verizonbusiness
Security Solutions powered by Cybertrust

Verizon® Security Services Description for Verizon Core

May 2, 2008, Version 1.1

www.verizonbusiness.com

Verizon Security Solutions
22001 Loudoun County Parkway
Ashburn, VA 20147
Phone (703) 886.5600
Fax (703) 886.0861

I. Introduction

Verizon, Inc. (Verizon) will address your requirements through a professional services engagement with highly qualified Verizon Security Consultants and Engineers using the full security intelligence and research capabilities of Verizon. Methodologies are included for the following services:

- Network Vulnerability Assessment
- System and Platform Security Testing
- Business Security Assessment

II. Methodologies

Network Vulnerability Assessment Description

The objective of the network vulnerability assessment is to identify security weaknesses exposed to the Internet that could be exploited by motivated malicious individuals to gain unauthorized access to your external systems, which could then expose critical systems to an attack.

Verizon will use a series of vulnerability scanning tools and a proprietary methodology to identify and validate Internet security vulnerabilities. Unlike traditional Vulnerability Scanning that produces large numbers of vulnerabilities in endless lists, Verizon's scanning provides an order-of-magnitude improvement in prioritizing vulnerability remediation. An integrated Topology Risk Analyzer computes network "line-of-sight" risk to prioritize vulnerabilities and report the "short list" that pose the most risk to critical systems.

It should be noted that while these automated techniques are useful and can yield important information, they give an incomplete picture of an organization's security posture. The real test of company's security posture though is when highly motivated and technically competent security consultants begin utilizing the reconnaissance information gained by the automated tools to begin examining the target the organization. No automated tool or standard procedures will test a system like being probed by a human mind. This is where Verizon provides real value to our customers.

Testing activities are closely coordinated wit the customer during the testing process. Throughout the engagement, the Verizon team will share results with your organization's authorized personnel to maximize information transfer. Where Verizon identifies critical or high-risk vulnerabilities, your designated project point-of-contact will be notified. Moderate and low risk vulnerabilities will be detailed in the final report of findings.

Phase I: Discovery

Verizon performs reconnaissance to gather information including registration data, operating system version and patch level, and service version and configuration.

Phase II: Vulnerability Identification

Verizon uses a combination of commercial and open-source tools to help guide our trained professionals in identifying security vulnerabilities in tested systems.

Phase III: Verification

Vulnerabilities identified will be confirmed by our security staff within the confines or the rules of engagement to minimize false positives to the greatest extent possible without performing actual exploits.

Tests

- Host Identification: Identify live hosts.
- DNS Queries: Query Name databases such ARIN to obtain domain names, IP address block assignments, and registrar information.
- Network Route Mapping: Map the network route to each system using trace route and Visual Route.
- Operating System Identification: Identify the operating system of each host through analysis of responses to specially crafted TCP/IP packets.
- Network Services Enumeration: Enumerate the services available on each system through TCP and UDP port scanning, using tools such as NMAP and SuperScan.
- Network Service Exploration: Build a detailed profile of each service through automated and manual banner grabbing and service exploration without exploiting any service vulnerabilities.
- Vulnerability Identification: Use commercial and open-source vulnerability scanners to identify known vulnerabilities on each system.

Tools

- nslookup
- dig
- nmap
- Ping/traceroute
- VisualRoute
- Fscan
- Firewalk

- DumpACL
- DumpEvt
- DumpReg
- DumpSec
- Enum
- nCircle
- nessus

The following tools may also be used by Verizon as needed to perform web application vulnerability scanning on web server systems included in the assessment. Due to the nature of application testing, alternate tools may be used (including those written by our team) to meet a specific requirement.

- AppScan
- WebSleuth
- WebProxy
- HP Software (Formally SPI Dynamcs) WebInspect

System and Platform Security Testing

Verizon identifies potential exposures in the application infrastructure through security configuration analysis and vulnerability testing. Systems in this category include operating systems, application servers, database servers, middleware servers, and network devices. The analysis is conducted within the context of the devices operational environment, validating the integration of functional components and systems.

Verizon analyzes the security configuration of each of the host operating systems. Verizon collects information using Verizon's proprietary tools and commercially available tools to gather information on both UNIX and Windows platforms. Verizon assesses the security configuration of servers and analyzes output for security vulnerabilities.

Verizon's analysis will include the following areas:

- User Authorization
- File Permissions
- Trust Relationships
- Service Configuration
- Checksum Validity Checks
- Auditing Configuration
- Patch Currency

Verizon tools will include the following:

- GFI LanGuard
- UnixRecon
- HFNetCheck

- Titan

Business Security Assessment (BSA) Description

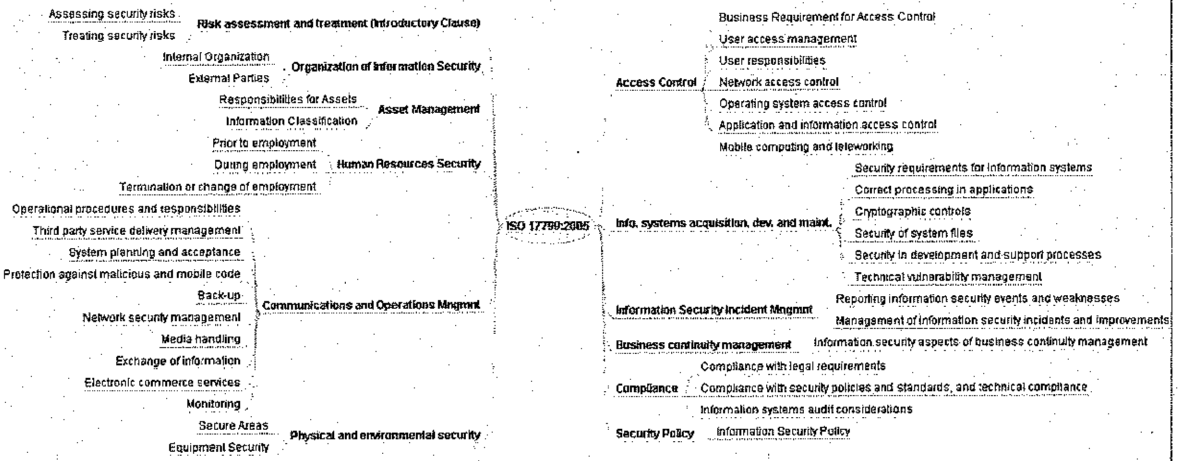
To meet the security requirements of most organizations today, Verizon respectfully commits to provide an independent, business-driven information security assessment, equally focused on people, process, and technologies that are critical to the operational structure of the environment. Verizon's Business Security Assessment (BSA) identifies information security risks in your enterprise and measures your organization's security management practices against criteria established by the international security standard ISO 17799:2005 "Information Technology – Code of Practice for Information Security Management". Gaps in an organization's information security program are identified and specific recommendations are made for areas of improvement that will reduce risk for your enterprise. Upon completion of the assessment, the resulting report provides an overview of your company's logical and physical security controls for your information technology infrastructure, and compares them to the "best practices" contained in ISO 17799:2005.

The assessment provides a comprehensive analysis of each area affected by current security issues and helps senior management determine how to allocate resources for information security risk mitigation. Verizon will develop a report of recommendations focused on providing guidance on how to best meet the best practices of the ISO standard which will have the greatest reduction in risk to the organization. This will result in a prioritized set of action items that can be used to develop a roadmap strategy for your organization.

Verizon has developed its security assessment methodology to offer a cost-effective way to measure an organization's security program within the business context. It leverages decades of experience of Verizon senior staff with assessing and developing effective information security programs. This methodology provides the following benefits for your organization:

- Provides comprehensive coverage of security issues by tracking a set of standard security criteria.
- It emphasizes relevance of the results to the organization by using an organizational model.
- It considers the organization against appropriate security best practices for its industry.
- It minimizes assessment cost by enforcing a structured methodology.

BSA is a carefully crafted methodology designed to quickly get to the heart of your business security issues. It does so with minimal disruption to the day-to-day essential processes that keeps operations running. The Verizon consultant will evaluate your existing security processes and controls using the Verizon Business Security Assessment™ methodology. Based on the ISO 17799:2005 standard, the methodology uncovers not only technical deficiencies in the design or implementation of security protections, but also the operating deficiencies associated with people and processes charged with security maintenance and management. Information will be collected through interviews with managers and staff, review of documentation, and observation of the environment. The methodology covers twelve important functional areas:



ISO 17799:2005
Risk assessment and treatment (Introductory Clause)
Assessing security risks
Treating security risks
Organization of Information Security
Internal Organization
External Parties
Asset Management
Responsibilities for Assets
Information Classification
Human Resources Security
Prior to employment
During employment
Termination or change of employment
Communications and Operations Mngmnt
Operational procedures and responsibilities
Third party service delivery management
System planning and acceptance
Protection against malicious and mobile code
Back-up
Network security management
Media handling
Exchange of information
Electronic commerce services
Monitoring
Physical and environmental security
Secure Areas
Equipment Security
Access Control
Business Requirement for Access Control
User access management
User responsibilities
Network access control
Operating system access control
Application and information access control
Mobile computing and teleworking
Info. systems acquisition, dev. and maint.
Security requirements for information systems
Correct processing in applications
Cryptographic controls
Security of system files
Security in development and support processes
Technical vulnerability management
Information Security Incident Mngmnt
Reporting information security events and weaknesses
Management of information security incidents and improvements
Business continuity management
Information security aspects of business continuity management
Compliance
Compliance with legal requirements
Compliance with security policies and standards, and technical compliance
Information systems audit considerations
Security Policy
Information Security Policy

1) **Risk Assessment and Treatment (ISO 17799:2005 introductory clause)**
    a) Develop methodology for Assessing and treating security risks.

2) **Security Policy**
    a) Provide management direction and support for information security in accordance with business requirements and relevant regulations.

3) **Organization of Information Security**
    a) Manage information security within the organization to initiate and control the implementation of information security within the organization.
    b) Maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

4) **Asset Management**
    a) Achieve and maintain appropriate protection of organizational assets.
    b) Provides an appropriate level of protection for information.

5) **Human Resources Security**

a) Assess whether employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.
b) Assess whether employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.
c) Assess whether employees, contractors and third party users exit an organization or change employment in an orderly manner.

6) Physical and environmental security

a) Prevent unauthorized physical access, damage, and interference to the organization's premises and information.
b) Prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

7) Communications and Operations Management

a) Assess the secure operation of information processing facilities.
b) Implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.
c) Minimize the risk of systems failures.
d) Protect the integrity of software and information.
e) Maintain the integrity and availability of information and information processing facilities.
f) Assess the protection of information in networks and the protection of the supporting infrastructure.
g) Prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.
h) Maintain the security of information and software exchanged within an organization and with any external entity.
i) Assess the security of electronic commerce services, and their secure use.
j) Detect unauthorized information processing activities.

8) Access Control

a) Control access to information.
b) Assess authorized user access and to prevent unauthorized access to information systems.
c) Prevent unauthorized user access, and compromise or theft of information and information processing facilities.
d) Prevent unauthorized access to networked services.
e) Prevent unauthorized access to operating systems.
f) Prevent unauthorized access to information held in application systems.
g) Assess information security when using mobile computing and teleworking facilities.

9) **Information systems acquisition, development and maintenance**
   a) Assess whether security is an integral part of information systems.
   b) Prevent errors, loss, unauthorized modification or misuse of information in applications.
   c) Protect the confidentiality, authenticity or integrity of information by cryptographic means.
   d) Evaluate the security of system files.
   e) Maintain the security of application system software and information.
   f) Reduce risks resulting from exploitation of published technical vulnerabilities.

10) **Information Security Incident Management**
   a) Assess whether information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
   b) Assess whether a consistent and effective approach is applied to the management of information security incidents.

11) **Business continuity management**
   a) Counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to allow for their timely resumption.

12) **Compliance**
   a) Avoid breaches of any statutory, regulatory or contractual obligations, and of any security requirements.
   b) Evaluate compliance of systems with organizational security policies and standards.
   c) Maximize the effectiveness of and to minimize interference to/from the information systems audit process.

The Verizon consultant will assess the security gaps and develop a set of recommendations to act upon that will bring your company up to a "best practices" state for its operational infrastructure, protective boundaries, and external factors. By recording the recommendations in a "Recommendations Repository", the Verizon consultant will be able to assign and record relative factors for cost and risk. The prioritization indicators are: Low, Medium, and High for cost, as well as Minimal, Moderate, Average, Significant, and Critical for risk.

III. Deliverables

Verizon will deliver a detailed written report of findings encountered during the course of the assessment. The report will include a description of each security-relevant finding, the system(s), the relative severity of each finding, and a suggested remediation strategy.

An Executive Summary will highlight the high-risk findings, and provide a summary of your organization's general security posture. This section focuses on providing an executive with prioritized recommendations that you can take to mitigate risks and threats, and improve the overall security posture. The report will go on to discuss the findings in detail and provide supporting evidence. The report vulnerabilities will be given a severity rating using the following severity levels:

- High Risk: Weaknesses that could result in serious system compromise or loss of data integrity. These weaknesses should be addressed as soon as possible.

- Medium Risk: Weaknesses which are important to overall security controls, data integrity, and reliability. These weaknesses should be addressed secondary to High Priority problems.

- Low Risk: Issues that will be raised as suggested improvements to enhance the security or system efficiency, but which are not necessarily vital to the security of the network.

- Information: Issues which are informational only in nature and present insignificant implication in terms of overall security risk. However, consideration of these points is important in light of the impacts of the assessment.

- Resolved: In a follow-up review of previous findings, we will consider an issue resolved when we find that adequate measures have been implemented to address the risk.

For each of the identified vulnerabilities classified as shown above, Verizon will provide you with remediation recommendations aimed at reducing or removing the risks associated with findings, enumerated during the assessment. Verizon will prioritize these recommendations based on the threat level and required "time to implement". Short-term recommendations will be steps that can be implemented quickly to improve an organizations overall security posture. Recommendations for risks that are deemed less severe, or that require more time to implement, will be documented as an integrated mitigation strategy comprised of longer-term goals.

Finally, at the conclusion of this project Verizon will meet with you to discuss the findings contained in the documentation provided. Significant findings and recommendations produced during the assessment will be formally presented and discussed with relevant team members, either during a conference call or a face-to-face meeting.

IV. Engagement Management

A. Approach

The overall Verizon management and delivery approach consists of the following steps:

1. Plan

A kickoff meeting will be held with the following agenda:

- ***Introduction:*** Introduction of Verizon engagement team and identify client project coordinator.

- ***Requirements, goals, and scope:*** clear definition of the requirement for the assessment, the goals of the assessment, and the scope

- ***Methods used:*** interviews, observation, testing, walk-through, documentation review, etc.

- ***Resources needed:*** documentation (e.g., prior work papers, policies, standards, etc.), people (e.g., system manager, system administrator, etc.), physical access, LAN access, system access, training, etc.

- ***Schedule:*** person-hours spent on overall tasks

The goals of these activities include minimizing the impact to production roll-out schedules, ensuring goals are understood, precisely defining the scope, and ensuring the availability of resources.

Verizon will designate an engagement manager who will act as the central point of contact for your organization throughout the entire engagement. The engagement manager is responsible for ensuring that the project meets our high standards for quality, schedule and budget. The engagement manager is also responsible for managing the change control process. Should your project requirements change during the course of the engagement, the engagement manager will review project modifications for impact on scope, budget and schedule, and document the agreed upon changes to make sure that your objectives are met. Verizon will also work with your designated personnel to develop a project plan that specifies resources, dates, times, and locations for the tasks described below. Verizon will obtain a final approval of the project plan from your organization prior to proceeding with project activities.

2. Updates and Status Reports

Verizon's overall engagement manager will coordinate with the project management team to review test plans and schedules and the need for revisions, updates, or other changes that may need to be communicated on an ongoing basis. The Verizon team will provide a weekly status report via e-mail to your designated project and technical contacts. This brief report will list the completed tasks from the previous week and the open tasks for the current week. The purpose of these reports is to provide weekly information on the status of the project along with any outstanding issues.

3. Analysis and Initial Findings Report

Verizon will analyze the data collected during the tasks and generate recommendations to mitigate vulnerabilities discovered. The recommendations will be relevant and specific to each of the environments reviewed. You will have the opportunity to provide feedback for updates to the initial report.

4. Internal Verizon Review

These activities provide quality control for the project's deliverables. Verizon employs a technical peer review process to review the accuracy and completeness of the findings. Management review evaluates findings for the proper business context.

5. Final Report/Deliverables Submission and Project Close-Out

These activities complete the assessment process. Verizon will use feedback from your designated personnel to finalize the report. Verizon will issue the final report to your company once the approved changes are made. The overall goals are to maximize knowledge transfer and for deliverables to meet their stated goals.

B. Project Team

Verizon will dedicate a highly qualified management team to oversee delivery of this engagement. The management team will coordinate the initiative so it proceeds in a collaborative fashion, producing a streamlined and consistent methodology, and approach for analyzing current security risks and identifying opportunities for business improvements.

V. Engagement Scope

External Vulnerability Assessment

- An External Vulnerability Assessment of up to Internet accessible IP addresses controlled by the customer. Includes port scanning of up to four (4) class C IP address ranges to identify the fifty (50) targets that will be included in the vulnerability assessment.

- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.

- All work will be performed remotely from Verizon facilities.

Internal Vulnerability Assessment – Thousand Oaks, CA

- An Internal Vulnerability Assessment for a sample set of up to sixteen (16) devices in the operational environment supporting the following four (4) EMS services at a customer facility in Thousand Oaks, CA. Included with each service is the number of devices that will be included in the assessment:
    - REDACTED

- Includes up to business days of onsite work at a customer facility in Thousand Oaks, CA. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy REDACTED, and applicable REDACTED .X configuration guidelines.

- The report will contain a section listing the results for each service.

- For all Vulnerability Assessment and System and Platform Testing tasks, the term "device" can refer to a server, network device, or workstation.

System and Platform Security Testing – Thousand Oaks, CA

- System and Platform Security Testing for a sample set of up to sixteen (16) devices in the operational environment supporting the following four (4) EMS

services at a customer facility in Thousand Oaks, CA. Included with each service is the number of devices that will be included in the assessment:
REDACTED

- Includes up to REDACTED business days of onsite work at a customer facility in Thousand Oaks, CA. Additional data analysis and report creation will be performed remotely from Verizon facilities.
- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.
- The report will contain a sect ion listing the results for each service.

Internal Vulnerability Assessment – Tampa, FL

- An Internal Vulnerability Assessment for a sample set of up to six (6) devices in the operational environment supporting the following one (1) EMS service at a customer facility in Tampa, FL. Included with each service is the number of devices that will be included in the assessment:
- REDACTED
- Includes up to REDACTED business day of onsite work at a customer facility in Tampa, FL. Additional data analysis and report creation will be performed remotely from Verizon facilities.
- Systems will be evaluated for compliance with security policy redacted, and applicable .X configuration guidelines.
- The report will contain a section listing the results for each service.

System and Platform Security Testing – Tampa, FL

- System and Platform Security Testing for a sample set of up to four (4) devices in the operational environment supporting the following one (1) EMS service at a customer facility in Tampa, FL. Included with each service is the number of devices that will be included in the assessment:

- Includes up to REDACTED business day of onsite work at a customer facility in Tampa, FL. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.

- The report will contain a section listing the results for each service.

Internal Vulnerability Assessment – Baltimore, MD, Area Locations

- An Internal Vulnerability Assessment for a sample set of up to ninety three (93) devices in the operational environment supporting the following sixteen (16) EMS services at facilities located at up to four (4) customer facilities in the Baltimore, MD metropolitan area. Included with each service is the number of devices that will be included in the assessment:
  - REDACTED
  -

- Includes up to REDACTED business days of onsite work at four (4) customer facilities located in the Baltimore, MD, metropolitan area. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.

- The report will contain a section listing the results for each service.

System and Platform Security Testing – Baltimore, MD, Area Locations

- System and Platform Security Testing for up to fifty five (55) devices in the operational environment supporting the following sixteen (16) EMS services at facilities located at up to four (4) customer facilities in the Baltimore, MD metropolitan area. Included with each service is the number of devices that will be included in the assessment:

- REDACTED

- Includes up to REDACTED business days of onsite work at four (4) customer facilities located in the Baltimore, MD, metropolitan area. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.

- The report will contain a section listing the results for each service.

Internal Vulnerability Assessment – Silver Spring, MD

- An Internal Vulnerability Assessment for a sample set of up to eight (8) devices in the operational environment supporting the following two (2) EMS services at one (1) customer facility in Silver Spring, MD. Included with each service is the number of devices that will be included in the assessment:
  - Redacted
  - Redacted

- Includes up to REDACTED business day of onsite work at one (1) customer facility located in Silver Spring, MD. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable configuration guidelines.

- The report will contain a section listing the results for each service.

System and Platform Security Testing – Silver Spring, MD

- System and Platform Security Testing for up to eight (8) devices in the operational environment supporting the following two (2) EMS services at one (1) customer facility in Silver Spring, MD. Included with each service is the number of devices that will be included in the assessment:
  - Redacted
  - Redacted

- Includes up to REDACTED business day of onsite work at one (1) customer facility located in Silver Spring, MD. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable configuration guidelines.

- The report will contain a section listing the results for each service.

Internal Vulnerability Assessment – Newark, NJ

- An Internal Vulnerability Assessment for a sample set of up to eight (8) devices in the operational environment supporting the following two (2) EMS services at one (1) customer facility in Newark, NJ. Included with each service is the number of devices that will be included in the assessment:
  - redacted
  - redacted

- Includes up to business day of onsite work at one (1) customer facility located in Newark, NJ. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.

- The report will contain a section listing the results for each service.

System and Platform Security Testing – Newark, NJ

- System and Platform Security Testing for up to eight (8) devices in the operational environment supporting the following two (2) EMS services at one (1) customer facility in Newark, NJ. Included with each service is the number of devices that will be included in the assessment:
  - redacted
  - redacted

- Includes up to , business day of onsite work at one (1) customer facility located in Newark, NJ. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.

- The report will contain a section listing the results for each service.

Internal Vulnerability Assessment – Blue Hill, NY

- An Internal Vulnerability Assessment for a sample set of up to fourteen (14) devices in the operational environment supporting the following one(1) EMS services at one (1) customer facility in Blue Hill, NY. Included with each service is the number of devices that will be included in the assessment:
  - redacted

REDACTED

- Includes up to business days of onsite work at one (1) customer facility located in Blue Hill, NY. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.

- The report will contain a section listing the results for each service.

System and Platform Security Testing – Blue Hill, NY

- System and Platform Security Testing for a sample set of up to six (6) devices in the operational environment supporting the following one(1) EMS services at one (1) customer facility in Blue Hill, NY. Included with each service is the number of devices that will be included in the assessment:
    - redacted

- Includes up to REDACTED business day of onsite work at one (1) customer facility located in Blue Hill, NY. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.

- The report will contain a section listing the results for each service.

Internal Vulnerability Assessment – Coppell, TX, Area Locations

- An Internal Vulnerability Assessment for a sample set of up to fifty four (54) devices in the operational environment supporting the following thirteen (13) EMS services at one (1) customer facility located in Coppell, TX. Included with each service is the number of devices that will be included in the assessment:

- REDACTED

- Includes up to business days of onsite work at one (1) customer facility located in Coppell, TX. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.

- The report will contain a section listing the results for each service.

REDACTED

System and Platform Security Testing – Coppell, TX, Area Locations

- System and Platform Security Testing for a sample set of up to forty (40) devices in the operational environment supporting the following thirteen (13) EMS services at facilities located at one (1) customer facility in Coppell, TX.. Included with each service is the number of devices that will be included in the assessment:

- REDACTED

- Includes up to business days of onsite work at one (1) customer facility located in Coppell, TX. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.

- The report will contain a section listing the results for each service.

Internal Vulnerability Assessment – Arlington, VA

- An Internal Vulnerability Assessment for a sample set of up to four (4) devices in the operational environment supporting the following one (1) EMS service at one (1) customer facility located in Arlington, VA. Included with each service is the number of devices that will be included in the assessment:

- Redacted

- Includes up to business day of onsite work at one (1) customer facility located in Arlington, VA. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.

- The report will contain a section listing the results for each service.

System and Platform Security Testing – Arlington, VA

- System and Platform Security Testing for a sample set of up to four (4) devices in the operational environment supporting the following one (1) EMS service at one (1) customer facility located in Arlington, VA. Included with each service is the number of devices that will be included in the assessment:

- Redacted

REDACTED

- Includes up to business day of onsite work at one (1) customer facility located in Arlington, VA. Additional data analysis and report creation will be performed remotely from Verizon facilities.
- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.
- The report will contain a section listing the results for each service..

Internal Vulnerability Assessment – Reston, VA, Area Locations

- An Internal Vulnerability Assessment for a sample set of up to twenty two (22) devices in the operational environment supporting the following four (4) EMS services at one (1) customer facility located in Reston, VA. Included with each service is the number of devices that will be included in the assessment:
    - REDACTED
- Includes up to business days of onsite work at one (1) customer facility located in Reston, VA. Additional data analysis and report creation will be performed remotely from Verizon facilities.
- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.
- The report will contain a section listing the results for each service.

System and Platform Security Testing – Reston, VA, Area Locations

- System and Platform Security Testing for a sample set of up to twelve (12) devices in the operational environment supporting the following four (4) EMS services at one (1) customer facility located in Reston, VA. Included with each service is the number of devices that will be included in the assessment:
- REDACTED
- Includes up to business days of onsite work at one (1) customer facility located in Reston, VA.
- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.
- The report will contain a section listing the results for each service.

Security Assessment – Central Office, Annapolis, MD

- A Security Assessment to include a Network Vulnerability Assessment and System and Platform Security Testing for a number of devices that will be determined based on an analysis of the site's IT resources and configuration.

- Includes up to REDACTED days of onsite work at one (1) customer facility located in Annapolis, MD. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy REDACTED, and applicable REDACTED.X configuration guidelines.

Security Assessment – Central Office, Lewinsville, MD

- A Security Assessment to include a Network Vulnerability Assessment and System and Platform Security Testing for a number of devices that will be determined based on an analysis of the site's IT resources and configuration.

- Includes up to days of onsite work at one (1) customer facility located in Lewinsville, MD. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.

Security Assessment – Central Office, Keller, TX

- A Security Assessment to include a Network Vulnerability Assessment and System and Platform Security Testing for a number of devices that will be determined based on an analysis of the site's IT resources and configuration.

- Includes up to days of onsite work at one (1) customer facility located in Keller, TX. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.

Security Assessment – Central Office, Baltimore, MD (Charles Street)

- A Security Assessment to include a Network Vulnerability Assessment and System and Platform Security Testing for a number of devices that will be determined based on an analysis of the site's IT resources and configuration.

- Includes up to days of onsite work at one (1) customer facility located in Baltimore, MD. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable . X configuration guidelines.

Security Assessment – Central Office, Thousand Oaks, CA

- A Security Assessment to include a Network Vulnerability Assessment and System and Platform Security Testing for a number of devices that will be determined based on an analysis of the site's IT resources and configuration.

- Includes up to days of onsite work at one (1) customer facility located in Thousand Oaks, CA. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable .X configuration guidelines.

Security Assessment – Client Facility, Madison, NJ (FSC)

- A Security Assessment to include a Network Vulnerability Assessment and System and Platform Security Testing for a number of devices that will be determined based on an analysis of the site's IT resources and configuration.

- Includes up to days of onsite work at one (1) customer facility located in Madison, NJ. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable . X configuration guidelines.

Security Assessment – Client Facility, Silver Spring, MD (MCO/OCO)

REDACTED

- A Security Assessment to include a Network Vulnerability Assessment and System and Platform Security Testing for a number of devices that will be determined based on an analysis of the site's IT resources and configuration.

- Includes up to days of onsite work at one (1) customer facility located in Silver Spring, MD. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy and applicable . X configuration guidelines.

Security Assessment – Client Facility, Reston, VA (NNMC)

- A Security Assessment to include a Network Vulnerability Assessment and System and Platform Security Testing for a number of devices that will be determined based on an analysis of the site's IT resources and configuration.

- Includes up to days of onsite work at one (1) customer facility located in Reston, VA. Additional data analysis and report creation will be performed remotely from Verizon facilities.

- Systems will be evaluated for compliance with security policy , and applicable . X configuration guidelines.

Business Security Assessment – Various U.S. Based Locations

- A Business Security Assessment to evaluate customer's compliance with ISO 17799:2005 "Information Technology – Code of Practice for Information Security Management", and security policy redacted.

- Includes up to business weeks of Verizon consulting time to perform work for the Business Security Assessment.

- Includes up to business weeks of onsite work, and up to week of additional data analysis and report creation performed remotely from Verizon facilities.

Pricing

Pricing Table	Cost
External Vulnerability Assessment	redacted
Internal Vulnerability Assessment –	redacted

Thousand Oaks, CA	
System and Platform Security Testing – Thousand Oaks, CA	redacted
Internal Vulnerability Assessment – Tampa, FL	redacted
System and Platform Security Testing – Tampa, FL	redacted
Internal Vulnerability Assessment – Baltimore, MD	redacted
System and Platform Security Testing – Baltimore, MD	redacted
Internal Vulnerability Assessment – Silver Spring, MD	redacted
System and Platform Security Testing – Silver Spring, MD	redacted
Internal Vulnerability Assessment – Newark, NJ	redacted
System and Platform Security Testing – Newark, NJ	redacted
Internal Vulnerability Assessment – Blue Hill, NY	redacted
System and Platform Security Testing – Blue Hill, NY	redacted
Internal Vulnerability Assessment – Coppell, TX	redacted
System and Platform Security Testing – Coppell, TX	redacted
Internal Vulnerability Assessment – Arlington, VA	redacted
System and Platform Security Testing – Arlington, VA	redacted
Internal Vulnerability Assessment – Reston, VA	redacted
System and Platform Security Testing – Reston, VA	redacted
Security Assessment – Central Office, Annapolis, MD	redacted
Security Assessment – Central Office, Lewinsville, MD	redacted
Security Assessment – Central Office, Keller, TX	redacted
Security Assessment – Central Office, Baltimore, MD (Charles Street)	redacted
Security Assessment – Central Office, Thousand Oaks, CA	redacted
Security Assessment – Client Facility, Madison, NJ (FSC)	redacted
Security Assessment – Client Facility, Silver Spring, MD (MCO/OCO)	redacted
Security Assessment – Client Facility, Reston, VA (NMMC)	redacted
Business Security Assessment	redacted

REDACTED

Total	redacted

The above quoted price is valid for a period of thirty (30) days from the date of issue. This is a fixed price engagement. The Professional Service fees quoted herein reflect the project as anticipated at the time and during the period of execution.

Travel and Expenses

Subject to compliance with Customer's normal and customary policies regarding substantiation and verification of business expenses, Verizon is authorized to incur, on your behalf, customary and reasonable travel, lodging and other expenses in connection with this assessment. Customer will reimburse Verizon for said expenses. Total travel expenses for this project will not exceed redacted.

REDACTED