on the customer's Intranet) will reveal the services that are available on targeted systems. Any vulnerabilities will be identified and documented, but will not be exploited by the Embarq team.

- B.** The next phase of the vulnerability scanning process utilizes medium intensity probes to identify the versions of service applications that are in use. Identification of service application version information is useful because vulnerabilities contained in network applications are version specific, and knowing the version number allows specific problems to be targeted. Embarq will develop a report that recaps the vulnerability scanning process and identifies the prioritized security findings and risks with risk mitigating recommendations. The vulnerabilities and risks levels are clearly listed for the overall test, and by system. The report also includes a listing of each active system identified during the scan, and all vulnerabilities that may be found on each system. Each vulnerability listing includes a description and recommendation for corrective action.
- C.** Embarq will perform internal vulnerability scanning on Intranet-accessible IP addresses. A full vulnerability scanning report will be delivered for the entire set of systems identified during the vulnerability scan.

3.9. Internal Ethical Hacking. This Service is an in-depth, network-based security assessment of Intranet accessible host IP addresses.

- A.** Embarq will use information from the Internal Target Identification to determine targets for performing the Internal Ethical Hacking. These targets will be used for more in-depth scans that attempt to identify the operating system, network services, applications, and versions of those items that are active on target systems. After the configuration of the systems and networks is defined in more detail, exploitable vulnerabilities known to exist in those configurations are identified and documented. In addition, data collected by the tools may allow the test team to identify operating systems in use on those systems, and network service applications that are available (SMTP, DNS, HTTP, etc).
- B.** During this phase, medium intensity probes are used to identify the versions of service applications that are in use. Identification of service application version information is useful because often vulnerabilities contained in network applications are version specific, and knowing the version number allows specific problems to be targeted. These types of tests typically involve use of telnet and DNS probes by the test team from the keyboard or via customized scripts that collect information about services in use. The information about systems behind the firewall that is collected during these tests can also help illustrate the effectiveness and implementation of the firewall's filtering rules and configuration.
- C.** Once the operating system and application versions have been identified, specific exploits can be identified for the ensuing attack plan. Embarq always works closely with Customer to determine whether specific vulnerabilities are approved to be exploited. Customer may determine that leaving a specific vulnerability open for exploit is too risky, and it should be immediately corrected rather than being allowed to remain open for even for short duration during testing. In some cases a specific vulnerability can be "partially" exploited to verify it exists, but no action is taken to actually enter a system, or expand access or privileges. Embarq will provide expert advice on vulnerability assessment and testing plan procedures, but in all cases the Customer has the final word on how exploit testing will be performed. Customer will be responsible for obtaining timely decisions on these activities.

-
- D. Embarq will try to exploit the vulnerabilities identified during previous tests in an effort to confirm the vulnerability itself, and to leverage any access gained to other systems on the targeted network. Exploit scripts and procedures obtained from the Internet and other sources are used to exploit identified vulnerabilities. After initial access is gained to a single system on the network, trust relationships between systems and networks can often be used to access other systems on the network.
 - E. Password files that can be obtained will have password cracking tools run against them. Network sniffers will be installed where possible to monitor the network for other user account and password information. This will help illustrate the extent to which the network can be compromised, if even a single system with a vulnerable configuration is available online. Since this type of activity involves exploitation of trust relationships from valid accounts on the internal network, it is unlikely that an intrusion detection system will identify these types of tests.
 - F. Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides a methodology of the testing process, vulnerabilities found, recommendations for corrections, and an analysis of strengths and weaknesses. The security risks will be risk-ranked so that the most critical risks can be addressed first.
 - G. As part of this phase, Embarq will provide knowledge transfer with Customer staff to help promote an understanding of how potential problems were identified, corrective actions that can be taken, and the impact of corrective actions on business operations and security. The Internet based testing will be performed remotely from a Embarq facility.
 - H. The Ethical Hacking team will not use the access or privileges gained on any system to intentionally modify data, delete files, or cause any other type of damage or service interruptions during the testing.
 - I. Internal Ethical Hacking will be performed on intranet accessible IP addresses for in-depth ethical hacking. The ethical hacking will be performed remotely from Embarq designated facilities. Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides methodology of the testing process, vulnerabilities found, recommendations for corrections, analysis of strengths and weaknesses, and ranking of security risks so that the most critical risks can be addressed first.

3.10. Dial-In Access Security Testing. This Service is the testing for publicly accessible phone numbers with area codes in the United States.

- A. Embarq will conduct Dial-In Access Security Testing (Wardial) against a specified list of phone numbers provided by Customer, and will perform an ethical hack against modem-connected devices that are discovered. The minimum scope for Dial In Testing is 500 phone lines. The Ethical Hacking will be performed on up to 2% of the number of lines dialed. The numbers can be dialed at specified time intervals, or during business and non-business hours, at Customer's discretion. Dial-in testing, data analysis, and report writing will be done remotely from Embarq facilities.
- B. Results are recorded, analyzed, and provided as a specific vulnerability snapshot of the modem connections available during the time the test was performed. The modem security testing service follows the following methodology:
 - (1) All numbers are dialed and results, banners, login screens, or modem responses, are recorded into a log file for analysis. If the number is busy, disconnected, or unresponsive at the time of the test, then it will be labeled as such. Busy numbers are dialed twice in an effort to identify all "carriers" (modem connections).

Identification of the type of system providing modem connectivity occurs in this phase.

- (2) Ethical hacking is performed against identified modem-connected devices. Each number identified as a data “carrier” (i.e. potential modem) is dialed again. Attempts are then made to gain access to the device via the modem connection. The activity of the connection is recorded. If access is achieved through the modem connection, the level of access is identified. Further access into the host and or network can be attempted at the discretion of Customer.
- C. Dial-In Access Security Testing will be performed on publicly accessible U.S. based phone numbers owned by Customer. Dial-In Access Security Testing will be performed remotely from Embarq facilities.

3.11. Host Security Assessment. This Service is the assessment performed on systems.

- A. Host Security Assessments are a hands-on collection and analysis of a system’s security configuration data. A system can be a server, router, firewall, IDS, or other type of device located within Customer’s IT environment. Certain aspects of a system’s configuration and security posture cannot be remotely analyzed across a network, and must be done in a hands-on manner. Automated tools and system commands are used to collect data related to system and application settings that can impact the security of the system. The process includes evaluating the patch level, network services that are running, significant applications installed on the system, and account management. Embarq will examine, review, assess and provide recommendations for improving the security of systems that are assessed.
- B. The operating system type, and number of each type included in the Host Security Assessment must be provided to Embarq prior to time of contract signature, to make sure the testing team assembles the appropriate set of tools and procedures to perform the tests. The types of systems involved in the assessment will also be a factor in determining the specific staff assignments for this task, as task assignments are based on expertise with specific types of technologies.
- C. The Host Security Assessment will require the Embarq test team to have system administrator privileges at the console on each device in order to run the tools and commands needed to collect the required data. If this is not possible, then Embarq will work with Customer to have a member of Customer’s staff run the tools and commands, and collect and transfer the data to Embarq for review. All systems included in the Host Security Assessment are assumed to be located at one (1) mutually agreed Customer facility, or other location local to that area. Tools are either loaded from a CD or downloaded from a Embarq laptop computer connected to the network.
- D. The security assessment tools will evaluate the system and security configuration settings of the specific system being evaluated, to look for potential problems. Data generated by the tools is dumped to files on the system being assessed. The data is typically collected and moved to a Embarq system for analysis to minimize the access and time required on Customer’s system. The time required for the tools to run and data collection to complete can vary depending on the type of operating system in use, the type of processor, and the number of files and users on the system.
- E. The data is analyzed for potential problems involving issues such as user account management settings, file and directory permissions, and network service configurations. Issues that are identified as findings are documented, and recommendations for corrective actions are provided. Findings are generated and reviewed in close communication with the Customer to promote data is interpreted in the proper technical and business context.

-
- F. The server devices included in the Host Security Assessment can be any combination of the following operating system types; Windows 2000/NT, AS/400, Solaris, HP-UX, AIX, or Linux.
 - G. A Host Security Assessment will be performed on systems. The security assessment will be performed at one (1) Customer facility. Includes at least 1 business day of onsite work per eight (8) systems reviewed by an Embarq senior security engineer. Additional data analysis and report creation will be performed remotely from a Embarq facility. Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides: methodology of the testing process, vulnerabilities found, recommendations for corrections, analysis of strengths and weaknesses, and ranking of security risks so that the most critical risks can be addressed first.

3.12. 802.11 Wireless Security Testing. This Service is the testing against 802.11b or 802.11g wireless access point(s).

- A. 802.11 Wireless Security Testing focuses on the configuration and accessibility of wireless access points (WAPs) connected to a corporate network. These can be devices that are authorized and deployed by the organization, or rogue devices set up by employees or someone else with access to the facility. WAPs that are identified are assessed for configuration information, vulnerabilities, and security settings. The wireless portion of the exercise must be performed locally and will require travel expenses for Embarq to work on Customer's site. The actual attacks must be conducted in close proximity to the Customer's network, since the range of the RF signal for wireless LANs is typically only a few hundred feet.
- B. During the attack, Embarq will attempt to break into the wireless access point and access any systems (WWW/FTP/SMTP servers, e-commerce servers and so on) identified on the network. Embarq can perform an attempt to break Wired Equivalent Privacy (WEP) encryption in order to demonstrate the tools and techniques used by hackers. If Customer wishes, Embarq can attempt to break the WEP encryption on any identified wireless network, or define a level of effort that would be required to break the WEP key.
- C. Optionally, Customer may opt to provide the encryption keys of known wireless networks. Once a wireless network has been compromised, research will be conducted to find vulnerabilities relating to the specific operating system (OS) type and version, and software application (if applicable) of systems identified from the wireless network. A detailed log of all activities, and keystroke logs are recorded and provided to Customer to ensure complete documentation of the test and results.
- D. Embarq will conduct a wireless ethical hack against 802.11b or 802.11g WAPs at a Customer facility. Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides methodology of the testing process, vulnerabilities found, recommendations for corrections, analysis of strengths and weaknesses, and ranking of security risks so that the most critical risks can be addressed first.

3.13. Firewall Configuration Review. This Service is an analysis performed on Customer's firewall configurations that consists of an evaluation of the firewall rules.

- A. The review of firewall configurations will consist of an evaluation of the firewall and Network Address Translation (NAT) rules. The firewall configuration provides front line protection from threats that are external to the network. A well configured firewall rule set helps to maximize protection of a network and the business operations it supports. A rule set can be configured to restrict access to services and systems on the internal network, and provide protection from certain types of network attacks such as denial of service attacks.

-
- B. The primary objective of the review is to evaluate the firewall rule set configurations to identify vulnerabilities with external firewalls. Firewall rule sets can change over time as new business requirements require changes to be made in the level of access allowed for services and systems on the network. The need for certain rules to remain in a rule set can also change due to changes in business requirements and operations. Periodic review of rule firewall sets can help determine vulnerabilities and weaknesses that may have been introduced by new rules, and identify rules that are no longer required and can be removed.
 - C. The firewall rule set, of up to one hundred (100) rules per firewall will be provided by Customer in order to eliminate the need for the Embarq test team personnel to have privileged access to the devices to obtain this information. For rule sets of more than 100 rules, custom pricing will be provided. The reviews will be performed in close coordination with key personnel responsible for the devices to help enable the Embarq test team has all the information about configuration settings related to business operations. Close coordination will also help enable knowledge transfer during this phase of the assessment process. Embarq will provide a report that includes description of the rule set, results of the analysis that was performed, and recommendations for modifications that could be made to the firewall to enhance the security of the network it protects.

3.14. Assessment Report. This Service is the report that will outline Customer's security compliance with applicable regulations.

- A. Embarq will develop a report that outlines a company's security regulations compliance to industry standards such as PCI, HIPPA, SOX, and GLBA. For example if a company needs to meet both GLBA and PCI requirements, Embarq can boil both regulations down into a single list of control objectives for the Customer. This will save the Customer time and effort by reducing duplicative effort where the regulations overlap. Embarq will spend up to sixty (60) hours of effort in support of this offering. If the initial evaluation of the engagement indicates that more than sixty (60) hours will be required, then custom pricing will be provided in the Customer SOW.
- B. Embarq will develop a concise list of control objectives and how those control objectives map back to each of the regulatory requirements. Embarq will provide a report that includes description of the each control objective, and list of applicable regulations that each of the control objective meets.

3.15. Security Policy Review. The Service is the review performed to evaluate both the breadth and depth of Customer's existing security policies and procedures to identify potential shortcomings and corresponding opportunities for improvement.

- A. Embarq will evaluate both the breadth and depth of Customer's existing security related policies, procedures, and business processes, in order to identify any potential weaknesses and corresponding opportunities for improvement. This analysis will be performed using industry common practices for security policy assessment and development, as well as leveraging Embarq's practical experience in assessing and developing corporate security policies.
- B. During the review process, Embarq will also take into consideration Customer's business objectives, operating environment, and future goals. Embarq will review relevant existing security policies and procedures documents, and perform interviews of key personnel to gain a better understanding of policy and procedure specifics. At the end of the review process, a set of recommendations will be developed in order to address any gaps or non-effective processes identified.
- C. Embarq will provide detailed assessments of Customer's current security policy situation versus a desired end-state (a Gap Analysis), and a set of recommendations advising Customer on changes to make to achieve the end-state. The desired end-state will be

assessed by Embarq based on their understanding of Customer's business needs, Customer's current situation and security posture, regulatory requirements relevant to Customer, and Embarq's understanding of business and other conditions unique to Customer based on information provided by Customer.

- D. Embarq's security consultants will evaluate both the breadth and depth of Customer's existing security policies and procedures in order to identify potential weaknesses and corresponding opportunities for improvement. Embarq will review how Customer uses its network and systems to support essential business functions and processes.
- E. This analysis will be performed using industry common practices for security policy assessment and development as well as leverage Embarq's practical experience in assessing and developing corporate security policies. During the review process, Embarq will also account for Customer's mission and operating environment and future goals. Embarq will review relevant existing security policies and procedures, whether formally documented or in the form of informal memoranda or other means. Embarq will also review existing documentation of Customer's networked computing resources, as provided by Customer.
- F. Embarq will gather the information described above via face-to-face or telephone interviews and email. Embarq requires access to Customer's key decision makers and managers responsible for business applications, network architecture, network management and IT security. At the end of the review process, a set of recommendations will be developed in order to address any gaps or non-effective processes identified.
- G. Consideration for the feasibility of implementing new security controls will be given relative to Customer's existing environment and planned growth. The list of recommendations will take into account Customer's immediate requirements and long-term goals, industry common practices, regulations, and standards. To the extent that Embarq proposes any new security control, however, it will ultimately be the Customer's responsibility to determine feasibility of implementation.

3.16. Security Gap Analysis Review. This Service is the review performed to evaluate both the breadth and depth of Customer's existing security policies and procedures, business goals, and proposed short term infrastructure changes, in order to identify any potential shortcomings when compared with industry common practice.

- A. Embarq will evaluate both the breadth and depth of Customer's existing security related policies, procedures, and business processes, in order to identify any potential weaknesses and corresponding opportunities for improvement. This analysis will be performed using industry common practices for security policy assessment and development, as well as leveraging Embarq's practical experience in assessing and developing corporate security policies. During the review process, Embarq will also take into consideration of the Customer's business objectives, operating environment, and future goals. Embarq will review relevant existing security policies and procedures documents, and perform interviews of key personnel to gain a better understanding of policy and procedure specifics. At the end of the review process, a set of recommendations will be developed in order to address any gaps or non-effective processes identified.
- B. Embarq will provide detailed assessments of Customer's current security policy situation versus a desired end-state (a gap analysis), and a set of recommendations advising Customer on changes to make to achieve the end-state. The desired end-state will be assessed by Embarq based on their understanding of Customer's business needs, Customer's current situation and security posture, and Embarq's understanding of business and other conditions unique to Customers based on information provided by Customer.
- C. Embarq will gather the information described above via face-to-face or telephone interviews and email. Embarq requires access to Customer's key decision makers and

managers responsible for business applications, network architecture, network management and IT security. At the end of the review process, a set of recommendations will be developed in order to address any gaps or non-effective processes identified. Consideration for the feasibility of implementing new security controls will be given relative to Customer's existing environment and planned growth. The list of recommendations will take into account Customer's immediate requirements and long-term goals, industry common practices, regulations, and standards. To the extent that Embarq proposes any new security control, however, it will ultimately be the Customer's responsibility to determine feasibility of implementation

3.17. Creation of Security Policy. This Service is the development of a policy that meets industry common practices to support compliancy needs.

- A. Embarq will create an initial security policy taking into consideration Customer's business objectives, operating environment, and future goals. Embarq will perform interviews with key personnel to gain a better understanding of policy and procedure needs. Ultimately, Embarq will develop a base security policy that is based on Embarq's understanding of Customer's business needs, Customer's current situation and security posture, and regulatory requirements relevant to Customer based on information provided by Customer.
- B. Embarq will gather the information described above via face-to-face or telephone interviews and email. Embarq requires access to Customer's key decision makers and managers responsible for business applications, network architecture, network management and IT security. At the end of the review process, a base security policy will be developed and delivered to the Customer. The security policy that Embarq delivers is based on the collection of data and its expertise, however, it will ultimately be Customer's responsibility to validate, distribute and maintain the policy within the Customer's environment.

3.18. Onsite Social Engineering. This Service is the engineering of physical locations in an attempt to gain access to the facility, workstation, and/or network located there. The site will also be surveyed for other information that may be available for an unauthorized person to take such as documents and employee badges.

- A. Embarq will perform onsite social engineering in an attempt to gain access to the facility, and workstation or network located there. The site will also be surveyed for other information that may be available for an unauthorized person to take such as documents and employee badges. Social engineering generally involves making attempts to trick employees into disclosing restricted or sensitive information, or to allow access to facilities. Attempts to gain information can include entering after a valid employee has opened a locked door with a swipe card, entering as a service provider, or reporting as a new employee. For onsite social engineering, Embarq will attempt to perform the following activities:
 - (1) one assigned Embarq individual will travel to an Customer facility;
 - (2) Embarq will attempt to make a minimum of two (2) access attempts during a one day period onsite; and
 - (3) Depending on the level of access gained, Embarq may attempt to connect a laptop computer to a network jack within the facility, use an unattended workstation, obtain an employee badge, and place floppy disks or CD into the drives of unattended workstations.
- B. Onsite Social Engineering includes up to one (1) Business Day onsite at a designated Customer location. Additional data analysis and report creation is performed remotely from an Embarq facility. Embarq will provide a report detailing the results of all social engineering activities to include details on our communications, responses received, results and any information that was obtained, and recommendations for correcting problems that may be identified.

3.19. Remote Social Engineering. This Service is the use of telephone calls, email, web pages, and other media in an attempt to gain access to sensitive or restricted information that would aid a person targeting Customer's IT infrastructure.

- A. Embarq will use available public sources of Internet-based information and social engineering in an attempt to obtain information about Customer that would aid a person targeting the company's IT infrastructure. Social engineering generally involves making attempts to trick employees into disclosing restricted or sensitive information. Attempts to gain information can include use of phone calls, e-mail, web pages, or other media. Embarq will perform an open source search about the company to search for any details our test engineers can exploit during the testing process. Open source searches will include usenets, world wide web (WWW), email lists, and message boards.
- B. Embarq will also attempt to learn more about Customer systems by using various phone and mailer techniques. For phone, e-mail, and mailer-based social engineering Embarq will perform the following types of activities:
 - (1) make up to three (3) calls to Customer numbers/call centers/support desks in attempt to gain access to privileged information to aid Embarq in our Ethical hack attempts;
 - (2) create up to three (3) unique e-mails, and send each to a maximum of twenty (20) Customer e-mail addresses in attempt to gain access to privileged information to aid Embarq in our Ethical hack attempts; and
 - (3) search of publicly accessible Internet based sources.
- C. Embarq may also attempt the following depending on the type of the Customer's Internet presence, the success of social engineering methods listed previously, and time permitting:
 - (1) attempt to get Customer representatives to set up accounts on web based business applications that provide transactions or other Customer support; and
 - (2) develop a CD mailer to send to Customer personnel in attempt to gain access to Customer systems.
- D. Embarq will generate a report that summarizes the methodology, a log of all actions performed and list of weakness identified during the social engineering process.

3.20. Network Architecture Analysis. This Service is the review of the existing architecture by reviewing existing network diagrams, proposed infrastructure change diagrams and an actual device configuration review of firewalls, router, switches, and one VPN concentrators.

- A. A network security architecture consists of several elements, some of which are intangible. One element is a process that includes administration and management; another is technology, which includes hardware systems, configurations, and applications. Planning & design elements include the business drivers, policies, and principles. When all the elements and other components are organized to work together then the overall security posture can improve. Embarq will evaluate all three (3) elements on specific network and security devices, in order to verify that all components are performing as designed, required, and are optimized to provide a formidable front door defense layer.
- B. The review of network device configurations will consist of an evaluation being preformed on devices including firewalls, routers, switches or a VPN concentrators followed by a review of the current network architecture. Additional devices can be added to the network assessment and will be custom priced as part of the Customer SOW.
 - (1) Firewall. The firewall configuration review will consist of a review of firewalls. The firewall configuration provides front line protection from threats that are external to the network. A well configured firewall rule set helps to maximize protection of a network and the business operations it supports. A rule set can be configured to restrict access to services and systems on the internal network, and provide protection from certain types of network attacks such as denial of service

attacks. The main objective of the review is to evaluate the firewall rule set configuration to determine if potential vulnerabilities exist through the external firewalls, and to verify that this device complies with Customer's security policies and business goals. Firewall rule sets can change over time as new business requirements require changes to be made in the level of access allowed for services and systems on the network. The need for certain rules to remain in a rule set can also change due to changes in business requirements and operations. Periodic reviews of firewall rule sets can help determine vulnerabilities and weaknesses that may have been introduced by new rules, and identify rules that are no longer required and can be removed.

- (2) Router, Switch and VPN Concentrator
 - (a) This review will consist of routers, switches and VPN concentrator configuration files. These network devices provide inter-infrastructure connectivity, as well as front line connectivity to the network. Often, access control lists (ACLs) are enabled on these devices to distribute the firewall processing load. There are a number of security checks that these devices can perform to weed out network "noise" (anticipated and common place connection attempts, that do not require in depth analysis, and can be blocked before ever entering Customer infrastructure), freeing up the firewall to focus on sophisticated access attempts. It is also possible to inadvertently duplicate security functionality and add unnecessary latency and processing, or the exact polar opposite of circumvention of the installed and required security devices and checks.
 - (b) All configuration and rule set files will be provided by Customer in order to eliminate the need for the Embarq delivery team personnel to have privileged access to the devices, to obtain the information. The reviews will be performed in close coordination with key Customer personnel responsible for the device, to help make sure that the Embarq delivery team has all the information about configuration settings related to business operations. Close coordination will also help enable knowledge transfer during this phase of the assessment process.
- (3) Network Review
 - (a) Customer will provide a network map for Embarq to review. Embarq will review Internet connectivity points, hosted services, remote site-to-site tunnel configurations, partner connections and data flow for business operations. Embarq will identify and document any gaps between customer's current configuration and industry common practices then make any applicable recommendations to correct those issues.
 - (b) Embarq will provide a report that includes description of each of the devices that were reviewed, description of the current network design, results of the analysis that was performed, and recommendations for any modifications that could be made to each device to enhance the security of the network it protects.

3.21. Security Engineering Support. This Service is support provided in hourly increments, over a period of six (6) months, for troubleshooting, web application reviews and architecture analysis work. As a part of the Customer SOW, Embarq will offer senior security engineers as security expert on-call technical support for security support activities. This technical support includes assisting staff with activities such as troubleshooting, web application reviews, architecture analysis and other security related type work. Embarq will reserve business hours that and Customer can use as and when necessary, over a period of three (3) months. All Security Engineering support is custom priced and will be specified in the Customer SOW.

3.22. VOIP Security Assessment. This Service is support provided in hourly increments for voice over internet protocol security assessments.

-
- A. Embarq will assess the security of a Voice over IP (VoIP) infrastructure by a two phase approach. First, we assess the resilience of the Voice network to a simulated attack, commonly referred to as an ethical hack. The methods used during this attack include the following:
 - (1) Network Scanning to identify vulnerabilities in phone and PBX firmware
 - (2) Denial of Service attacks to phone infrastructure
 - (3) TFTP impersonation attacks to adjust the operating firmware
 - (4) Attempt to bypass any toll restrictions and commit toll fraud
 - (5) DHCP Assault/Starvation attacks
 - (6) DHCP Server impersonation attacks
 - (7) Man in the Middle attacks

 - B. As voice networks continue to grow on top of existing data infrastructure, the trust in the confidentiality of voice communications can be circumvented therefore our focus of the ethical voice assessment is to capture, intercept, or modify live voice communications. The results of the ethical assessment will provide a risk ranking to the cause and effect of the specific attacks that can be leveraged by the client's security staff to adjust existing infrastructure or anticipate future threats by being aware of weaknesses with the VoIP products deployed within the network.

 - C. The second phase of the VoIP Assessment is a risk assessment and architecture review. VoIP may be implemented using data networking technologies but the risks of voice interception and the high cost of voice outages requires a more aggressive security posture within the VoIP network. Embarq will perform a risk assessment of the client's VoIP strategy in addition to analysis of the VoIP related policies, procedures, and processes. After the risk assessment is performed, the network architecture of the client's voice network will be analyzed. The focus of the architecture review will be reliability, resilience to network level attacks, and ensuring the proper security controls are in-place within highly confidential call time such as conference calls, executive extensions, and customer call center traffic. Lastly, the architecture review analyzes network layer security device configurations such as Firewall, IPS/IDS, logging, encryption and their VoIP specific configuration requirements.

 - D. Lastly, our VoIP Assessment produces an actionable deliverable the identifies the key risks within the voice network, recommendations on how the client can mitigate the risks, and a list of practices for use in growing and scaling the voice infrastructure.

4. SOFTWARE AND HARDWARE TECHNOLOGIES THAT MAY BE APPLIED

- 4.1. Embarq will create a more definitive and appropriate toolset for the assessment after additional information is obtained about the types of platforms that will be evaluated and scanned at various points during the project. For example, if particular types of platforms and operating system version types are identified during an ethical hack, a specific set of tools will be used to further probe and potentially attempt to exploit vulnerabilities. The types of systems included in the assessment will also affect the set of tools. The list of tools below contains representative examples that may be used during an engagement. The specific tools will be adjusted as needed for specific projects.
 - A. Nmap is a freeware port scanner and traffic generator tool. It can conduct scans using unconventional methods that would not ordinarily be caught by either an intrusion detection system (IDS) or a firewall. It can be used to launch various attacks including denial of service.

 - B. Nessus is a freeware security scanning tool for identifying vulnerabilities. This tool also requires, as a pre-requisite, the presence of nmap on the system used for the launch of the Nessus scan.

 - C. Qualys is a commercial security scanning tool for identifying vulnerabilities. This tool can be launched as a service from the Internet or internal to a client via an appliance.

-
- D. Webscanner is an open-source Perl script used to scan web sites for common configuration errors and software vulnerabilities.
 - E. Achilles is a local web proxy used to test web applications. It allows manipulation of input values and cookies sent to the web server.
 - F. Burp Proxy is a Java based web proxy used to capture or alter inbound and outbound http/https traffic. It runs on Windows, Linux and Solaris.
 - G. Dig stands for Domain Information Groper - This tool is used to perform various types of domain name service lookups. This tool is part of the latest Linux distributions.
 - H. Ike-scan is an open source VPN server scanning tool. Ike-scan attempts to establish an ike (VPN) connection with target hosts and reports successful connections.
 - I. BRUTUS is a password cracking utility. It is especially useful, as it will connect on well-known ports to accomplish its attacks.
 - J. Unix Utilities (Nslookup, Ping, Traceroute). There are several utilities built into the Red Hat operating system that are used during an assessment.
 - K. Ethereal is a network packet sniffer that can also display packets captured with a number of other tools, and it works on Unix and Windows platforms.
 - L. Wireless Tools. Embarq uses the following industry proven tools for the wireless assessment: NetStumbler, Kismet, TCPDump / Wireshark, airodump, aircrack and airtsnort. These tools are the industry standard for assessing wireless networks and are designed to detect all 802.11 (b/g) wireless devices that are active and in range.

4.2. Embarq may use customized scripts and command line operations for certain aspects of the project. For example, when working host based assessments on UNIX based servers, scripts and system commands can be used to collect the information needed for the assessment.

4.3. The ethical hacking may involve loading tools such as a sniffer, depending on the types of vulnerabilities that are identified and available for exploit. Embarq will not proceed with exploiting vulnerabilities and subsequent installation of tools until Customer has provided approval for the activity.

5. **ENGAGEMENT COMPLETION REPORT.**

5.1. **Completion Report.** Upon engagement completion, Embarq will provide to the Customer at no additional cost a comprehensive report containing results from all services tested in this engagement. Included in the report is detailed information related to exposed security vulnerabilities, including: executive summary, scope of the project and a non-technical overview of vulnerabilities found, prioritized list of vulnerabilities, technical list of vulnerabilities found during the penetration testing, risks associated with vulnerabilities, business risks if a specific vulnerability is not resolved, suggested solutions to securing vulnerabilities, types of attacks that were performed, detailed list of attacks, including any tools used and our methodology, recommendations for remediation of potential vulnerabilities based on the ethical hacking and the security architecture assessment, and recommendations on long-term and strategic initiatives to enhance security, by leveraging industry common practices and design principles.

5.2. **Timeline.** The timeframe for delivery of all reports for these services is dependent on the scope and number of services ordered. The timeframe for delivery of all reports will be discussed with Embarq and the Customer as part of the Customer SOW and subsequent kick-off meeting.

6. **ANTICIPATED PROJECT TIMELINE.** The actual delivery timeline for each service will be defined between Embarq and Customer with the Customer SOW developed as part of the Agreement. The timeline for delivery will be dependent on the scope of testing performed.

7. CUSTOMER RESPONSIBILITIES.

- 7.1. Customer will provide the authorization required for Embarq and its agent, TekSecure Labs, to perform the Services described herein, specifically including the following authorizations.
- A. Services. Embarq and TekSecure Labs will utilize automated and manual tools and methods as required to perform electronic scans of Customer's networks, hosts and/or devices.
 - B. Services. Embarq has obtained from Customer authorization and Customer permits both Embarq and TekSecure Labs to access Customer's networks, hosts, telephone numbers, and/or devices indicated in the Agreement and Customer SOW sufficient for Embarq and TekSecure Labs to perform Services.
 - C. Authority to Copy Information. In the event that Services performed by Embarq and TekSecure Labs enable the ability to gain access to the target platforms, Customer authorizes Embarq and TekSecure Labs to copy information only for the purpose of defining established access to the platform or network sniffing capabilities. Information will be provided back to an authorized agent of Customer through a penetration test report document, or encrypted electronic file attachment.
 - D. Warranty Disclaimer THE SERVICES ARE PROVIDED AS IS, WHERE IS, WITH NO WARRANTIES OF ANY TYPE OR KIND, WHETHER EXPRESS OR IMPLIED, AND THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. Embarq and TekSecure Labs make no representation or warranty that its security vulnerability testing services will disclose all vulnerabilities, and Embarq and TekSecure Labs, by providing Services, do not warrant the security of Customer's network or computer system from invasion, attack or damage from acts of any person, entity or organization.
 - E. Limitation of Liability. Customer agrees that, under no circumstances, will TekSecure Labs or Tekmark Global Solutions, LLC, its members, officers, directors, employees, contractors, suppliers and agents ("TekSecure Labs Parties") be liable for direct, indirect, consequential, incidental or exemplary damages or for any lost profits, revenues, goodwill or savings arising out of the Agreement. Customer agrees to indemnify and hold harmless all TekSecure Labs Parties from any and all costs (including attorneys fees), damages, expenses and fines, that a TekSecure Labs Party incurs, either directly or indirectly, as a result of performing the Services.
- 7.2. Customer will provide Embarq with a point of contact to serve as primary point of contact between Embarq and Customer. Customer will coordinate its activities for the project and for providing qualified technical personnel to review plans, assessments, recommendations and complete deliverables. Customer will also provide project management, scheduling, and tracking assistance.
- 7.3. Customer will provide Embarq with specific information necessary to perform the consulting prior to on-site engagement (e.g., IP address list and contact information). For each task, Embarq requires certain information such as target IP addresses and contact information, for the execution of this engagement. This information will be determined in the initial project scope and requirements meeting. Embarq will identify the required information and both parties will agree on the times at which this information will be provided. The work schedule will be devised in accordance with the availability of information.
- 7.4. Customer must certify that all information presently known to be necessary for the performance of Services as stated in this SOW has been disclosed or provided to Embarq and will provide information reasonably requested by Embarq.
- 7.5. Customer will participate in meetings to resolve all engagement related issues and make specific personnel readily available for such meetings.

-
- 7.6. Customer will inform Embarq of any information or changes, which may affect Embarq' performance of Services.
 - 7.7. Customer will escalate any Customer issues to Embarq' project manager in accordance to the escalation plan agreed upon during project kickoff.
 - 7.8. Customer will assign the appropriate personnel to work with Embarq during the course of a project.
 - 7.9. Customer will provide ten (10) day advanced notice for any out of scope travel to Customer sites not included as a part of the Services.
 - 7.10. Customer will provide Embarq with access to the premises of the applicable facility if required. The designated Customer facility will be mutually agreed upon. Customer will make available to Embarq personnel office space and/or the appropriate facilities without charge including computer services, presentation aids, and tools, if required.
 - 7.11. If needed, Customer will insure adequate software vendor support, e.g., operating systems and applications systems.
 - 7.12. Customer is responsible for software vendor support costs, which may be incurred during the project when such support is mutually agreed as being required.
 - 7.13. If required, Customer will make all changes to the existing systems to allow Embarq access to Customer's systems.
 - 7.14. Customer will ensure that any requested review and approval of information prepared by Embarq is delivered in a timely manner, so as to permit Embarq to properly perform its obligations hereunder.
 - 7.15. Customer is responsible for the accuracy of all information supplied to Embarq by the Customer designated project team and Embarq relies upon in the performance of Services to Customers.
 - 7.16. In the event Customer fails to perform its responsibilities hereunder, Embarq may, at Embarq's option, assume or fulfill any and/or all of the Customer's responsibilities, directly or through contract with third parties.
 - 7.17. In addition to providing Embarq with full, good faith cooperation and such information as may be required by Embarq in order to perform its obligations hereunder, the Customer will:
 - F. Provide Embarq with specific and detailed information in writing concerning the Customer use of the traffic monitoring and management tools as may be required for the performance of the Services, and
 - G. Make available to each Embarq employee physically located on the Customer premises, computer time and storage on the system configuration sufficient for Embarq to properly perform its obligations hereunder. This will be during regular working hours and such additional hours as reasonably requested by Embarq to provide the Services.
 - 7.18. Customer will provide all necessary computer services, information and access to key personnel needed to provide the Services.

8. PROJECT GOVERNANCE

8.1. Engagement Management Team

- A. Embarq will provide a project manager, who will be responsible for providing a single point of contact at Embarq for status reports and for tracking the tasks defined in the Customer SOW (the "TekSecure Project Manager"). The TekSecure Project Manager will schedule and host conference calls, send out status updates, coordinate the activities of the testing team and be responsible for the deliverable to Customer.

-
- B. Customer will provide its information for the project such as company IP information, coordinate facility access for on-site engagements, and execution of the Acceptance Form. Customer will also provide customer specific information needed to perform the engagement in a timely manner. Specific activities could include providing company IP addresses, providing firewall configurations, determining authorized hours to perform testing and coordinating the acquisition of available work space for any on-site work performed at the Customer facility.
 - C. Embarq will provide an account manager to coordinate with Customer establishment of a project schedule, manage changes to the project schedule, and provide project status reports. Customer designated, authorized employee or agent will provide approvals, on Customer's behalf, for all Services provided by Embarq.

8.2. Engagement Tracking, Communications, and Escalation. Embarq will provide a weekly status report that it will review with Customer, as requested by Customer and Embarq. The format of the status report will be coordinated by Customer and Embarq. Customer must initiate and maintain timely communication with Embarq regarding the Services. As part of the initial planning meeting among the engagement team defined above, an escalation path among Embarq and Customer will be established.

8.3. Cancellation of Service Orders. Customer SOWs may be cancelled by Embarq at any time. If Embarq cancels a Customer SOW prior to Embarq's delivery of the Services, there will be no cost to Embarq. If Embarq cancels a Customer SOW after or during delivery of the Services, Customer will pay Embarq for Services already provided to the Customer prior to such cancellation.

9. ADDITIONAL TERMS.

9.1. Embarq reserves the right to utilize sub-contractors and agents as needed to provide the Services. Embarq remains responsible and primarily liable for all work performed by sub-contractors and agents pursuant to the Agreement.

9.2. Activities to complete the tasks are based on accurate and validated information provided by Customer. Should any of this information prove to be inaccurate, Embarq will evaluate the impact of the misinformation, and initiate a change request if required. The change request may include changes in scope, schedule, and/or price. Embarq will not be held liable for any inaccuracies, errors or misstatements resulting from incorrect information provided by Customer or Customer network devices, that later affect Customer's environment.

9.3. Due to the nature of the assessment being performed, unintentional service disruption is possible even with destructive probing disabled. Embarq will not be held responsible for interruptions of the Customer's network services during the security assessment activities.

9.4. Embarq and Customer understand and agree that the performance of this service, as provided in accordance with this proposal, may improve the Customer's security posture. However, these services can neither identify nor eliminate all risks by unauthorized or authorized parties to affect the Customer's environment. Further, this project is limited in scope to the work tasks listed; Embarq will not be held liable for modifications made to the Customer network implemented after completion of this service, whether or not said modifications are made as a result of the service.

9.5. Embarq's delivery of Services to Customer may involve testing and activities which could result in unforeseen consequences. Embarq and Customer will agree in advance to the scope of such activities. If additional details are required, such will be set forth in a testing authorization form, which shall be a part of the Customer SOW between the parties.

10. ADDITIONAL TERMS

10.1. Activities to complete the tasks described in this Annex are based on accurate and validated information provided by Customer. Should any of this information prove to be inaccurate, Embarq will evaluate the impact of the misinformation and may, if required, initiate a change in the Services.

Changes may include changes in scope, schedule, and price. Embarq is not liable or responsible for any inaccuracies, errors or misstatements resulting from incorrect information provided by or through Customer or Customer's network devices, that later affect the Customer's environment.

- 10.2.** Embarq and Customer understand and agree that the performance of Services may improve Customer's security posture. But Services can neither identify nor eliminate all risks by unauthorized or authorized parties to affect Customer's environment. Services are limited to the description in this Annex, and Embarq is not liable or responsible for modifications made to Customer's network implemented after completion of Services, whether or not the modifications result from the Services.

EXHIBIT A

FORM OF CUSTOMER SOW

EMBARQ SECURITY ASSESSMENT SERVICES PROPOSAL



Security Assessment Services

for

[customer_name]

[proposal_date]

Embarq and its agent, TekSecure Labs, (collectively referred to here as “Embarq”) propose to provide the professional services described in this proposal to [customer_name] (“Customer”) to assess the Customer’s security posture. This assessment task includes:

- **External Target Identification** scanning of up to [eti_number_name] ([eti_number_digit]) Internet accessible host IP addresses to identify the number targets for a vulnerability scan or in-depth ethical hacking.
- **External Vulnerability Scan** of up to [evs_number_name] ([evs_number_digit]) IP addresses. Vulnerability scanning relies on the use of automated tools with a review by a senior security engineer.
- **External PCI Scan** of up to [pci_number_name] ([pci_number_digit]) IP addresses for four (4) quarters to identify risks to the enterprises based on attack methodologies from external network interfaces.
- **External Ethical Hacking** of up to [eh_number_name] ([eh_number_digit]) Internet accessible host IP addresses.
- **Web Application Security Testing** of the components of [wat_number_name] ([wat_number_digit]) external (Internet accessible) IP address to include the operating system platform, web server, middleware, and associated databases. The test will encompass the following:

[wa_url]

- **Internal Target Identification** scanning of up to [iti_number_name] ([iti_number_digit]) Internet accessible host IP addresses to identify the number targets for a vulnerability scan or in-depth ethical hacking.
- **Internal Vulnerability Scan** of up to [ivs_number_name] ([ivs_number_digit]) Intranet accessible host IP addresses. Includes initial ping sweep of Class-B sized network to identify targets.
- **Internal Ethical Hacking** of up to [ieh_number_name] ([ieh_number_digit]) Internet accessible host IP addresses.
- **Dial-In Access Security Testing** for up to [ms_number_name] ([ms_number_digit]) publicly accessible phone numbers with area codes in the United States.
- **Host Assessment** will be performed on up to [hbsa_number_name] ([hbsa_number_digit]) systems.
- **Wireless Security Testing** against up to [wst_number_name] ([wst_number_digit]) 802.11b or 802.11g Wireless Access Point(s).
- **Firewall Analysis** will be performed on the firewall configurations will consist of an evaluation of the firewall rules.
- **Assessment Report** will outline a company’s security compliance regulations to industry standards.

The task descriptions, deliverables, schedule, and dependencies will be discussed in the sections below.

Embarq shall provide a strategic assessment of Customer’s security posture, and then provide documentation and advice showing Customer how to achieve the desired end-point. This end point shall be a situation such that Customer’s security posture is equivalent to those of Customer’s peers in the industry, with due regard to applicable parts of common industry standards and practices.

A methodology and process description is provided for each proposed service.

External Target Identification

Often times a client may know that they own a network range, but are unsure of the active IP addresses on their external network. Embarq can perform broad scans of large network segments to identify active systems for a vulnerability scan or in-depth ethical hack.

Embarq will scan [iti_number_name] ([iti_number_digit]) IP addresses and identify active hosts on the network. This information will be used in conjunction with the vulnerability scanning or ethical hacking services.

External Vulnerability Scanning

After the set of [customer_name] Internet accessible addresses is defined in the reconnaissance phase, Embarq will meet with [customer_name] to determine which addresses will be included in the full vulnerability scan and in-depth ethical hacking. Vulnerability scanning identifies information about the operating system, network services, applications, and versions of those items that are active on targeted systems. After the configuration of the systems and networks is defined in more detail, exploitable vulnerabilities known to exist in those configurations are identified and documented. In addition, data collected by the tools may allow the test team to identify operating systems in use on those systems, and network service applications that are available (SMTP, DNS, HTTP, etc). External scanning (i.e. performed across the Internet) will reveal the services that are available on targeted systems from outside the [customer_name] environment. Any vulnerabilities will be identified and documented, but will not be exploited by the Embarq team.

The next phase of the vulnerability scanning process utilizes medium intensity probes to identify the versions of service applications that are in use. Identification of service application version information is useful because many vulnerabilities contained in network applications are version specific, and knowing the version number allows specific problems to be targeted. Embarq will develop a report that recaps the vulnerability scanning process and identifies the prioritized security findings and risks with risk mitigating recommendations. The vulnerabilities and risks levels are clearly listed for the overall test, and by system. The report also includes a listing of each active system identified during the scan, and all vulnerabilities that may be found on each system. Each vulnerability listing includes a description and recommendation for corrective action.

A full vulnerability scanning report will be delivered for the entire set of systems that were included in the vulnerability scan.

PCI Scanning

The vulnerability scanning service provided by Embarq has been certified as Payment Card Industry (PCI) compliant by the PCI Security Council. MasterCard, Visa, American Express, and Discover also recognize this certification

The customer provides an initial list of Internet accessible IP addresses targeted for vulnerability scanning. Embarq will verify that the list is comprehensive using PCI compliant network discovery techniques. The scans identify IP addresses that are active on the network, and information about the operating system, network services, applications, and versions of those items that are active on targeted systems. After the configuration of the systems and networks is defined in more detail, exploitable vulnerabilities known to exist in those configurations are identified and documented. In addition, data collected by the tools may allow the test team to identify operating systems in use on those systems, and network service applications that are available (SMTP, DNS, HTTP, etc). External scanning (i.e. performed across the Internet) will reveal the services that are available on targeted systems from outside the customer's environment. Any vulnerabilities will be identified and documented, but will not be exploited by the Embarq team.

The next phase of the vulnerability scanning process utilizes medium intensity probes to identify the vulnerabilities and the recommended remediation procedures for eliminating these vulnerabilities.

Embarq will develop a report that recaps the vulnerability scanning process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides a PCI standard "Pass" or "Fail" status for the network, based on the vulnerabilities identified and the risks associated with those vulnerabilities. The vulnerabilities and risks levels are clearly listed for the overall test, and by system. The report also includes a listing of each active system identified during the scan, and all vulnerabilities that may be found on each system. Each vulnerability listing includes a description and any recommendation for corrective action.

A report will be delivered in electronic format within one (1) week of the completion of each vulnerability scan. The initial vulnerability scan will be performed within one (1) week of contract signing, and three (3) subsequent vulnerability scans will be performed at three (3) month intervals.

External Ethical Hacking

Embarq will employ what are commonly known as “soft” reconnaissance techniques to collect information from public information sources, such as newsgroups, web sites, and registration databases. Embarq will use this information to determine user email addresses, job functions, and current projects. This information will help Embarq determine the technology that is deployed in a company’s environment, allowing the testing team to focus and tune its attacks to specific types of platforms.

This initial step will also help identify and confirm the ownership of the networks and systems the customer has submitted for testing, as well as the identities of service providers and systems that are active on a network. Service port numbers that are open on the systems identified, as well as traffic filtering that may be in place anywhere between the attacking and targeted systems. The information obtained during this process helps to verify the set of systems defined for testing, and provides a framework for more in-depth testing that occurs during the next phase.

During Phase II, the provided list of targets (from Phase I) is used for more in-depth scans that attempt to identify the operating system, network services, applications, and versions of those items that are active on target systems. After the configuration of the systems and networks is defined in more detail, exploitable vulnerabilities known to exist in those configurations are identified and documented. In addition, data collected by the tools may allow the test team to identify operating systems in use on those systems, and network service applications that are available (SMTP, DNS, HTTP, etc). Scanning will reveal the services that are available on routers, firewalls, and servers from outside the customer environment.

During Phase II, medium intensity probes are used to identify the versions of service applications that are in use. Identification of service application version information is useful because many vulnerabilities contained in network applications are version specific, and knowing the version number allows specific problems to be targeted. These types of tests typically involve use of telnet and DNS probes by the test team from the keyboard or via customized scripts that collect information about services in use. The information about systems behind the firewall that is collected during these tests can also help illustrate the effectiveness and implementation of the firewall’s filtering rules and configuration.

Once the operating system and application versions have been identified, specific exploits can be identified for the ensuing attack plan. Embarq always works closely with the customer to determine whether specific vulnerabilities are approved to be exploited. A customer may determine that leaving a vulnerability open for exploit is too risky, and it should be immediately corrected rather than being allowed to remain open for even for short duration during testing. In some cases a vulnerability can be “partially” exploited to verify it exists, but no action is taken to actually enter a system, or expand access or privileges. Embarq will provide expert advice on vulnerability assessment and testing plan procedures, but in all cases the customer has the final word on how exploit testing will be performed.

Finally Embarq will try to exploit the vulnerabilities identified during previous tests in an effort to confirm the vulnerability itself, and to leverage any access gained to other systems on the targeted network. Exploit scripts and procedures obtained from the Internet and other sources are used to exploit identified vulnerabilities. After initial access is gained to a single system on the network, trust relationships between systems and networks can often be used to access other systems on the network.

Password files that can be obtained will have password cracking tools run against them. Network sniffers will be installed where possible to monitor the network for other user account and password information. This will help illustrate the extent to which the network can be compromised, if even a single system with a vulnerable configuration is available online. Since this type of activity involves exploitation of trust relationships from valid accounts on the internal network, it is unlikely that an intrusion detection system will identify these types of tests.

Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides a methodology of the testing process,

vulnerabilities found, recommendations for corrections, and an analysis of strengths and weaknesses. The security risks will be risk-ranked so that the most critical risks can be addressed first.

As part of this phase Embarq will provide knowledge transfer with CUSTOMER staff to help promote an understanding of how potential problems were identified, corrective actions that can be taken, and the impact of corrective actions on business operations and security. The Internet based testing will be performed remotely from an Embarq facility.

Note: The Ethical Hacking team will not use the access or privileges gained on any system to intentionally modify data, delete files, or cause any other type of damage or service interruptions during Phase II.

External Ethical Hacking will be performed on up to [eh_number_name] ([eh_number_digit]) Internet accessible IP addresses for in-depth ethical hacking. The ethical hacking will be performed remotely from Embarq designated facilities. Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides:

- Methodology of the testing process
- Vulnerabilities found
- Recommendations for corrections,
- Analysis of strengths and weaknesses:
- Ranking of security risks so that the most critical risks can be addressed first.

Internal Target Identification

Often times a client may know that they own a network range, but are unsure of the active IP addresses on their external network. Embarq can perform broad scans of large network segments to identify active systems for a vulnerability scan or in-depth ethical hack.

Embarq will scan [iti_number_name] ([iti_number_digit]) network ranges and identify active hosts on the network. This information will be used in conjunction with the vulnerability scanning or ethical hacking services.

Internal Vulnerability Scanning

After the set of [customer_name] Internet accessible addresses is defined in the reconnaissance phase, Embarq will meet with [customer_name] to determine which addresses will be included in the full vulnerability scan and in-depth ethical hacking. Vulnerability scanning identifies IP addresses that are active on the network, and information about the operating system, network services, applications, and versions of those items that are active on targeted systems. After the configuration of the systems and networks is defined in more detail, exploitable vulnerabilities known to exist in those configurations are identified and documented. In addition, data collected by the tools may allow the test team to identify operating systems in use on those systems, and network service applications that are available (SMTP, DNS, HTTP, etc). External scanning (i.e. performed across the Internet) will reveal the services that are available on targeted systems from outside the [customer_name] environment. Any vulnerabilities will be identified and documented, but will not be exploited by the Embarq team.

The next phase of the vulnerability scanning process utilizes medium intensity probes to identify the versions of service applications that are in use. Identification of service application version information is useful because many vulnerabilities contained in network applications are version specific, and knowing the version number allows specific problems to be targeted. Embarq will develop a report that recaps the vulnerability scanning process and identifies the prioritized security findings and risks with risk mitigating recommendations. The vulnerabilities and risks levels are clearly listed for the overall test, and by system. The report also includes a listing of each active system identified during the scan, and all vulnerabilities that may be found on each system. Each vulnerability listing includes a description and recommendation for corrective action.

Embarq will perform internal vulnerability scanning on up to [ivs_number_name] ([ivs_number_digit]) Internet-accessible IP addresses. A full vulnerability scanning report will be delivered for the entire set of systems identified during the vulnerability scan.

Internal Ethical Hacking

Embarq will use information from the Internal Target Identification to determine targets for performing the ethical hacking. These targets will be used for more in-depth scans that attempt to identify the operating system, network services, applications, and versions of those items that are active on target systems. After the configuration of the systems and networks is defined in more detail, exploitable vulnerabilities known to exist in those configurations are identified and documented. In addition, data collected by the tools may allow the test team to identify operating systems in use on those systems, and network service applications that are available (SMTP, DNS, HTTP, etc). Scanning will reveal the services that are available on routers, firewalls, and servers from outside the customer environment.

During Phase II, medium intensity probes are used to identify the versions of service applications that are in use. Identification of service application version information is useful because many vulnerabilities contained in network applications are version specific, and knowing the version number allows specific problems to be targeted. These types of tests typically involve use of telnet and DNS probes by the test team from the keyboard or via customized scripts that collect information about services in use. The information about systems behind the firewall that is collected during these tests can also help illustrate the effectiveness and implementation of the firewall's filtering rules and configuration.

Once the operating system and application versions have been identified, specific exploits can be identified for the ensuing attack plan. Embarq always works closely with the customer to determine whether specific vulnerabilities are approved to be exploited. A customer may determine that leaving a vulnerability open for exploit is too risky, and it should be immediately corrected rather than being allowed to remain open for even for short duration during testing. In some cases a vulnerability can be "partially" exploited to verify it exists, but no action is taken to actually enter a system, or expand access or privileges. Embarq will provide expert advice on vulnerability assessment and testing plan procedures, but in all cases the customer has the final word on how exploit testing will be performed.

Finally Embarq will try to exploit the vulnerabilities identified during previous tests in an effort to confirm the vulnerability itself, and to leverage any access gained to other systems on the targeted network. Exploit scripts and procedures obtained from the Internet and other sources are used to exploit identified vulnerabilities. After initial access is gained to a single system on the network, trust relationships between systems and networks can often be used to access other systems on the network.

Password files that can be obtained will have password cracking tools run against them. Network sniffers will be installed where possible to monitor the network for other user account and password information. This will help illustrate the extent to which the network can be compromised, if even a single system with a vulnerable configuration is available online. Since this type of activity involves exploitation of trust relationships from valid accounts on the internal network, it is unlikely that an intrusion detection system will identify these types of tests.

Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides a methodology of the testing process, vulnerabilities found, recommendations for corrections, and an analysis of strengths and weaknesses. The security risks will be risk-ranked so that the most critical risks can be addressed first.

As part of this phase Embarq will provide knowledge transfer with customer staff to help promote an understanding of how potential problems were identified, corrective actions that can be taken, and the impact of corrective actions on business operations and security. The Internet based testing will be performed remotely from an Embarq facility.

Note: The Ethical Hacking team will not use the access or privileges gained on any system to intentionally modify data, delete files, or cause any other type of damage or service interruptions during Phase II.

Internal Ethical Hacking will be performed on up to [ieh_number_name] ([ieh_number_digit]) Internet accessible IP addresses for in-depth ethical hacking. The ethical hacking will be performed remotely from Embarq designated facilities. Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides:

- Methodology of the testing process

-
- Vulnerabilities found
 - Recommendations for corrections,
 - Analysis of strengths and weaknesses:
 - Ranking of security risks so that the most critical risks can be addressed first.

Web Application Security Test

The web application security testing process consists of an in-depth evaluation of all the major components of a typical web application to include the operating system, web server platform, middleware, and associated databases. The test can be performed from the perspective of an internal or external user of an application, and attempts to determine what type of access an attacker could gain using publicly available hacking tools and techniques. Playing the role of an attacker, the objectives of the test team would be to gain access to the network with the intent to steal or manipulate data that resides there, or to deface the web site. The team will not actually perform any of these malicious acts during the testing process, but will attempt to identify ways an attacker with those objectives could find entry to the network and its systems.

The web applications that are targeted will be evaluated for vulnerabilities in the operating system, web server, middleware, and any associated databases that are accessible. Vulnerabilities that can affect the platform include those that could allow unauthorized access to the system, modification of web site content, viewing and modifying other users' data, or access to entire databases. If possible and applicable, the team will also attempt to gain elevated privileges and expand access to other systems on the network. Any attempt to gain elevated privileges or expand access to other systems would ONLY be done after gaining explicit approval from the customer. System logs and screenshots collected during the testing process can help illustrate the presence and risk of certain vulnerabilities without performing an exploit, and Embarq will use these resources to document and support findings in the reports.

Note that for applications that allow user logins, five (5) temporary test accounts are required to be set up on the application for testing purposes. Additional accounts may be required depending on the number and types of roles that are defined by the application. The test accounts are used in determining whether an authorized user or customer of the application could break out of their defined security role to access and manipulate other users' data, or databases associated with the application. The team will provide a report at the end of the testing process that includes a list of vulnerabilities with associated corrective actions for the tested application. The team will provide immediate verbal notification of all HIGH priority vulnerabilities identified in the web-based application during the testing process. Web Application Security Tests are performed the process defined in six (6) task steps that are summarized below.

- Task 1: Verification of target information and basic scanning and identification procedures used to identify operational systems and service.
- Task 2: Probing the identified systems for known vulnerabilities.
 - i. In depth scans of all 65,535 ports to identify the operating system, network services, applications, and versions of those items that are active on target systems.
 - ii. Identify the versions of service applications that are in use.
 - iii. Identify candidate exploits, and develop an attack plan.
- Task 3: Exploiting of web server vulnerabilities in a manner to identify what an attacker would be capable of.
 - Active scans are performed using commercial, public, and custom tools designed to identify and/or exploit specific vulnerabilities.
 - Scans for default material.
- Task 4: Exploiting of database vulnerabilities, if accessible, in a manner to identify what an attacker would be capable of.
 - Active scans are performed using commercial, public, and custom tools designed to identify and/or exploit specific vulnerabilities.
 - Attempt connections with default usernames and passwords.

-
- Task 5: Exploiting of middleware vulnerabilities in a manner to identify what an attacker would be capable of.
 - Use proxy to intercept and change data transmissions to determine effect on application.
 - Task 6: Exploiting of the application to identify what an attacker would be capable of.
 - Active scans are performed using commercial, public, and custom tools designed to identify and/or exploit specific vulnerabilities.
 - The following items are tested for potential weaknesses:
 - Authentication
 - Account Lockout
 - Buffer Overflows
 - Error messages
 - Password Policy
 - Session Tracking
 - Session Hi-jacking
 - IP hopping
 - Concurrency
 - Proper Cookie Usage
 - Session timeouts
 - Encryption
 - Username Harvesting

Web Application Security Testing will be performed on [wat_number_name] ([wat_number_digit]) Internet accessible web-based application owned by the Customer, and their background databases. The testing of the Internet accessible web-based application will be performed remotely from Embarq designated facilities. Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides:

- Methodology of the testing process
- Vulnerabilities found
- Recommendations for corrections,
- Analysis of strengths and weaknesses:
- Ranking of security risks so that the most critical risks can be addressed first.

Dial-In and Remote Access Security Testing

Embarq will conduct Dial-In Access Security Testing, also known as a wardial, against a list of phone numbers provided by [customer_name], and will perform an ethical hack against modem-connected devices that are discovered. The numbers can be dialed at specified time intervals, or during business and non-business hours, at [customer_name]'s discretion. Dial-in testing, data analysis, and report writing will be done remotely from Embarq facilities.

Results are recorded, analyzed, and provided as a vulnerability snapshot of the modem connections available during the time the test was performed. The modem security testing service follows this methodology.

- All numbers are dialed and results, banners, login screens, or modem responses, are recorded into a log file for analysis. If the number is busy, disconnected, or unresponsive at the time of the test, then it will be labeled as such. Busy numbers are dialed twice in an effort to identify all “carriers” (modem connections). Identification of the type of system providing modem connectivity occurs in this phase.
- Ethical hacking is performed against identified modem-connected devices. Each number identified as a data “carrier” (i.e. potential modem) is dialed again. Attempts are then made to gain access to the device via the modem connection. The activity of the connection is recorded. If access is achieved through the modem connection, the level of access is identified. Further access into the host and or network can be attempted at the discretion of [customer_name].

Dial-In Access Security Testing will be performed on up to [ms_number_name] ([ms_number_digit]) publicly accessible U.S. based phone numbers owned by [customer_name]. Dial-In Access Security Testing will be performed remotely from Embarq facilities.

Host Based Security Assessment

Host Security Assessments are a hands-on collection and analysis of a system's security configuration data. A system can be a server, router, firewall, IDS, or other type of device located within the customer's IT environment. Certain aspects of a system's configuration and security posture cannot be remotely analyzed across a network, and must be done in a hands-on manner. Automated tools and system commands are used to collect data related to system and application settings that can impact the security of the system. The process includes evaluating the patch level, network services that are running, significant applications installed on the system, and account management. Embarq will examine, review, assess and provide recommendations for improving the security of systems that are assessed.

Note that the operating system type, and number of each type included in the host security assessment must be provided to Embarq at the time of contract signature, to make sure the testing team assembles the appropriate set of tools and procedures to perform the tests. The types of systems involved in the assessment will also be a factor in determining the specific staff assignments for this task, as task assignments are based on expertise with specific types of technologies.

The Host Security Assessment will require the Embarq test team to have system administrator privileges at the console on each device in order to run the tools and commands needed to collect the required data. If this is not possible, then Embarq can work with customer to have a member of customer's staff run the tools and commands, and collect and transfer the data to Embarq for review. All systems included in the host security assessment are assumed to be located at one (1) mutually agreed customer facility, or other location local to that area. Tools are either loaded from a CD or downloaded from an Embarq laptop computer connected to the network. The security assessment tools will evaluate the system and security configuration settings of the specific system being evaluated, to look for potential problems. Data generated by the tools is dumped to files on the system being assessed. The data is typically collected and moved to an Embarq system for analysis to minimize the access and time required on the customer system. The time required for the tools to run and data collection to complete can vary depending on the type of operating system in use, the type of processor, and the number of files and users on the system.

The data is analyzed for potential problems involving issues such as user account management settings, file and directory permissions, and network service configurations. Issues that are identified as findings are documented, and recommendations for corrective actions are provided. Findings are generated and reviewed in close communication with the customer to promote data is interpreted in the proper technical and business context.

The server devices included in the host security assessment can be any combination of the following operating system types; Windows 2000/NT, AS/400, Solaris, HP-UX, AIX, or Linux.

A Host Security Assessment will be performed on up to [hbsa_number_name] ([hbsa_number_digit]) systems. The security assessment will be performed as one (1) customer facility. Includes at least 1 business day of onsite work per eight (8) systems reviewed by an Embarq senior security engineer. Additional data analysis and report creation will be performed remotely from an Embarq facility. Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides:

- Methodology of the testing process
- Vulnerabilities found
- Recommendations for corrections,
- Analysis of strengths and weaknesses:
- Ranking of security risks so that the most critical risks can be addressed first.

802.11 Wireless Security Testing

802.11 Wireless security testing focuses on the configuration and accessibility of wireless access points (WAP's) connected to a corporate network. These can be devices that are authorized and deployed by the organization, or rogue devices set up by employees or someone else with access to the facility. WAP's that are identified are assessed for configuration information, vulnerabilities, and security settings. The wireless portion of the exercise must be performed locally and will require travel expenses for Embarq to work on customer's site. The actual attacks must be conducted in close proximity to the customer's network, since the range of the RF signal for wireless LANs is typically only a few hundred feet.

During the attack, Embarq will attempt to break into the wireless access point and access any systems (WWW/FTP/SMTP servers, e-commerce servers and so on) identified on the network. Embarq can perform an attempt to break Wired Equivalent Privacy (WEP) encryption in order to demonstrate the tools and techniques used by hackers. If the customer wishes, we can attempt to break the WEP encryption on any identified wireless network, or define a level of effort that would be required to break the WEP key.

Optionally, the customer may opt to provide the encryption keys of known wireless networks. Once a wireless network has been compromised, research will be conducted to find vulnerabilities relating to the specific OS type and version, and software application (if applicable) of systems identified from the wireless network. A detailed log of all activities, and keystroke logs are recorded and provided to the customer to ensure complete documentation of the test and results.

Embarq will conduct a wireless ethical hack against up to [wst_number_name] ([wst_number_digit]) 802.11b or 802.11g WAPs at one (1) customer facility. Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides:

- Methodology of the testing process
- Vulnerabilities found
- Recommendations for corrections,
- Analysis of strengths and weaknesses:
- Ranking of security risks so that the most critical risks can be addressed first.

Firewall Configuration Review

The review of firewall configurations will consist of an evaluation of the firewall and Network Address Translation (NAT) rules. The firewall configuration provides front line protection from threats that are external to the network. A well configured firewall rule set helps to maximize protection of a network and the business operations it supports. A rule set can be configured to restrict access to services and systems on the internal network, and provide protection from certain types of network attacks such as denial of service attacks. The main objective of the review is to evaluate the firewall rule set configurations to determine if potential vulnerabilities exist through the external firewalls. Firewall rule sets can change over time as new business requirements require changes to be made in the level of access allowed for services and systems on the network. The need for certain rules to remain in a rule set can also change due to changes in business requirements and operations. Periodic review of rule firewall sets can help determine vulnerabilities and weaknesses that may have been introduced by new rules, and identify rules that are no longer required and can be removed.

The firewall rule set files will be provided by customer in order to eliminate the need for the Embarq test team personnel to have privileged access to the devices to obtain the information. The reviews will be performed in close coordination with key personnel responsible for the devices to help enable the Embarq test team has all the information about configuration settings related to business operations. Close coordination will also help enable knowledge transfer during this phase of the assessment process. Embarq will provide a report that includes:

- Description of the rule set
- Results of the analysis that was performed
- Recommendations for modifications that could be made to the firewall to enhance the security of the network it protects.

Assessment Report

Embarq will develop a report that outlines a company's security compliance regulations to industry standards. For example if a company needs to meet both GLBA and PCI requirements, Embarq can boil both regulations down into a single list of control objectives for the customer. This will save the customer time and effort by reducing duplicative effort where the regulations overlap.

Embarq will develop a concise list of control objectives and how those control objectives map back to each of the regulatory requirements. Embarq will provide a report that includes:

- Description of the each control objective
- List of applicable regulations that each of the control objective meets

External Ethical Hacking Approach - Reconnaissance

Embarq will employ what are commonly known as "soft" reconnaissance techniques to collect information from public information sources, such as newsgroups, web sites, and registration databases. Embarq will use this information to determine user email addresses, job functions, and current projects. This information will help Embarq determine the technology that is deployed in a Customer's environment, allowing the testing team to focus and tune its attacks to specific types of platforms.

This initial step will also help identify and confirm the ownership of the networks and systems the Customer has submitted for testing, as well as the identities of service providers and systems that are active on a network. Service port numbers that are open on the systems identified, as well as traffic filtering that may be in place anywhere between the attacking and targeted systems. The information obtained during this process helps to verify the set of systems defined for testing, and provides a framework for more in-depth testing that occurs during the next phase.

Ethical Hacking Approach - Vulnerability Assessment

The provided list of targets is used for more in-depth scans that attempt to identify the operating system, network services, applications, and versions of those items that are active on target systems. After the configuration of the systems and networks is defined in more detail, exploitable vulnerabilities known to exist in those configurations are identified and documented. In addition, data collected by the tools may allow the test team to identify operating systems in use on those systems, and network service applications that are available (SMTP, DNS, HTTP, etc). Scanning will reveal the services that are available on routers, firewalls, and servers from outside the Customer environment.

Next, medium intensity probes are used to identify the versions of service applications that are in use. Identification of service application version information is useful because many vulnerabilities contained in network applications are version specific, and knowing the version number allows specific problems to be targeted. These types of tests by the test team from the keyboard or via customized scripts that collect information about services in use. The information about systems behind a firewall that is collected during these tests can also help illustrate the effectiveness and implementation of the firewall's filtering rules and configuration.

Once the operating system and application versions have been identified, specific exploits can be identified for the ensuing attack plan. Embarq always works closely with the Customer to determine whether specific vulnerabilities are approved to be exploited. A Customer may determine that leaving a vulnerability open for exploit is too risky and it should be immediately corrected rather than being allowed to remain open for even the short duration during testing. In some cases a vulnerability can be "partially" exploited to verify it exists, but no action is taken to actually enter a system, or expand access or privileges. Embarq will provide expert advice on vulnerability assessment and testing plan procedures, but in all cases the Customer has the final word on how exploit testing will be performed.

Finally Embarq will try to exploit the vulnerabilities identified during previous tests in an effort to confirm the vulnerability itself, and to leverage any access gained to other systems on the targeted network. Exploit scripts and procedures obtained from the Internet and other sources are used to exploit identified vulnerabilities. After initial access is gained to a single system on the network, trust relationships between systems and networks can often be used to access other systems on the network.

-
1. Password files that can be obtained will have password cracking tools run against them. Network sniffers will be installed where possible to monitor the network for other user account and password information. This will help illustrate the extent to which the network can be compromised, if even a single system with a vulnerable configuration is available online. Since this type of activity involves exploitation of trust relationships from valid accounts on the internal network, it is unlikely that an intrusion detection system will identify these types of tests.
 2. As part of this phase Embarq will provide knowledge transfer with Customer staff to help promote an understanding of how potential problems were identified, corrective actions that can be taken, and the impact of corrective actions on business operations and security. The Internet based testing will be performed remotely from a Embarq facility.
 3. Note: The Ethical Hacking team will not use the access or privileges gained on any system to intentionally modify data, delete files, or cause any type of damage or service interruptions during the testing period.

External Ethical Hack will be performed on up to three hundred (300) Internet accessible IP address. The ethical hacking will be performed remotely from Embarq designated facilities. Embarq will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations. The report provides:

- Methodology of the testing process
- Vulnerabilities found
- Recommendations for corrections,
- Analysis of strengths and weaknesses:
- Ranking of security risks so that the most critical risks can be addressed first.

PCI Compliancy Scanning

The Tek+Detect scanning service provided by Embarq is certified by the PCI Security Council (certificate 3894-01-01) as compliant by the PCI Approved Scanning Vendors program. MasterCard, Visa, American Express, and Diners Club also recognize this certification. The customer provides a list of systems targeted for PCI vulnerability scanning. The customer will identify specific targets from the list of three hundred (300) that are targeted for Ethical Hacking in the previous phase, that need to be scanned and reported on for PCI compliancy. The first phase of this process is designed to identify the operating system, network services, applications, and versions of those items that are active on targeted systems. After the configuration of the systems and networks is defined in more detail, exploitable vulnerabilities known to exist in those configurations are identified and documented. In addition, data collected by the tools may allow the test team to identify operating systems in use on those systems, and network service applications that are available (SMTP, DNS, HTTP, etc). External scanning (i.e. performed across the Internet) will reveal the services that are available on targeted systems from outside the customer's environment. Vulnerabilities will be identified and documented, but will not be exploited by the Embarq test team.

The next phase of the vulnerability scanning process utilizes medium intensity probes to identify the versions of service applications that are in use. Identification of service application version information is useful because many vulnerabilities contained in network applications are version specific, and knowing the version number allows specific problems to be targeted. These types of tests typically involve use of telnet and DNS probes by the test team from the keyboard or via customized scripts that collect information about services in use. The information about systems behind any firewall that is collected during these tests can also help illustrate the effectiveness and implementation of the firewall's filtering rules and configuration.

Embarq will develop a report that states the overall PCI compliancy of the network, PCI compliancy by host, recaps the vulnerability scanning process and identifies the prioritized security findings and risks with risk mitigating recommendations. The security risks will be risk-ranked so that the most critical can be addressed first.

Software/hardware technologies that may be utilized

Embarq will create a more definitive and appropriate toolset for the assessment after more information is obtained about the types of platforms that will be evaluated and scanned at various points during the project. For example, if particular types of platforms and operating system version types are identified during the vulnerability scanning, a

specific set of tools will be used to further probe and potentially attempt to exploit vulnerabilities. The list of tools below is a good starting point for most assessments, and will be adjusted as needed for specific projects.

- **Nmap** – A freeware port scanner and traffic generator tool.
- **Nessus** – A freeware security scanning tool for identifying vulnerabilities. This tool also requires, as a prerequisite, the presence of nmap on the system used for the launch of the Nessus scan.
- **Webscanner** – An open-source Java/Perl script used to scan web sites for common configuration errors and software vulnerabilities.
- **Qualys Guard** – A commercial product used for assisting with the vulnerability scanning.
- **Burp Proxy** – A Java based web proxy used to capture or alter inbound and outbound http/https traffic. It runs on Windows, Linux and Solaris.

Embarq will also use customized scripts and command line operations for certain aspects of the project.

2.1 Anticipated Project Timeline

Estimates of the timeframe required for each of the individual services are provided in the list below. Some of the services could be performed in parallel, and the overall timeframe for performing all services in this proposal is estimated to take approximately four (4) weeks.

- External Target Identification will be performed by scanning up to [eti_number_name] (eti_number_digit) IP addresses. The time required to complete this task can vary on many factors from network size to firewall and router configuration; but is estimated to be no more than one (1) week.
- External Vulnerability Scanning of up to [evs_number_name] ([evs_number_digit]) Internet accessible host IP addresses. The time required to complete this task (including reporting) is estimated to be no more than three (3) weeks.
- PCI Scanning of up to [pci_number_name] ([pci_number_digit]) Internet accessible host IP addresses. The time required to complete this task (including reporting) is estimated to be no more than three (3) weeks.
- External Ethical Hacking of up to [eh_number_name] ([eh_number_digit]) Internet accessible IP addresses for in-depth ethical hack. The time required to complete this task can vary on many factors from network size to firewall and router configuration; but is estimated to be no more than three (3) weeks.
- Internal Target Identification will be performed by scanning up to [iti_number_name] (iti_number_digit) IP addresses. The time required to complete this task can vary on many factors from network size to firewall and router configuration; but is estimated to be no more than one (1) week.
- Internal Vulnerability Scanning of up to [ivs_number_name] ([ivs_number_digit]) Intranet accessible host IP addresses. The time required to complete this task (including reporting) is estimated to be no more than three (3) weeks.
- Internal Ethical Hacking of up to [ieh_number_name] ([ieh_number_digit]) Intranet accessible IP addresses for in-depth ethical hack. The time required to complete this task can vary on many factors from network size to firewall and router configuration; but is estimated to be no more than three (3) weeks.
- Web Application Security Test of [wat_number_name] ([wat_number_digit]) Internet accessible web-based application is estimated to take up to one (1) week.
- Dial in Access Testing for up to [ms_number_name] ([ms_number_digit]) publicly accessible phone numbers with area codes in the United States. The time required to complete this task (including reporting) is estimated to be no more than three (3) weeks.
- Host Assessment of [hbsa_number_name] ([hbsa_number_digit]) systems will be performed at one (1) customer facility. Includes at least 1 business day of onsite work per eight (8) systems. The time required to complete this task (including reporting) is estimated to be no more than three (3) weeks.

- 80211 wireless testing of [wst_number_name] ([wst_number_digit]) 802.11b or 802.11g WAPs at one (1) customer facility. The time required to complete this task (including reporting) is estimated to be no more than two (2) weeks.
- Firewall configuration review of one (1) firewall. The time required to complete this task (including reporting) is estimated to be no more than one (1) week.
- Assessment report. The time required to complete this task (including reporting) is estimated to be no more than two (2) weeks.

3.0 CUSTOMER RESPONSIBILITIES:

- Designate a single point of contact (SPoC) for all project support issues within the scope of this project. Such person shall have the authority to act on all Customer aspects of the Services.
- Ensure that Embarq's request for information or documentation is delivered within the agreed upon timeframe.
- Notify the Embarq Project Manager of any schedule changes at least five (5) business days prior to the date of task delivery. Any Customer-scheduled requests with less than five (5) business day's prior notice will incur additional charges in the form of a rescheduling fee.
- Customer's SPoC shall participate in meetings to resolve all engagement related issues and shall make its personnel readily available for such meetings.
- Customer will keep Embarq informed of any information or changes, which may affect Embarq's performance of services.
- Customer shall provide Embarq with reasonable access to the premises of Customer facilities if needed. The designated Customer facility will be mutually agreed upon. Customer will make available to Embarq personnel office space and/or the appropriate facilities (without charge) including computer services, presentation aids, if required.
- If requested, Customer shall provide programming and operations documentation standards in writing to Embarq.
- Customer must provide Embarq with other mutually agreed upon specific information necessary to perform the security consulting that may not be readily available within Embarq. Embarq will identify the required information and both parties will agree on the times at which this information will be provided. The work schedule will be devised in accordance with the availability of information.
- In addition to providing Embarq with full, good faith cooperation and such information as may be reasonably required by Embarq in order to perform its obligations hereunder, Customer shall:
 - Make available to each Embarq employee physically located on Customer premises: computer time and an analog data connection sufficient for Embarq to properly perform its obligations hereunder. This will be during regular working hours and such additional hours as reasonably requested by Embarq to provide the Services and Deliverables
 - In general, to provide all necessary computer services, information and access to key personnel needed to provide the Services and Deliverables
- The work items do not include the implementation of any suggested or recommended changes to Customer's network or security policy.

3.1 Change Control Procedure

Embarq manages changes that have cost or schedule impact as contractual changes through a disciplined contracting process. Either Party must submit change requests to contractual documents in writing. The party requesting the change must submit a written request to the other party and the receiving party shall issue a written response within

five (5) business days of the receipt of the request, including whether the receiving party accepts or rejects the request and/or any changes to the Terms and Conditions. Once agreed upon, both parties must execute the change control document.

3.2 Approval/Acceptance

Embarq and the customer will mutually agree on the process steps necessary to achieve Acceptance of the Services during the start-up period for the Project.

4.0 Schedule of Fees

Embarq shall provide the Services for a fixed fee. Embarq will invoice the Service Fees upon Acceptance, as defined in Table 1 below. Prices quoted herein are valid for sixty (60) days from the date this proposal is presented to the Customer for execution; in the event this proposal is not executed by the Customer within sixty (60) days, Embarq reserves the right to modify the pricing, terms and/or conditions herein. This engagement must commence within ninety (90) days of the Effective Date, or Embarq reserves the right to modify the pricing, terms and/or conditions herein.

Table 1: Pricing Breakdown

Work Item	Price	Consultant Level
External Target Identification <ul style="list-style-type: none"> • scanning of up to [eti_number_name] ([eti_number_digit]) of Internet accessible host IP addresses to identify the number targets for a vulnerability scan or in-depth ethical hacking. 		
External Vulnerability Scan <ul style="list-style-type: none"> • Vulnerability Scanning of up to [evs_number_name] ([evs_number_digit]) IP addresses. • Data analysis and report creation 		
PCI Scanning <ul style="list-style-type: none"> • Vulnerability Scanning of up to [pci_number_name] ([pci_number_digit]) IP addresses. • Data analysis and report creation 		
External Ethical Hacking <ul style="list-style-type: none"> • Scanning of a maximum of one thousand twenty four (1024) Internet accessible IP addresses to identify a target list • Targeting of a maximum of [eh_number_name] ([eh_number_digit]) Internet accessible IP addresses for in-depth phase of ethical hacking. • Data analysis and report creation 		

<p>Web Application Security Testing</p> <ul style="list-style-type: none"> • Security Testing of [wat_number_name] ([wat_number_digit]) Internet accessible web-based application • Data analysis and report creation 		
<p>Internal Target Identification</p> <ul style="list-style-type: none"> • Scanning of up to [eti_number_name] ([eti_number_digit]) or Internal accessible host IP addresses to identify the number targets for a vulnerability scan or in-depth ethical hacking. 		
<p>Internal Vulnerability Scan</p> <ul style="list-style-type: none"> • Vulnerability Scanning of up to [evs_number_name] ([evs_number_digit]) IP addresses. • Data analysis and report creation 		
<p>Internal Ethical Hacking</p> <ul style="list-style-type: none"> • Scanning of a maximum of one thousand twenty four (1024) Internet accessible IP addresses to identify a target list • Targeting of a maximum of [eh_number_name] ([eh_number_digit]) intranet accessible IP addresses for in-depth phase of ethical hacking. • Data analysis and report creation 		
<p>Dial-In Modem Scan Testing</p> <ul style="list-style-type: none"> • Scan up to [ms_number_name] ([ms_number_digit]) publicly accessible phone numbers • Ethical hack for up to XXX (X) modems identified during the phone number scan. • Data analysis and report creation 		
<p>Host Assessment</p> <ul style="list-style-type: none"> • Host Scan will be performed on up to [hbsa_number_name] ([hbsa_number_digit]) systems. • Data analysis and report creation 		
<p>Wireless Security Testing</p> <ul style="list-style-type: none"> • Testing against up to [wst_number_name] ([wst_number_digit]) 802.11b or 802.11g Wireless Access Point(s). • Data analysis and report creation 		
<p>Firewall Analysis</p> <ul style="list-style-type: none"> • Firewall Analysis will be performed on the firewall configurations • Data analysis and report creation 		

Assessment Report <ul style="list-style-type: none"> Will outlines a company's security compliance regulations to industry standards. 		
Total	\$ plus expenses	

4.1 Travel and Material Expenses

The Parties agree that the engagement meetings will be conducted using teleconference calls and all work will be executed at a Embarq facility unless other arrangements have been agreed upon. If Customer's requires Embarq personnel to travel to perform work on or visit a client site, or attend a meeting with Customer's staff, standard business expenses, (e.g., travel; food and lodging) Embarq personnel incur in connection with provisioning services under this proposal will be invoiced separately to Customer's.

4.2 Taxes

All taxes, excise fees, and other expenses are the responsibility of Customer and have not been included in the above-listed pricing.

4.3 Time and Material Rate

In the event that the scope of work changes, Embarq will bill Customer at a Time & Materials ("T&M") increased rate of two hundred fifty dollars (\$250) per hour for the additional time spent on the change requests.

5.0 Engagement Assumptions

The proposal outlined herein is based on the below assumptions:

- The Project Scope is based upon the activities and services listed in this proposal, which is valid for sixty (60) days from the date presented to the Customer.
- Initiation of the security services will occur within ninety (90) days following the contract signature.
- Schedule change requests made within this proposal or requests to expedite work activities will be made through the designated Customer SPOC to the Embarq Project Manager, which may result in a change in contract fees and pricing.
- Activities to complete the tasks outlined in this proposal are based on accurate and validated information provided by the Customer.
- Embarq and the Customer understand and agree that the performance of this service, as provided in accordance with this proposal, may improve the Customer's security posture. However, these services can neither identify nor eliminate all risks by unauthorized or authorized parties to affect the Customer's environment. Further, this project is limited in scope to the work tasks listed. Embarq will not be held liable for any inaccuracies, errors or misstatements that later affect the Customer's environment.
- During the review and analysis phase, Embarq will need to have ad-hoc access to the Customer personnel. This ongoing access will allow resolution of any questions or issues as they arise.

-
- For each task, Embarq requires certain information such as IP addresses specified in this text, along with contact information, for the execution of this engagement. This information will be determined in the initial project scope and requirements meeting.
 - Customer shall ensure that any requested review and approval of information prepared by Embarq is delivered in a timely manner, so as to permit Embarq to properly perform its obligations hereunder.
 - The Customer is responsible for the accuracy of all information supplied to Embarq by the Customer designated project team and Embarq relies upon in the performance of this Agreement.
 - In the event that access is gained to any server, firewall or router, Embarq will stop the attack and seek guidance from the Customer. Any severe security problems found will be escalated immediately to the Customer contact.
 - The following services are not included in this proposal: (a) denial of service, (b) social engineering, and (c) removing vulnerabilities identified by the security assessment services.
 - This document is for planning purposes only. Final terms and conditions will be subject to a written contract to be mutually agreed upon in writing by both parties.