



elert & associates
technology consultants

ORIGINAL

140 third street south, stillwater, mn 55082
phone . 651.430.2772, fax . 651.430.2661 www.elert.com

January 19, 2015

Mr. Guy L. Nisbet
Department of Administration, Purchasing Division
State of West Virginia
2019 Washington Street East
Charleston, WV 25305-0130

Dear Mr. Nisbet:

Elert & Associates Networking Division, Inc. (Elert & Associates (E&A)) is pleased to have the opportunity to respond to the State of West Virginia's Request for Quotation CRFQ 0203 CPR1500000001.

Elert & Associates is a security and technology consulting firm. E&A was established in March of 1984. Our firm employs over 40 staff members, operates out of multiple offices, and has served hundreds of government entities throughout the United States.

From risk, vulnerability, and threat assessments to reviewing policies, procedures, people, building modifications, and equipment, to design, bid, and implementation, E&A works with you to develop and implement a comprehensive security program and supporting systems.

E&A's Security Consulting Division consists of past law enforcement personnel, policy specialists, and ASIS members, including the Physical Security Professional (PSP) certification. Gary Elert founded the firm in 1984 and holds the PSP certification.

E&A fully complies and understands scope of work as outlined in RFP and will meet and/or exceed expectations of project based on phased approach. E&A acknowledges all addenda as part of RFP. E&A also acknowledges Exhibit A and Exhibits B-E.

We have enclosed six hard copies and six electronic copies on CD, as requested. We look forward to working with you and your staff on this project, and will be in contact with you in the near future. If we can be of any assistance in the interim, please feel free to contact Rick Anderson at (651) 705-1249 or rick.anderson@elert.com.

Sincerely,

Tom Pavek, Senior Vice President
Elert & Associates

01/21/15 09:39:41
WV Purchasing Division

State of West Virginia

Team Elert Proposal

Information Security and Network Vulnerability Assessment

Bid Number CRFQ 0203 CPR1500000001

January 19, 2015

Prepared by:

Rick Anderson
Gary Elert, PSP
Gus Fritschie, CTO / SeNet



Elert & Associates Networking Division, Inc.
140 Third Street South
Stillwater, MN 55082
(651) 430-2772
www.elert.com

Contact Person:

Rick Anderson, Technology Consultant
Phone: (651) 705-1249
Fax: (651) 430-2661
Email: rick.anderson@elert.com

Table of Contents

	Page
SECTION 1: TEAM ELERT TECHNICAL OVERVIEW	1
SECTION 2: REQUEST FOR QUOTATION / SPECIFICATIONS	34
SECTION 3: ATTACHMENT 1 – VENDOR REFERENCES	45
SECTION 4: ATTACHMENT 2 – VENDOR PRIMARY STAFF REFERENCES	49
SECTION 5: ATTACHMENT 3 – ATTESTATION AND CONFIRMATIONS	69
SECTION 6: ATTACHMENT 4 – CONFIDENTIALITY AND NON-DISCLOSURE STATEMENT.....	72
SECTION 7: EXHIBIT A - PRICING PAGE & RFQ SIGNED DOCUMENTS.....	74
SECTION 8: VENDOR PREFERENCE CERTIFICATE	80
SECTION 9: PURCHASING AFFIDAVIT	82
SECTION 10: ADDENDUM ACKNOWLEDGEMENT FORM & SIGNATURE PAGES	84
SECTION 11: CERTIFICATION AND SIGNATURE PAGE	91

SECTION 1: Team Elert Technical Overview

Team Elert

Elert & Associates

Elert & Associates (E&A) was established in March of 1984 and has been in business for the past 30 years. Today, Elert & Associates employs over 40 technology and consulting staff, operates out of multiple offices, and has served hundreds of clients throughout the United States.

Elert & Associates' authorized representative is:

Name: Gary Elert, PSP
Title: President
Company Name: Elert & Associates Networking Division, Inc. (Elert & Associates (E&A))
Company Address: 140 Third Street South, Stillwater, MN 55082
Phone: (651) 705-1222 (Direct); (651) 430-2772 (Main)
Email: gary.elert@elert.com

SeNet International Corporation

SeNet is an innovative leader in IT services, specializing in networking and information systems security consulting for Federal agencies and commercial entities. SeNet focuses on helping clients meet their network infrastructure and information security goals by establishing close working relationships and by mapping clients' goals and mission requirements to proven solutions. At all times, SeNet maintains an awareness of clients' established policies and procedures and ensures that all of our work efforts are compliant with government regulations and corporate industry best practices.

SeNet is an SBA-certified small business. Headquartered in Fairfax, Virginia, SeNet has been in business since 1998 assisting over 150 public- and private-sector clients in improving their information security. The services we provide include vulnerability assessments and penetration testing, security program development and planning, security architecture design and implementation, security operations, and compliance verification, among others. SeNet's executives are IT industry veterans who possess both subject matter technical expertise as well as extensive experience in managing large-scale projects. The company is managed by its co-founders, Ilan Katz and Anatoly Kozushin.

Both executives maintain a hands-on approach, emphasizing attention to detail in providing client solutions. Mr. Katz and Mr. Kozushin have been very involved with the hundreds of tasks SeNet has successfully performed and completed over the years.

The founders' practical and straightforward approach has enabled SeNet to successfully combine best business practices with innovative ideas, making full use of the inherently simplified decision making processes of a small company. This innovation has had a positive effect on SeNet's processes, adopted technologies, and relationships with both clients and partners.

SeNet forms strong partnerships with its clients to ensure an effective management structure for these complex tasks. Our services empower customers to effectively achieve their organizational goals by focusing on their primary business.

Information security covers a wide range of topics and issues. SeNet has gained substantial experience and expertise over the years, ranging from simple system security reviews to ground-up information security system deployments. We offer this experience and expertise through a range of services that are specifically tailored to our clients' individual needs and are backed by our continuing commitment to excellence. The spectrum of these services is illustrated in the following table.

Table 1: Team Elert Services

Team Elert Service Offerings	
Compliance Verification & Validation	Business Continuity/Disaster Recovery Planning
Risk Assessment	Firewall/VPN/IDS Integration
Penetration Testing	Application Code Level Review
Network Architecture	Program/Project Management
Network Analysis	Subject Matter Expert Assistance
Performance Monitoring	Network Monitoring/NOC
Security Monitoring/SOC	Policies & Procedures Development
Vulnerability Analysis	Security Product Tune-Up
Security Program Planning	Remote Monitoring/Administrating
System Security Planning	User Awareness Training
Security Administrator Training	

Our product and technology expertise includes:

Table 2: Team Elert Technology Expertise

Team Elert Technology Expertise	
NETWORK PROTECTION Firewalls VPN Appliances/Gateways Intrusion Detection Systems (IDS) Content Filters/URL Blockers Antivirus Protectors	AUTHENTICATION Smart Cards Biometric Devices Directory Services/LDAP Single Sign-On (SSO)
REMOTE ACCESS Terminal Servers Remote Control Encrypted Tunnels	PKI/ENCRYPTION IPSec Digital Certificate Certificate Authority (CA) Digital Signature
CERTIFICATION AND ACCREDITATION FISMA NIST DIACAP	

Certifications & Professional Affiliations

◆ AICP	American Institute of Certified Planners
◆ APCO	Association of Public-Safety Communications Officials
◆ ASIS	American Society for Industrial Security
◆ BICSI	Building Industry Construction Services International
◆ CBCP	Certified Business Continuity Planner
◆ CCNA	Cisco Certified Network Associate, Routing and Switching Certification
◆ CDT	Construction Documents Technologist
◆ CHS-III	Certified Homeland Security Professional
◆ CPO	Crime Prevention Officer
◆ CPTED	Crime Prevention Through Environmental Design Certification
◆ CSS	Certified Security Supervisor
◆ CTS	Certified Technology Specialist
◆ CTS-D	Certified Technology Specialist – Design
◆ Ed.M.	Master of Education
◆ EE	Electrical Engineer
◆ FCC	General Class Radiotelephone License
◆ ICIA	International Communications Industries Association, Inc.
◆ IEEE	Institute of Electrical & Electronic Engineers
◆ LEED AP	Leadership in Energy and Environmental Design, Accredited Professional
◆ LEED GA	Leadership in Energy and Environmental Design, Green Associate
◆ MCTS	Microsoft Certified Technology Specialist: Windows® 7, Configuration
◆ MTA	Minnesota Telecommunications Association
◆ 911 ENP	Emergency Number Professional
◆ PE	Professional Engineer (<i>selected states</i>)
◆ PMP	Project Management Professional
◆ PSP	Physical Security Professional
◆ RCDD	Registered Communications Distribution Designer (<i>Certified in all major structured cabling systems</i>)
◆ RTBAV	Certified Instructor in “Refuse To Be A Victim” Training Program
◆ SCTE	Society of Cable Telecommunications Engineers Membership
◆ STC	Society of Telecommunications Consultants Membership
◆ USGBC	U.S. Green Building Council Membership

Mandatory Contract Services Requirements and Deliverables

1.1 Key Personnel Qualifications

“4.1.1 Primary persons responsible for the engagement must have a minimum of 5 years of experience in security design and testing of Microsoft .Net, Microsoft SQL Server, and Cisco Systems Networking. As part of the solicitation response, please provide copies of professional certifications which support this requirement and provide the pertinent reference information on Attachment 2.”

An extensive security assessment project such as WVCPRB’s calls for technical and analytical expertise covering networking technologies, directory services, Windows security, servers, and desktops. The following section provides a detailed organizational chart and synopses of team members’ expertise.

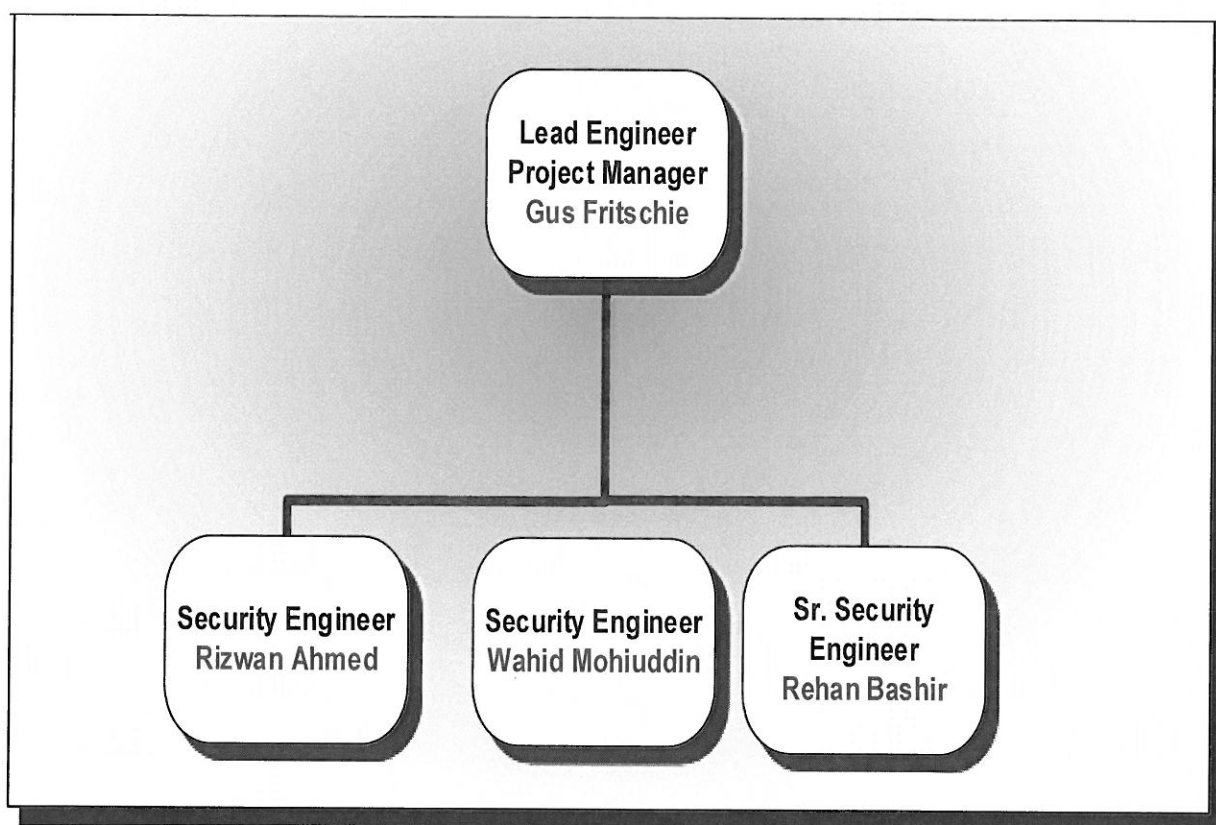


Figure 1: Team Elert Assessment Team

Short synopses of our proposed team members’ backgrounds are provided below. Further details and complete resumes are enclosed as requested.

- **Mr. Gus Fritschie, CISSP** will be the Project Manager and Lead Engineer. Prior to Team Elert, Mr. Fritschie was a member of the information security consulting practices at KPMG and Deloitte & Touché. He led and performed numerous vulnerability assessments and penetration tests in support of financial audits and other compliance-related efforts. Clients included Fortune 500 companies, civilian agencies, and the Department of Defense (DOD).

Mr. Fritschie joined Team Elert as a Senior Security Engineer over ten years ago and was promoted to the level of Director, Security Assessments and Engineering. Mr. Fritschie has led several large-scale projects. Some projects included enterprise-wide vulnerability assessments for multiple government and commercial clients, management of Certification and Accreditation (C&A) efforts, and Web application penetration tests. As Team Elert's Director of Engineering and Security Assessments, he is responsible for all technical deliverables and projects for the company.

Mr. Fritschie has proven work performance with organizations and clients such as the Department of Health and Human Services (HHS), Department of Agriculture (USDA), Department of Labor (DOL), Department of the Interior (DOI), Government Printing Office (GPO), and Amtrak. He was the project lead for the Minerals Management Service (MMS) vulnerability assessments that were conducted by Team Elert in 2006. Mr. Fritschie retains strong technical skills in all areas of security test and evaluation (ST&E) and vulnerability testing, leading his staff in evaluating new commercial and public domain testing tools and other security products.

Mr. Fritschie has spoken at a number of security conferences such as DefCon 2011, HackerCon 2011, DerbyCon 2012, and RVASEC 2013. He has also presented at numerous government agencies on a wide variety of information security topics.

- **Mr. Rehan Bashir, CISSP, Sr. Security Engineer** – Mr. Bashir has been with Team Elert for the past seven years. He performs vulnerability testing for government and commercial agencies. These assessments involve wireless, network, and mainframe vulnerability and penetration testing. He deploys open source and proprietary software and tools to perform the penetration testing for multiple environments including but not limited to Windows, UNIX, Linux, mainframe, database, and Web application architectures. He assists in the C&A testing.
- **Mr. Rizwan Ahmed, CEH, Security Engineer** – Mr. Ahmed is seasoned in performing security operations and forensics. He has also run vulnerability scanning and management programs for large organizations.
- **Mr. Wahid Mohiuddin, MCSE, Security Engineer** – Mr. Mohiuddin provides support to Team Elert's ST&E and Vulnerability Assessments teams. He is an Active Directory subject matter expert and has performed previous assessments on AD. He is a self-motivated achiever, innovative thinker, and effective problem solver with a strong work ethic. He is proficient in all of the major vulnerability testing tools, including Nessus, Nmap, and Metasploit.

All of the proposed team members are full time employees of Team Elert and are available immediately to begin performance against this task. Their resumes and professional certifications are included as part of this proposal.

1.2 Information Security and Network Vulnerability Assessment

“Perform the Information Security and Network Vulnerability Assessment in accordance with the National Institute of Standards and Technology Standards referenced in Section 3.3.”

Our technical approach to conducting the WV Consolidated Public Retirement Board (WVCPRB) Information Security and Network Vulnerability Assessment is based on over 15 years of successfully conducting enterprise-wide security assessments of large scale Federal Government organizations, State & Local agencies and private industry firms. Team Elert’s primary focus and line of business is Information Technology (IT) Security and has been so since our inception in 1998.

Our assessment methodology adheres to NIST Special Publication 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* and is augmented by other IT Security frameworks and guidelines such as IRS Publication 1075, Federal Information Security Management Act (FISMA) and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Knowledge transfer is one of our main objectives in our assessment efforts and we will work closely with State and agency officials not only to explain our findings but also to propose the most practical and economical mitigation solutions.

Our effort will be led by an experienced Program Manager, Mr. Gus Fritschie, SeNet’s Chief Technology Officer and a published IT Security expert with over 10 years of IT Security Vulnerability Assessments and Penetration Testing. He will be assisted by our team of security engineers and analysts that all have relevant industry certifications including CISSP, CAP, and CEH.

We are confident that our past experience, as evidenced by our past performance with large organizations such as the US Department of Agriculture, the US Department of Health and Human Services (HHS), and the US Department of the Interior (DOI), combined with the skills and expertise of our staff, will ensure the success of this effort.

1.2.1 Security Policies and Procedures

“4.1.2.1 Evaluation of the security policy and procedures”

Team Elert will conduct a thorough review of WVCPRB’s existing IT Security Policies and Procedures. We will request to obtain the current versions and perform a gap analysis against the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-Series, mainly NIST SP 800-37 and NIST SP-53. The NIST guidelines identify 17 security control “families.” Each family contains security controls (or requirements) covering a particular information assurance area/domain. The first control listed will be typically a requirement for a written policy for this area. For example, the Access Control (AC) area requirements states: “The organization Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: (1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;” The second part calls for written procedures to support the policy: “(2) Procedures to facilitate the implementation of the access control policy and associated access controls.”

Similarly, the other control families follow the same pattern, covering the key controls required for that security domain.

We will begin our review by collecting and logging all current security policies and procedures into a database. Then we will evaluate each policy against the NIST control requirements. Any gap or discrepancy will be noted and recorded in our database. We will also note the date of publication and last revision of each policy as NIST guidelines call for periodic reviews and updates of all security policies.

The other part of the security policies and procedures evaluation will be to actually assess how these policies and procedures are implemented and followed throughout the organization. This will be accomplished through a combination of interviews with key WVCPRB IT stakeholders and examinations of security controls in place, incident response reports, and audit logs, etc. Team Elert has developed a tool that organizes NIST SP 800-53 controls by testing method. This reduces the time needed to conduct necessary observations and interviews, and allows us to minimize the time needed to interact with busy WVCPRB IT Officials.

Our report section for the Security Policies and Procedures evaluation will identify for each policy how it stands against the NIST guidelines and how well it is implemented per our observations and interviews.

1.2.2 External Vulnerability Scans

"4.1.2.2 A scan of external entry points into the network"

Team Elert has developed and follows an established multi-step methodology when performing network penetration testing and vulnerability assessments. It should be noted that actual penetration testing, i.e., the attempt to exploit vulnerabilities follows a vulnerability assessment or identification phase. Limited vulnerability assessment techniques need to be used order to identify potential vulnerabilities to exploit, but the focus of this effort will be on exploitation. The exact process differs slightly based on whether the testing is being performed from an internal or external perspective. The figure below illustrates Team Elert's overall methodology.

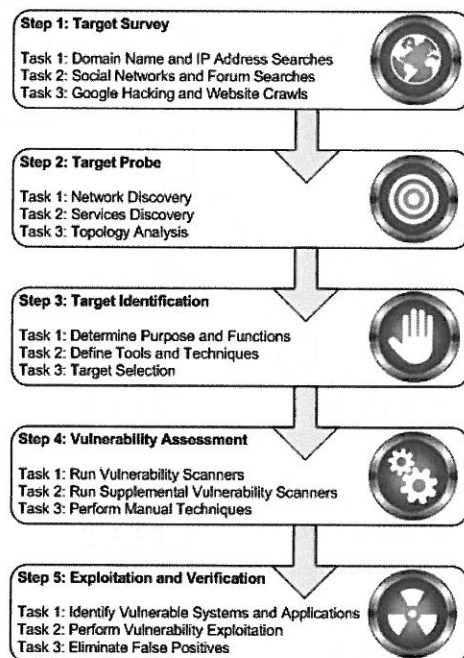


Figure 2: Team Elert's Testing Methodology

Step 1 – Target Survey

During this initial phase, Team Elert engineers will use search engines, domain name and IP registrars, social networking and forum Web sites, custom Web manipulation scripts, and automated and manual Web site analyzing tools to harvest as much information about the WVCPRB's infrastructures as possible. This methodology is divided into three tasks:

Task 1 – Domain Name and IP Address Searches

When purchasing a domain name for an organization, there is the option to have a private registration for an additional fee. Many organizations feel this is unnecessary and opt out of this benefit. This allows attackers to gather contact information including addresses, phone numbers, etc., which could be used for spam, or more often social engineering.

If your organization is moderate to large, most likely you have purchased a large range of publicly routable IP addresses for your Internet-facing systems and applications. There are a few sites that house this information. The Team Elert team will review various domestic and international Internet registries in search for sensitive information such as:

- Registered domain names;
- Configured domain name servers (DNS);
- Registered IP addresses; and
- Contact and ownership information.

For private networks, internal IP addresses and domain name servers will be investigated.

Task 2 – Social Networks and Forum Searches

Social networks and Web forums are everywhere these days. Oftentimes, it has been discovered that users are posting information on these Web sites that contain sensitive information that could give an attacker insight into the organization for which the user works either inadvertently or maliciously. These types of sites will be searched thoroughly for information that may have been leaked to them such as:

- Network schemas and locations;
- Connectivity and access points;
- Application and database schemas;
- Host name and internal IP disclosures;
- Internal-only and sensitive documents;
- Infrastructure diagrams;
- Employee names, titles, phone numbers, and e-mail addresses; and
- Inventories.

Task 3 – Google Hacking and Web Site Crawls

One of the latest methods that an attacker can use to find information about a particular Web site or organization is through the use of specially-crafted Google searches or "Google Dorks." This type of reconnaissance, also known as "Google Hacking" can quickly assist in identifying file types such as Microsoft Word, Excel, PowerPoint, and Visio that are either directly available or stored in Google's caches.

Many times, an administrator or user may put information such as network diagrams or financial information in a directory of a publicly-available site temporarily, thinking it is just there until the appropriate person downloads it without realizing that Web crawlers for search engines may have cached the document. There are Web sites dedicated to Google Hacking that include thousands of documents, password files, and configuration files discovered using this technique.

Before Google Hacking was invented, Web sites were crawled using automated and manual Web analyzers such as Paros. These tools scanned Web sites looking through the site's code for sensitive information or directories, links, and other information. They also have the ability to scan common directories like temp, admin, and images, looking further for information that could assist an attacker in breaching the infrastructure.

Step 2 – Target Probe

Exploration tests will follow to validate and augment the base profile established in “Step 1 – Target Survey” with technical network layout information. More specifically, our team will perform the following tasks:

Task 1 – Network Discovery

Commercial, freeware, open-source, and custom tools will be run against the external and/or internal networks to determine the existence, location, type, and network path of network connected systems and devices. Information gathered during this phase may include:

- System, device, and network discovery using protocols such as:
 - Internet Control Message Protocol (ICMP)
 - Transmission Control Protocol (TCP)
 - User Datagram Protocol (UDP)
 - Stream Control Transmission Protocol (SCTP)
 - Address Resolution Protocol (ARP)
 - Border Gateway Protocol (BGP)
- SNMP, CDP, BOOTP scans for network managed devices
- Querying authoritative primary and slave DNS servers for hosts
- DNS records using zone transfers (AXFR)
- Examining e-mail headers, bounced mails, and read receipts for server trails
- Reviewing Web site non-generic error messages for server trails.

Task 2 – Services Discovery

Port scanning is the practice of identifying operating systems (OSs), services running on the discovered OS, and possibly the versions of the running services on a remote system or network connected device. A thorough port scan is a key component to a successful vulnerability assessment. The results that are returned by the port scan will determine what additional tools will be required during “Step 3 – Target Identification” and “Step 4 – Vulnerability Assessment” of Team Elert's methodology.

To more easily explain this technique, each network-enabled system has 65,536 TCP and UDP ports that could potentially have a remotely accessible service running on them. These ports could host legitimate business required services as well as unnecessary or malicious services if the system and/or network device was configured improperly or has been compromised prior to the testing.

Using port scans helps Team Elert to discover what types of services are being hosted on the remote system/device and allows us to compare these findings to standardized best security practices such as those from the NIST, the Center for Internet Security (CIS), and published malware databases.

Depending on the scope of the network and the time allotted for testing, it is not always necessary or feasible to test every port on every system. For these situations, Team Elert typically uses a customized port list that includes the most common ports. For this part of the testing, Team Elert relies mostly on the following port scanners:

Table 1: Team Elert Sample Toolset for Port Scanners

Tool	License
Nessus	Commercial
Nmap	Open-Source
NetCat	Open-Source
Angry IP Scanner	Open-Source
SuperScan	Freeware

Task 3 – Topology Analysis

Routing and networking protocols will be examined, compared, and consolidated to create a logical network schema of the Internet-accessible network. This schema will be used in order to identify critical and/or production networks, development and testing or isolated/separate networks, and create a target environment layout. During this analysis, Team Elert engineers will also determine if access control lists (ACLs) are configured on any discovered isolated/separate networks or Virtual Local Area Networks (VLANs) as approved by the WVCPRB designated POC.

Step 3 – Target Identification

Once the target environment layout for the WVCPRB's external-facing network(s) has been obtained, various tools and techniques will be used to determine the types of hardware, software, and applications that are deployed on the discovered systems and devices. Depending on the configurations of the OS, services, and applications, some of this information may have been retrieved during the "Step 2 – Target Probe" phase of this methodology. Some methods that Team Elert will use to determine this information are:

- Protocol stack signatures;
- Banner responses;
- Device responses;
- Communication protocols;
- Hardware-specific services;
- Software-specific services; and
- Source code analysis.

Task 1 – Determine Purpose and Functions

By correlating discovered services and specific details identified with the networking layout, Team Elert will accurately determine the purpose and function of each component. At first, it might seem difficult to identify a system's purpose or function without proper documentation; however, Team Elert engineers have extensive experience in discovering critical components of an infrastructure. For instance, if Team Elert comes across a system with open TCP ports 389 and 636, they can determine this is an LDAP server. To further identify this system, they might find ports such as TCP 22 open, which is the SSH service more commonly found on a UNIX or Linux operating system. They may find TCP ports 135, 445, and 3389 instead, which would hint to NetBIOS, SMB, and RDP services most commonly found on Windows operating systems.

Task 2 – Define Tools and Techniques

Once the services on the systems and network connected devices have been properly identified, Team Elert will determine which tools to use to accurately assess their security posture. Tools chosen normally map to the way the service delivers its information. Certain services require specific tools or scripts configured in a particular way, whereas other services simply just need to be connected.

Task 3 – Target Selection

This task of target identification has multiple factors that decide how many systems and/or devices are tested. Typically, Team Elert scans all targets within the scope of the SOW with network-based vulnerability scanners. However, Team Elert may or may not scan certain systems or network-connected devices based on their criticality. We will furnish a list of possible targets and it will be at the WVCPRB's discretion which systems Team Elert is to attempt to exploit (and approve our proposed method of penetration)

Step 4 – Vulnerability Assessment

With the profile of the WVCPRB external facing network(s) completed, Team Elert will evaluate the security posture of the network segment as a whole by testing the connection points of the network hosts on that network. Some assessment models rely heavily on commercial tools, while others do not use them at all. Team Elert believes that although such tools are often laden with false positives, they do provide an efficient and effective means to obtain a summary of the networking environment and a broad security baseline. Depending on the target environment, our team may execute a combination of commercial, freeware, open-source, and custom assessment tools, such as:

Table 2: Team Elert Sample Toolset for Vulnerability Assessments

Tool	License
Nessus	Commercial
Nmap	Open-Source
Wireshark	Open-Source
Ettercap	Open-Source
EtherApe	Open-Source

In addition to these baseline network tools, Team Elert will utilize a series of manual “point” tools and scripts. These tools provide more thorough tests for specific vulnerabilities such as Web servers (e.g., Microsoft IIS, Apache, Oracle Application Server), Web code (e.g., ASP, JavaScript, PHP, .NET), and other non-standard services. The use of these specific tools allows us to further adjust the tests to ensure that as many environmentally-unique configurations as possible are analyzed. Some of these tools Team Elert uses for specific testing are:

Table 3: Team Elert Sample Toolset for “Point” Tools

Tool	License
Metasploit	Open-Source
Nikto	Open-Source
OneSixtyOne	Open-Source
NBTScan	Open-Source
DISA SRR Scripts	Open-Source

Step 5 – Exploitation and Verification

The more critical and time-consuming aspect of the active testing process is the vulnerability verification. The penetration testing component will only take place on those systems approved by the WVCPRB designated POC. However, based on the results of the vulnerability scans (we plan to scan all visible systems) our team may suggest additional penetration targets. Suspected vulnerabilities identified previously are manually re-checked to confirm their existence, and the potential risk impact is assessed. Oftentimes, a vulnerability in one system may lead to the exposure of many other systems and applications on the target network, a technique known as pivoting. Such secondary targets cannot be identified in the first (automated) pass or until a first successful exploitation of a suspected vulnerability is made.

When performing vulnerability assessments or penetration tests, one of the biggest obstacles in providing a valuable product is dealing with false positives. Once the raw results from the automated and manual tools are collected, Team Elert’s team begins the process of verifying and cross-referencing them against not only our extensive vulnerability knowledgebase, but also against the Common Vulnerabilities and Exposure (CVE), National Vulnerability Database (NVD), and several other knowledgebases used throughout the security community. Findings discovered by the automated tools are further tested to ensure false positives, possibly caused by customizations, are eliminated. Weaknesses are also correlated against our knowledgebase to determine if potential false negatives were omitted. In order to verify whether a vulnerability is a false positive, we will often need to attempt to exploit it. Prior to attempting any such exploits, Team Elert will notify the WVCPRB officials and coordinate all penetration efforts. Team Elert will not attempt to exploit any vulnerability that may cause a Denial of Service (DoS) or other disruption unless explicitly approved by the WVCPRB designated POC.

A series of sophisticated tests then follows where our team leverages our extensive experience and proprietary knowledgebase of security software, attack profiles, test scripts, and exploit programs to assess the security of the target environment.

Incorrectly configured and/or unsecured network protocols and services that may be exploited include:

- Protocols
 - Transmission Control Protocol (TCP)
 - User Datagram Protocol (UDP)
 - Border Gateway Protocol (BGP)
 - Routing Information Protocol (RIP)
 - Stream Control Transmission Protocol (SCTP)
 - Address Resolution Protocol (ARP)
 - Simple Network Management Protocol (SNMP)
 - Cisco Discovery Protocol (CDP)
 - Bootstrap Protocol (BOOTP)
 - Internetwork Packet Exchange (IPX)
- Services
 - DNS(SEC)
 - NetBIOS
 - RPC
 - Samba
 - HTTP(S)
 - FTP(S)
 - SMTP(S)
 - IMAP(S)
 - POP(S)

Exploitation will generally be targeted to:

- Escalate access permissions.
- Gain access to sensitive files.
- Leverage exploited systems for new attacks.
- Hide evidence of intrusion.

To illustrate our verification and exploitation approach, please see the sample below. In this case, the vulnerability scan reported that a web server had dangerous HTTP methods, including PUT, enabled.

The DELETE method allows an attacker to delete arbitrary content from the web server.

Solution

Disable the PUT and/or DELETE method in the web server configuration.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

BID	12141
XREF	OSVDB:397
XREF	OSVDB:5646
XREF	OWASP:OWASP-CM-001

Exploitable with

Metasploit (true)

Plugin Information:

Publication date: 2000/08/30, Modification date: 2011/09/14

Hosts

.248.39 (tcp/443)

The remote web server supports the following methods :

- PUT (the file '/vvvvov1.html' has been uploaded)
- DELETE (the file '/vvvvov1.html' has been deleted)

Figure 3: Sample Vulnerability Scan Report

Instead of just reporting this as a finding, our team's approach is to verify the vulnerability using multiple tools and manual techniques. We first used Metasploit to determine if the vulnerability was a false-positive or not. As you can see in the figure below, it was not successful.

```
Basic options:
  Name      Current Setting  Required  Description
  ----      -
  ACTION     PUT                    yes        PUT or DELETE
  FILEDATA   msf_test_file          no         The data to upload into the file
  FILENAME   msf_http_put_test.txt  yes        The file to attempt to write or delete
  PATH       /                      yes        The path to attempt to write or delete
  Proxies    [REDACTED]             no         Use a proxy chain
  RHOSTS     [REDACTED].248.39      yes        The target address range or CIDR identifier
  RPORT      443                   yes        The target port
  THREADS    1                     yes        The number of concurrent threads
  VHOST      [REDACTED]             no         HTTP server virtual host

Description:
  This module can abuse misconfigured web servers to upload and delete web content via PUT and DELETE HTTP requests. Set ACTION to either PUT or DELETE. PUT is the default. If filename isn't specified, the module will generate a random string for you as a .txt file. If DELETE is used, a filename is required.

References:
  http://www.osvdb.org/397

msf auxiliary(http_put) > run

[-] File doesn't seem to exist. The upload probably failed.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 4: Metasploit scan showing exploitation failure

We then used Nmap with a NSE script to confirm the finding. Here it was successful as seen in the figure below. Manual attempts could also have been used to confirm the vulnerability.

```
fritschieg@packet-too-large:/opt/metasploit-framework$ sudo nmap --script=http-  
methods.nse --script-args http-methods.retest=1 [REDACTED].248.39  
[sudo] password for fritschieg:  
  
Starting Nmap 6.25 ( http://nmap.org ) at 2014-01-08 10:09 EST  
Nmap scan report for [REDACTED].248.39  
Host is up (0.014s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
80/tcp    open  http  
|_ http-methods: No Allow or Public header in OPTIONS response (status code 403)  
443/tcp    open  https  
|_ http-methods: OPTIONS TRACE GET HEAD DELETE COPY MOVE PROPFIND PROPPATCH SEARCH  
MKCOL LOCK UNLOCK PUT POST  
|_ Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MK  
COL LOCK UNLOCK PUT  
|_ See http://nmap.org/nsedoc/scripts/http-methods.html  
|_ OPTIONS / -> HTTP/1.1 200 OK  
  
|_ TRACE / -> HTTP/1.1 501 Not Implemented  
  
|_ GET / -> HTTP/1.1 302 Object moved  
  
|_ HEAD / -> HTTP/1.1 302 Object moved  
  
|_ DELETE / -> Error getting response  
|_ COPY / -> HTTP/1.1 400 Bad Request  
  
|_ MOVE / -> HTTP/1.1 400 Bad Request  
  
|_ PROPFIND / -> HTTP/1.1 411 Length Required  
  
|_ PROPPATCH / -> HTTP/1.1 400 Bad Request  
  
|_ SEARCH / -> HTTP/1.1 411 Length Required  
  
|_ MKCOL / -> HTTP/1.1 405 Method Not Allowed  
  
|_ LOCK / -> HTTP/1.1 403 Forbidden
```

Figure 5: Nmap NSE Script Successful

The figure above shows that Team Elert engineers do not just accept the scan results and instead we attempt to verify the existence of the findings. This effort does result in additional time being spent on the testing; however, we believe the benefits outweigh the extra effort. In order to increase efficiency, we group similar findings from multiple hosts together and do not verify each finding on all hosts. Rather, we perform a sampling approach as it relates to vulnerability verification.

1.2.3 Internal Vulnerability Assessment

"4.1.2.3 A review of all of the devices on the network with static IP addresses"

The internal vulnerability testing process is quite similar to the external penetration tests described above but with a few exceptions – typically when conducting the internal tests we are provided the scope of devices and range of IP addresses rather than having to perform preliminary data gathering. Also, our testers are not hindered by IDS/IPS systems so there is no need to use stealth techniques and the scan rate is thus much quicker. Being inside the security perimeter we are also often provided with access privileges which allow us to run “host-based” tests on a selected sample of servers and workstations to assess compliance with industry best practices. Host-based testing is used to evaluate local security policies. Some of the following areas will be examined using this type of testing:

- Account and password policies
- Auditing and logging policies
- Local or group policy enforcement
- Host-based firewall configurations
- Antivirus configurations
- Security patch and update compliance

Nessus with compliance checking enabled, or similar tools such as security benchmark scoring tools from Center for Internet Security (CIS), will be used to compare the system to several standardized security benchmarks, such as those from National Institute of Standards and Technology (NIST) and the System Administration, Networking, and Security Institute (SANS).

1.2.4 Review of Network Device Configurations

"4.1.2.4 A review of the server, firewall, and IDS configurations"

Firewall Review

Firewalls are typically the primary method that organizations use to control ingress and egress access to their networks and systems. Team Elert has a great deal of experience in performing firewall reviews and assessments. The majority of the larger vulnerability assessment tasks we have conducted involve an analysis of the firewall security architecture, including the rule base. Team Elert has performed this type of work for both Federal and commercial customers. Some of these clients, such as Amtrak and the National Finance Center (NFC), had extremely large and complex firewall architectures. Others, such as City of Alexandria were more basic, but in all cases, our analysis allowed them to make improvements to enhance their firewall security architecture.

In performing this review, Team Elert will follow its proven methodology based on NIST guidelines, including SP 800-41, *Guidelines on Firewalls and Firewall Policy*, as well as industry-standardized, security-established guidelines from Center for Internet Security (CIS). Previous firewall reviews, if available, will be closely examined in order to provide continuity, as well as to verify that any findings noted previously were addressed.

The firewall audit and review will be performed in four tasks:

- Information gathering;
- Automated and manual testing;
- Raw data analysis; and
- Deliverables compilation.

Team Elert's security engineers will inspect actual firewall settings and configuration parameters against those listed in the system documentation and firewall policies. For example, we will verify that all network interfaces of each firewall are properly documented and all rules in the rule-set can be traced back via configuration management documentation. In performing these inspection activities, Team Elert will work with the firewall administrators but will not require a user name and password access to the firewalls. The firewall configuration will also be compared to vendor recommendations, best security practices, security benchmarking guidelines, and WVCPRB's firewall policies. Areas such as traffic and protocols allowed inbound and outbound, number of rules, duplications, rules with the source and/or destination ANY, configuration settings, logging parameters, and more will be examined.

Our past experience indicates that the longer the rule-set table(s), the higher the risk of unintended access permissions. Rule-sets containing more than a few dozen lines become unwieldy to manage, especially in a multi-firewall environment. Over time, rule-sets may fall out of step with current security policies; consequently, irrelevant rules may proliferate.

Similarly, as more rules are added to the rule-set table(s), overall firewall performance will degrade as more rules have to be evaluated in top-to-bottom fashion until a proper decision is made or the packet is dropped. In order to improve performance, we will identify which rules are used the most and recommend moving them up the table as long as this does not conflict with the overall logic of the security policy. In reviewing the firewall configuration, we will examine (for example) if:

- The firewall placement, from a network topology perspective, is most logical.
- The firewall has isolation between servers that reside in different security zones.
- No externally accessible systems or devices lie within the internal network zone.
- Hardware, operating system, and firewall software versions are up to date.
- The firewall location is secure with physically-controlled access.
- Administrative accounts are current and utilize strong authentication policies.

Router/Switch Review

Routers and switches are the backbone of an organization's IT infrastructure. If a malicious attacker is able to gain access to these devices, some of the following actions could be performed:

- Map the network.
- Forward traffic.
- Sniff traffic.
- Establish encrypted backchannels.
- Cause Denial of Service (DoS).

In order to assess the security controls of WVCPRB's routers and switches, a series of tests will be performed. Initially, automated vulnerability scans will be executed to examine the security posture. For example, Nmap will be used to determine the ports that are open on the devices and Nessus can be used to determine whether any network vulnerabilities are visible. However, these network scanning tools are only effective to a certain level. The most effective way to determine the overall security posture for these types of devices is a thorough review of the device configurations. In order for Team Elert to complete this task, our team will need to be provided with exported configurations from WVCPRB's routers and switches by the appropriate network personnel. Once Team Elert has obtained these configurations, they will be run through an automated configuration analysis tool such as Nipper or the Router Auditing Tool (RAT), which will compare the configurations to standardized best security practices and security benchmarks. This allows Team Elert to find significant vulnerabilities or the "low hanging fruit" quickly.

Once the reports from the automated analysis tools is complete and reviewed by Team Elert engineers, a more thorough manual analysis will be done by trained and certified security engineers to first verify that vulnerabilities discovered by the automated tools are not false-positives, but to also ensure that vulnerabilities don't exist that might have been missed by these automated tools. WVCPRB's router and switch configurations will be reviewed line-by-line looking for potential misconfigurations or other errors such as:

- Lax or non-existent access control lists (ACLs)
- Port security configurations
- Unsecure management policies
- Unsecure services enabled
- Default or weak passwords
- Unsecure VLAN configurations.

Due to the number of routers and switches that WVCPRB has deployed, a sampling approach may be utilized.

Server Security Controls

A new phase is also added to the internal testing known as "Host-Based" (i.e. authenticated scans) testing. Previous testing done externally and the beginning of the internal testing are considered "Network-Based" testing. While network-based testing is used to identify network level vulnerabilities, host-based testing is used to evaluate local security policies. Some of the following areas will be examined using this type of testing:

- Account and password policies
- Auditing and logging policies
- Local or group policy enforcement
- Host-based firewall configurations
- Antivirus configurations
- Security patch and update compliance

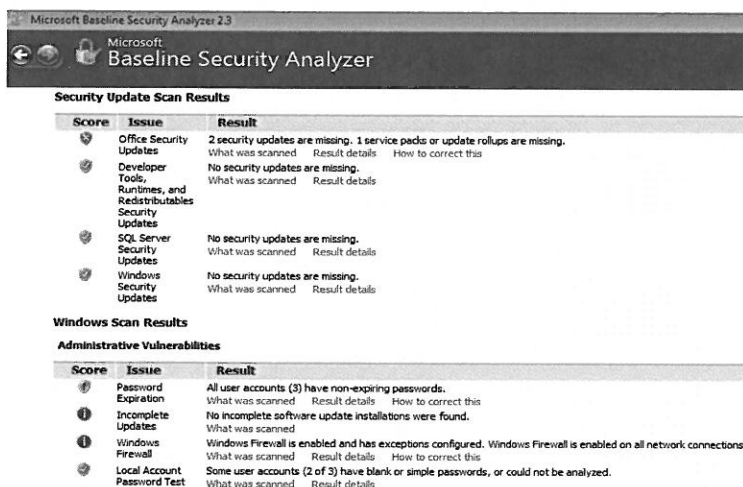
Nessus with compliance checking enabled, or similar tools such as security benchmark scoring tools from CIS, will be used to compare the system to several standardized security benchmarks, such as those from NIST and the System Administration, Networking, and Security Institute (SANS).

Microsoft's Baseline Security Analyzer (MBSA) may also be utilized to evaluate Windows systems, primarily for patch compliance. Close coordination with WVCPRB's system administrators will be required as administrator/root privileges are needed to run these tools.

The figure below shows an example of the types of compliance checks that are available.

Windows Server 2008 R2 v2.1.0	Windows Server 2008 R2 MS v2.1.0	Windows Server 2008	This audit file implements the recommendations provided by the CIS Microsoft Windows Server 2008 R2 Benchmark v2.1.0. <i>Note: This policy is currently under review by the CIS organization for certification. The final certified audit may contain different tests and descriptions than this current policy.</i> (Last updated July 30, 2014.)
Windows 7 v1.1.0	Windows 7 Ent Desktop v1.1.0	Windows 7	This audit file implements a majority of the configuration checks from the CIS Microsoft Windows 7 Benchmark v1.1.0 for Enterprise Desktops. In addition to the checks implemented in the .audit file, a full patch audit (the entire Windows: Microsoft Bulletins plugin family) as well as plugins "SMB NativeLanMan" (#10785), "Insecure Logical Drive FileSystem" (#24871) and "DEP is disabled" (#24282) are required. (Last updated December 20, 2011.)
Windows 7 v1.1.0	Windows 7 Ent Laptop v1.1.0	Windows 7	This audit file implements a majority of the configuration checks from the CIS Microsoft Windows 7 Benchmark v1.1.0 for Enterprise Laptops. In addition to the checks implemented in the .audit file, a full patch audit (the entire Windows: Microsoft Bulletins plugin family) as well as plugins "SMB NativeLanMan" (#10785), "Insecure Logical Drive FileSystem" (#24871) and "DEP is disabled" (#24282) are required. (Last updated December 20, 2011.)
Windows 7 v1.1.0	Windows 7 SSLF Desktop v1.1.0	Windows 7	This audit file implements a majority of the configuration checks from the CIS Microsoft Windows 7 Benchmark v1.1.0 for SSLF Desktops. In addition to the checks implemented in the .audit file, a full patch audit (the entire Windows: Microsoft Bulletins plugin family) as well as plugins "SMB NativeLanMan" (#10785), "Insecure Logical Drive FileSystem" (#24871) and "DEP is disabled" (#24282) are required. (Last updated July 26, 2011.)
Windows 7 v1.1.0	Windows 7 SSLF Laptop v1.1.0	Windows 7	This audit file implements a majority of the configuration checks from the CIS Microsoft Windows 7 Benchmark v1.1.0 for SSLF Laptops. In addition to the checks implemented in the .audit file

Figure 6: Windows Compliance Checks



This allows our testing team to quickly and accurately discover the security posture of Windows systems by performing a simple scan. We then review these results and if needed verify the settings on the actual systems. For those systems that cannot be scanned, we will perform a manual review using the benchmark. The Microsoft Baseline Security Analyzer (MBSA) will also be used as a secondary tool in order to verify some of the results.

MBSA is a tool developed by Microsoft which provides a streamlined method to identify missing security updates and common security mis-configurations.

1.2.5 Remediation Services

“4.1.2.5 Provide Post-Assessment Remediation Services if prime contractor cannot address the identified vulnerabilities.”

Team Elert successfully performed numerous remediation activities following security vulnerability assessments and penetration testing exercises. Should WVCPRB need our support beyond the assessment phase, our security engineers will be available to make necessary changes and/or to re-test IT infrastructure components to ensure that vulnerabilities have been properly mitigated.

1.3 Ranking Discovered Vulnerabilities

“4.1.2 Prioritize and rank the discovered vulnerabilities using the Common Vulnerability Scoring System (CVSS).”

Our report will rank all findings in accordance with the Common Vulnerability Scoring System Version 2.0 and will include the Base, Temporal and Environmental metrics for each vulnerability.

1.4 Assessment Report

“4.1.3 For each assessment, provide a written report, including at a minimum, the following:

4.1.3.1 Executive Summary

4.1.3.2 Summary of Target Environment

4.1.3.3 Scope (including systems assessed and method used)

4.1.3.4 Findings (in social engineering, data loss prevention, firewall architecture and policy, and endpoint assessment)

4.1.3.5 Recommendations (including “quick wins” and strategic recommendations)

4.1.3.6 Support or cross-reference all observed deficiencies and associated recommendations to one or more of the following standards or guidelines: National Institute of Standards and Technology Special Publication 800-53 2, or SANS Consensus Audit Guidelines³.

4.1.3.7 Appendix (including evidence and screenshots).”

For each iteration of our security vulnerability assessment, Team Elert will produce a detailed test report. Team Elert never delivers machine-produced scans as “test reports.” Such information is usually included in an attached CD-ROM as raw results. For this engagement, we will develop two separate reports, one for the social engineering task and another for the external penetration testing. A typical audit report for an effort of such magnitude will contain the following sections:

- An Executive Summary providing a high-level review of the effort including objective and target systems/environment and the main finding, as well as synopsis of the report.
- An overview of the findings grouped by category of tests or inspections:
- A step-by-step description of each of the test conducted along with key screen captures documenting the testing process.
- A table of findings titled “Findings, Implications, and Recommendations” listing all identified vulnerabilities and notable information concerning tested devices. Each table entry contains a list of affected devices identified by IP addresses, a brief description of the vulnerability along with its common vulnerabilities and exposures (CVE – if applicable), its ease of exploitation, an impact analysis, an overall CVSS V2 risk rating, and recommended corrective action with applicable pointers to external resources.

In order to simplify the tracking of corrective actions and to conserve space, we will combine identical vulnerabilities of different devices into a single line in the table.

- Conclusions and detailed recommendations for remediation actions along with estimated level of effort are necessary for implementation. The Recommendations section is divided into subsections addressing each of the assessment areas requested in the Statement of Work (SOW).
- An appendix will contain all relevant screen captures and raw tests results referenced in the report. If the volume of raw test results is too large, it will be provided on a separate CD-ROM.

The Test Report will be provided first in a draft form to allow WVCPRB officials to review and comment on its findings. Team Elert will make necessary updates as identified in WVCPRB feedback and deliver a final version.

Our final reports are meticulously detailed. Because all tests are documented as they are performed, we accumulate a wealth of information, which we try to convey in the most concise and clear form in our report.

Unlike other formats we encountered where the raw test output was submitted as the report, we take a significant effort to analyze and interpret the results. The bulk of the report will be in a table format known as the Vulnerability Summary Matrix. Each identified vulnerability will be listed, with its CVE ID when it is known.

We will assign a relative measure of risk to the vulnerability (Low, Medium and High, Critical), and outline potential remedies in the Recommendations Section. An appendix will contain all relevant raw tests results referenced in the report.

All findings will be reviewed and assigned a risk rating. Each vulnerability is assigned a "severity level" based on the following definition:

- **CRITICAL:** If exploited, this vulnerability would yield complete control of the subject system or give hackers access to extremely sensitive data. It could severely disrupt system operations and integrity.
- **HIGH:** If exploited, this vulnerability would give over at least partial control of the system; allow access to sensitive data, and compromise system controls or system integrity.
- **MEDIUM:** While not directly leading to a system security breach, exploiting this vulnerability may play a significant role in degrading a system if combined with other vulnerabilities or pertinent system information available to an attacker.
- **LOW:** A vulnerability which is unlikely in itself to lead directly to a system compromise, but it can in some way aid an attacker indirectly in mounting attacks against the subject system.
- **N/A:** Does not necessarily indicate a vulnerability. It is used when a risk level cannot be assigned. Most often it is used when a service is detected. For example, if port scans identify port 25 (SMTP) open it is not necessarily a vulnerability because the service may be needed for a business purpose. However, unnecessary services often are enabled by default and are not needed.

Each vulnerability is also assigned a “difficulty of exploit” rating:

- **Trivial:** Requires a beginner-intermediate skill set, nominal time commitment, and possible use of tools/knowledge commonly available.
- **Moderate:** Requires an intermediate skill set and knowledge, such as the ability to create simple script and simple programs.
- **Sophisticated:** Requires the dedicated effort of a professional-calibre cracker.

Team Elert provides specific recommendations for each finding in the vulnerability matrix. These recommendations are based on industry best practices, vendor recommendations, and our own experience. The majority of the recommendations are listed in the Vulnerability Matrix table. For example, if a vulnerability is noted that is caused by a patch not being applied, the specific patch that needs to be applied will be listed in the recommendations section of the matrix. Other general recommendations are listed in the Recommendations section, where they are divided into the following categories:

- **Quick Hits:** Recommendations that can be applied quickly to mitigate a vulnerability (i.e., apply the appropriate patch).
- **Next Steps:** Recommendations that take more time to implement or investigate.
- **Strategic Initiatives:** Recommendations that may take a while to implement as they suggest changes that may seriously affect the network.

All recommendations will include the estimated time and level of effort to apply the corrective actions.

1.5 Firewall Architecture and Policy Review

“4.1.4 Firewall Architecture and Policy Review

4.1.4.1 Perform external automated vulnerability scanning using a vulnerability scanning solution approved by the Security Content Automation Protocol (SCAP) to identify Internet-exposed weaknesses at the network and host level.

4.1.4.2 Use Expert interview, paper analysis, and direct observation to identify deficiencies in firewall policy, architecture, and administration.

4.1.4.3 Quantify the Internet attack surface and provide specific recommendations to reduce and manage risks from the Internet vector.”

Firewall Review

Firewalls are typically the primary method that organizations use to control ingress and egress access to their networks and systems. Team Elert has a great deal of experience in performing firewall reviews and assessments. The majority of the larger vulnerability assessment tasks we have conducted involve an analysis of the firewall security architecture, including the rule base. Team Elert has performed this type of work for both Federal and commercial customers. Some of these clients, such as Amtrak and the National Finance Center (NFC), had extremely large and complex firewall architectures. Others, such as the City of Alexandria were more basic, but in all cases our analysis allowed them to make improvements to enhance their firewall security architecture.

In performing this review, Team Elert will follow its proven methodology based on NIST guidelines, including SP 800-41, *Guidelines on Firewalls and Firewall Policy*, as well as industry-standardized, security-established guidelines from Center for Internet Security (CIS). Previous firewall reviews, if available, will be closely examined in order to provide continuity, as well as to verify that any findings noted previously were addressed.

The firewall audit and review will be performed in four tasks:

- Information gathering;
- Automated and manual testing;
- Raw data analysis; and
- Deliverables compilation.

Team Elert's security engineers will inspect actual firewall settings and configuration parameters against those listed in the system documentation and firewall policies. For example, we will verify that all network interfaces of each firewall are properly documented and all rules in the rule-set can be traced back via configuration management documentation. In performing these inspection activities, Team Elert will work with the firewall administrators but will not require a user name and password access to the firewalls. The firewall configuration will also be compared to vendor recommendations, best security practices, security benchmarking guidelines, and WVCPRB's firewall policies. Areas such as traffic and protocols allowed inbound and outbound, number of rules, duplications, rules with the source and/or destination ANY, configuration settings, logging parameters, and more will be examined.

Our past experience indicates that the longer the rule-set table(s), the higher the risk of unintended access permissions. Rule-sets containing more than a few dozen lines become unwieldy to manage, especially in a multi-firewall environment. Over time, rule-sets may fall out of step with current security policies; consequently, irrelevant rules may proliferate.

Similarly, as more rules are added to the rule-set table(s), overall firewall performance will degrade as more rules have to be evaluated in top-to-bottom fashion until a proper decision is made or the packet is dropped. In order to improve performance, we will identify which rules are used the most and recommend moving them up the table as long as this does not conflict with the overall logic of the security policy. In reviewing the firewall configuration, we will examine (for example) if:

- The firewall placement, from a network topology perspective, is most logical.
- The firewall has isolation between servers that reside in different security zones.
- No externally accessible systems or devices lie within the internal network zone.
- Hardware, operating system, and firewall software versions are up to date.
- The firewall location is secure with physically-controlled access.
- Administrative accounts are current and utilize strong authentication policies

We will also verify that a documented configuration management policy/process is followed to implement and track Firewall configuration changes. All rule-set changes are approved at the appropriate level and include the reason for the change.

We will compare findings from the remote penetration test with the rule set to examine if the external foot print contain devices and/or services which should not be accessible from the outside and make recommendations on changes to the firewall architecture, rule-set and device placement as necessary.

1.6 End Point Devices Assessment

“4.1.5 Endpoint Assessment

4.1.5.1 Perform automated host-based scanning against a sample of 15 desktop and laptop systems to identify weaknesses that facilitate remote desktop compromise.

4.1.5.2 Identify ways to optimize currently deployed technologies which monitor, detect, and respond to endpoint exploit and compromise.

4.1.5.3 Provide a vendor-agnostic roadmap for closing discovered endpoint gaps and aligning CPRB with endpoint security best practices within 18 months of the assessment.”

Team Elert’s extensive experience in providing turn-key security solutions to our clients extends to protecting end user devices that include desktops, laptops, peripherals and mobile devices. We believe that the majority of potential end user device vulnerabilities can be tightly controlled by diligent application of the following processes:

Configuration Control. To simplify the management of end user environment, we highly recommend strict control of desktop and laptop hardware and software configurations keeping them uniform across the entire organization. Maintaining current inventory of all devices goes a long way towards this goal, as does the utilization of centralized version and patch management for operating systems and applications.

In the performance of the assessment project, Team Elert will verify if CPRB has standard configurations defined. We will also confirm the implementation of the existing standards and whether end users are aware of their existence. Finally, we will recommend any improvements to the process, including recommended tools that will simplify the process.

Access Control. We strongly recommend restricting end user access to the minimum that is required for performing their job duties. Specifically, preventing end users from installing their own software packages or modifying operating systems helps to reduce the overhead of maintaining the modified devices and ensure consistent effects of all security controls. Of course there will always be exceptions for power users (i.e., network administrators, CAD and publishing software users, etc.).

The best way to achieve compliance with this rule is through the use of group policies. There are numerous tools that help simplify this process, and Team Elert will be happy to recommend the most advantageous solution for CPRB.

Periodic Security Scans. This can be done by preinstalling a host-based tool and running it on a schedule either remotely or locally.

The most common tool used for this purpose is Microsoft Baseline Security Analyzer (MSBA) available from Microsoft free of charge. MSBA provides a streamlined method to identify missing security updates and common security misconfigurations. MSBA 2.3 release adds support for Windows 8.1, Windows 8, Windows Server 2012 R2, and Windows Server 2012.

MBSA is built on the Windows Update Agent and Microsoft Update infrastructure, ensuring consistency across Microsoft management products, including Microsoft Update (MU), Windows Server Update Services 2.0 and 3.0 (WSUS), Systems Management Server Inventory Tool for Microsoft Update (ITMU) (SMS), System Center Configuration Manager (SCCM) 2007, and Small Business Server (SBS). The tool also inspects most Microsoft applications, such as Microsoft Office, Microsoft PowerPoint, Microsoft SharePoint, etc.

Intrusion Detection/Prevention. Although this technology is used primarily for network and shared devices, it may be advisable to apply it to critical and sensitive end user devices.

One of the popular open source intrusion detection systems is distributed by OSSEC (www.ossec.net). It monitors various devices running Windows, Linux, MacOS, Solaris, HP-UX, and AIX. It requires installing a very small agent software on each monitored host while most settings are contained in the centralized manager device.

There are numerous options for IPS/IDS implementations. After reviewing CPRB environment, Team Elert will recommend solutions tailored to the organization's need and budget.

Security Awareness Training. In our opinion, this is by far the most effective and efficient way to improve the organization's security posture. An educated user is much more attuned to the risks associated with using information systems. As the result, the user accepts the "burdens" inevitably imposed by security controls.

1.7 Data Loss Prevention

"4.1.6 Data Loss Prevention Gap Analysis

4.1.6.1 Use Expert interview, paper analysis, and direct observation to audit how CPRB exchanges confidential data with external parties, and identify weaknesses.

4.1.6.2 Identify ways to optimize currently deployed technologies to monitor, detect, and respond to data loss caused by stolen or lost mobile and portable storage devices.

4.1.6.3 Provide a vendor-agnostic roadmap for closing discovered gaps and aligning CPRB with data loss prevention best practices within 18 months of the assessment."

Due to the increasing risk and potential exposure to sensitive data (i.e. credit card numbers, PII), CPRB is seeking a trusted partner to perform a data discovery and data loss prevention (DLP) assessment. Protecting PII and other sensitive data is difficult as it can "leak out" intentionally and unintentionally in many ways, such as:

- E-mail attachments
- Printouts and faxes
- Lost tapes, zip drives, and other storage media
- Lost or stolen laptops
- Social networking
- Instant messaging programs
- File sharing programs
- Unsecure Web sites
- Active attacks by bad actors

Methods to protect PII range from operational and management controls to technical controls such as:

- Encryption
- Multi-factor Authentication
- Strong Access Controls
- Security Awareness Training
- Endpoint Security
- Data Leakage Prevention

During the course of Team Elert's review, we will identify the paths that data may leave the network as well as evaluate existing controls in-place. However, initially we need to establish the definition of "sensitive data", and determine all possible locations where sensitive data resides on the network in order to accurately protect it both at the server level and the endpoints.

Team Elert's approach is a combination of manual and automated techniques in order to determine the location of this data. We will conduct interviews with various stakeholders to determine the most likely locations of this data. Additionally, automated techniques either using active scanning or passive analysis via an agent may be utilized.

Once we have completed the interviews and other data collection efforts, we will have an understanding of CPRB's current data footprint. This includes where sensitive data resides and the mechanisms it is transmitted into and out of the network. Once the current environment is fully documented and understood, Team Elert will perform a gap analysis and determine areas where the design and data security do not meet established best practices (i.e. DISA, CIS, NIST).

Gap Analysis is all about evaluating and improving business performance. In information technology, gap analysis is the study of the differences between two different information systems or applications, often for the purpose of determining how to get from one state to a new state. A gap is sometimes spoken of as "the space between where we are and where we want to be." Gap analysis is undertaken as a means of bridging that space.

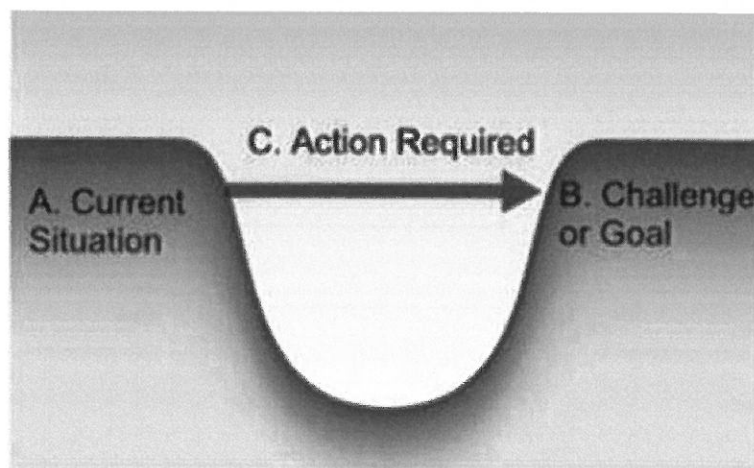


Figure 7: Gap Analysis

This will show where they are currently and what the gaps are that need to be met in order to bridge those deficiencies. Depending on the results of the testing we will recommend solutions for CPRB to follow. These may include updating process and procedures to implementing technical security controls such as DLP solutions. By implementing a strong DLP program, CPRB will be able to address the requirements of Continuous Monitoring (NIST SP 800-137) in the Risk Management Framework. Additionally, it can be used to satisfy the recommended security controls for Federal Information Systems and Organizations defined (NIST SP 800-53).

- Information Flow Enforcement (AC-4)
- Remote Access (AC-17)
- Information System Connections (CA-3)
- Continuous Monitoring (CA-7)
- Least Functionality (CM-7)
- Information Output Handling and Retention (SI-12)

1.8 Executive Presentation

“4.1.7 Collaborate with the CPRB Guidance Team to develop and deliver executive presentations of the assessment and its results.”

Team Elert will conduct an executive briefing at the conclusion of each security vulnerability assessment iteration. We will strive to work closely with WVCPRB guidance team in order to maximize knowledge transfer at the various stake-holder levels. Typically a single out-brief presentation will be held, but if needed, multiple presentations can be arranged for different audiences (e.g., networking staff, application maintenance staff, etc.). The presentations will cover highlights of the effort – objectives, tools and methodologies, main vulnerabilities, conclusions, and recommendations.

The presentation notes are intended as a backdrop for an open discussion and transfer of knowledge between Team Elert and the relevant WVCPRB stakeholders. We can also discuss, at WVCPRB’s discretion, optional services to be provided by Team Elert as follow-on tasks. Such activities will be geared to assist WVCPRB in implementing the corrections and security upgrades resulting from this study.

1.9 Past Performance Examples

“4.1.8 Provide documented evidence of the performance of a vulnerability assessment and/or penetration test on a government entity or corporation that has the minimum of 5,000 employees. Evidence of this should be in the form of a list of the Vendor’s clients meeting this requirement with the total number of employees for each client identified with the client name. The employee count should be the total number of employees in the entire organization (federal agency, state government, county government, corporation, etc.), including all divisions, agencies, sections, etc. and may be rounded to the nearest hundred. (For example, the State of West Virginia has approximately 30,000 employees.)”

SeNet International Corporation (SeNet), a member of Team Elert, is an innovative leader in IT services, specializing in networking and information systems security consulting for Federal agencies and commercial entities. SeNet focuses on helping clients meet their network infrastructure and information security goals by establishing close working relationships and by mapping clients’ goals and mission requirements to proven solutions. At all times, SeNet maintains an awareness of clients’ established policies and procedures and ensures that all of our work efforts are compliant with government regulations and corporate industry best practices.

SeNet is an SBA-certified small business based just outside of Washington D.C. and has been in business since 1998 assisting over 150 public- and private-sector clients in improving their information security. The services SeNet provides include vulnerability assessments and penetration testing, security program development and planning, security architecture design and implementation, security operations, and compliance verification, among others. SeNet's executives are IT industry veterans who possess both subject matter technical expertise as well as extensive experience in managing large-scale projects.

SeNet specializes in performing vulnerability assessments and penetration testing. They have conducted these types of assessments for large complex organization such as Amtrak, United States governmental components such as the Department of Health and Human Services and the Department of Education, as well as smaller organizations such as the City of Alexandria and Iowa Lottery. We are proud of all of the testing work we have performed and what makes Team Elert successful is our passion for information security, approaching testing as more than a "check-box" exercise, our staff's experience and technical skills, and management's hands-on involvement.

The table below provides a snapshot of some of our clients and the tasks we have performed.

Client	Information Services Provided (Abbreviated List)					
	Penetration Testing	Security Code Review	Vulnerability Assessments	Social Engineering	Web Application Testing	Wireless Security
BWIN.Party	✓		✓		✓	
Iowa Lottery			✓			✓
Amtrak	✓	✓	✓	✓	✓	✓
HRSA	✓		✓	✓	✓	✓
City of Alexandria	✓		✓			✓
Railroad Retirement Board		✓			✓	
Department of Education	✓		✓		✓	✓
USAC	✓				✓	
State of Maryland	✓		✓		✓	
District of Columbia	✓		✓		✓	

**Department Health and Human Services
Health Resources and Services Administration (HRSA)
IT Security Support (3,000 employees)**

**Contact Information: Steve Davis, Chief
Information Security Officer, OIT**
Phone: (301) 443-9660
Email: sdavis@hrsa.gov
COTR: Steve Davis

Period of Performance: 2007-Present

Contract Number: HHSH250200722014B

Contract Type: Fixed Firm Price

Contracting Point of Contact: Kimberly Lewis

Phone: (301) 443-2750

Scope of Project:

In November 2007, Team Elert was awarded a task order by HRSA to provide a wide range of technical assistance in conjunction with the agency's Information Security Program Plan. This included obtaining an independent assessment of HRSA's information systems; monitoring the security-related activities of these systems, and recommending changes that would enhance security across the entire spectrum of HRSA's IT infrastructure. This task was awarded competitively under a broad scope IT Security BPA issued earlier in 2007. This is a wide scope support task that covers among others the following areas:

- Penetration Testing and Vulnerability Assessments
- Information Systems Security Program Plan Implementation and Maintenance
- IT Infrastructure Evaluation and Recommendation
- Cyber Protection and Surveillance
- Incident Response Support
- Information Systems Security Policy Development and Implementation
- Support in Agency, Departmental and OIG Initiatives
- Security Awareness and Training
- Risk Assessment and Compliance Management

Under the guidance of the agency's CISO, our team of on-site analysts and engineers, assisted by subject matter experts based in our headquarters, has been successfully helping HRSA in a diverse range of IT security issues including:

- Revamping the agency set of IT security policies and procedures.
- Conducting an agency wide network inventory in order to establish an updated security baseline of knowledge about networks, systems and applications.
- Evaluating the HRSA's security program against the Departmental "Secure One" initiative.
- Assess and recommend Data at Rest (DAR) encryption solution.

In a relatively short time, Team Elert managed to establish the confidence and trust of end users, system owners, and HRSA's network operations team. Our on-site staff and headquarters based subject matter experts proactively evaluate and recommend activities that enhance HRSA's IT Security Program performance. Consulting with and borrowing solution ideas from other Team Elert staff members on other projects help us to improve team effectiveness, reduce implementation time lines and ensures a consistent and reliable technical performance. As in all other Team Elert task orders, a senior official is directly responsible for all personnel, deliverable, and contractual issues. Our executive management team is routinely engaged in technical discussions with the client and is closely familiar with all task activities.

National Railroad Passenger Corporation (Amtrak) Network Vulnerability Assessment and Security Support	
Contact Information: Amtrak 10 G Street, N.E., Washington, DC 20002 Project POC: Ron Baklarz, CISO Phone: 202-906-4935 Fax: 202-906-4427 E-mail: BaklarR@Amtrak.com	Period of Performance: 03/2006 -Present Contract Number: 2500010055
Scope of Project: Team Elert conducted a comprehensive network wide technical vulnerability assessment that encompasses the following elements: • External penetration testing. • Internal network vulnerability scans. • PCI vulnerability assessments and penetration testing. • Mobile application security review. • Host-based scans (representative samples). • Review of firewall, IDS, and router security configuration. • Web-application testing of Amtrak's major ticketing system and credit card processing application. • Wireless Scanning. • "War dialing" to identify un-authorized/insecure modem connections among Amtrak's 5000 phone lines. • "Social engineering" of selected technical service functions. • Physical security and operations security review of a large call center and the main Data Center. Prior to embarking on this extensive effort, Team Elert prepared a Test Plan and detailed schedule. The Test Plan was submitted to Amtrak's review and was approved prior to beginning this effort. All activities are tightly coordinated with the Director of Information Security and the respective systems maintainers.	

Department of Education (ED) Office of the Inspector General (OIG) FISMA Audit Support Services (5,000 employees)	
Contact Information: ED 550 12 th Street Southwest, Washington, DC 20202 Project POC: Therese Campbell Phone: (202) 245-7367 E-mail: Therese.Campbell@ed.gov	Period of Performance: 06/2012-Present Contract Number: ED-OIG-12-A-0018
Scope of Project: Team Elert currently is a holder of an ED OIG Blanket Purchase Agreement (BPA) Task Order supporting the ED OIG. We have three full-time employees (FTE) on-site assisting in the annual FISMA audit and other cyber security tasks. We perform internal control reviews of the major categories outlined in FISMA by following strict audit standards and guidelines. We are responsible for performing the interviews and examinations to determine if controls are in place and the documentation of these results in work-papers. Additionally, Team Elert performs the vulnerability and penetration testing in support of these audits. Most recently we performed an internal/external penetration test on 2 class-B networks. This consisted of running network, host, database, web, and other scans. Team Elert also frequently advises the OIG on technical security questions and concerns.	

SECTION 2: Request for Quotation / Specifications

Please see the RFQ / Specifications on the following pages.

REQUEST FOR QUOTATION
Information Security and Network Vulnerability Assessment
WV Consolidated Public Retirement Board

SPECIFICATIONS

- 1 PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of West Virginia Consolidated Public Retirement Board to establish a contract for information security and network vulnerability assessment.

The contract will be for a two (2) year period, with the possibility of four (4) one-year renewals.

The West Virginia Consolidated Public Retirement Board (WVCPRB) is requesting quotations from information security consulting vendor for an Information Security and Network Vulnerability Assessment (Assessment). The Assessment will need to be performed at five distinct milestone points over the next four (4) years in conjunction with the new pension administration system being implemented Deloitte Consulting LLP.

The First Assessment: will be focused on the data conversion server(s). **The Second Assessment:** will be focused on the remaining installation of the development and test environments. **The Third Assessment:** will be approximately eighteen months later, and just prior to the migration to the new production environment. **The Fourth Assessment:** will be approximately one year later and just prior to the final phase deployment of member self-service features. **The Fifth and Final Assessment:** will be approximately one year after the release of the final phase, occurring during the system warranty period and prior to final handoff of the solution to WVCPRB.

The Consolidated Public Retirement Board is responsible for the administration of all State retirement plans for educational employees, public employees, deputy sheriffs, judges, and public safety personnel, with the exclusion of some higher educational plans. The plans administered include defined benefit and defined contribution retirement systems. Benefits include service retirement, disability and survivor benefits, and access to health care coverage for benefit recipients and their dependents. General administration and management of the plans by the Retirement Board is established under West Virginia law.

Current Operating Environment: CPRB employs approximately 80 people. The current computing environment includes:

- The main facility located at MacCorkle Avenue, Charleston, WV, and the current systems site located at the Capitol Complex in Charleston, West Virginia.
- Approximately 85 PC workstations Windows 7
- Windows servers
- Office 365 environment

REQUEST FOR QUOTATION
Information Security and Network Vulnerability Assessment
WV Consolidated Public Retirement Board

- Cisco Ethernet switches and fiber runs for LAN
- 10Mb connection to state backbone and rely on state's primary firewall services

Expectations: In addition, at the time of the initial assessment, the new development environment will include:

- The main facility located at MacCorkle Avenue, Charleston, WV, the production hosting site located in downtown Charleston, West Virginia, and the remote Disaster Recovery facility (hot site) located in rural West Virginia.
- VMware Server software, version 5.5

Also, at the time of the last assessment, the technical environment will also include a full production and disaster recovery site:

- The main facility located at MacCorkle Avenue, Charleston, WV, the production hosting site located at the State Capitol Complex in Charleston, West Virginia, and the remote business continuity facility (hot site) located in rural West Virginia
- Browser based Windows .Net framework, Visual Studio, version 2012
- SQL Server, version 2012, VM Ware, version 5.5, SharePoint, version 2013, MS Dynamics, version 2013
- 4 separate technical environments including Development, Test, Production, and Training/Ad Hoc environments
- Web portals for employers, staff, and participant members

2 DEFINITIONS: The terms listed below shall have the meanings assigned to them below. Additional definitions can be found in Section 2 of the General Terms and Conditions.

2.1 "Contract Services" means information security and network vulnerability assessment.

2.2 "Pricing Page" means the pages contained in wvOASIS or attached as *Exhibit "A,"* upon which the Vendor should list its proposed price for the Contract Services.

2.3 "Solicitation" means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

REQUEST FOR QUOTATION
Information Security and Network Vulnerability Assessment
WV Consolidated Public Retirement Board

- 2.4 “Common Vulnerability Scoring System” (CVSS)** is a free and open industry standard for assessing the severity of computer system security vulnerabilities.
- 2.5 Security Content Automation Protocol (SCAP)** is a method for using commonly accepted standards to enable automated vulnerability management and security policy compliance metrics.
- 2.6 “Expert”** – Vendor staff having fifteen or greater years of experience in the required services described in this RFQ. The Expert level consultant will use current information security technology disciplines and practices to ensure the confidentiality, integrity and availability of agency information assets in accordance with established standards and procedures. Provides knowledge and counsel on changing regulatory, threat, and technology landscapes to develop or maintain security policies and standards, and ensure the systems are secure. Either the Expert level or Senior Level consultant should have an OSCP (Offensive Security Certified Professional) or equivalent level of certification for Penetration Testing.
- 2.7 “Senior”** – Vendor staff having ten or more years of experience in the required services. The Senior level staff performs all procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. This role will interact with CPRB to understand the overall security needs and may require familiarity with domain structures, user authentication, and digital signatures. The Senior level vendor conducts accurate evaluation of the level of security required and must be able to weigh business needs against security concerns and articulate issues to management. Either the Expert level or Senior Level consultant should have an OSCP (Offensive Security Certified Professional) or equivalent level of certification for Penetration Testing.
- 2.8 “Specialist”** – Vendor staff having five or more years of service, with a greater depth of knowledge and experience than a technician. The Specialist level will assist the more senior level consultants in developing the deliverables in this RFQ, and will be knowledgeable on the changing regulatory, threat, and technology landscapes.
- 2.9 “Technician”** – Vendor staff having five or more years of service, possessing the basic knowledge and abilities to perform the required work. Works under the general direction of the Specialist, Senior, or Expert level consultant and performs activities that support the deliverables in this RFQ.

3 QUALIFICATIONS

REQUEST FOR QUOTATION
Information Security and Network Vulnerability Assessment
WV Consolidated Public Retirement Board

3.1 Subsequent to contract award, but prior to the start of work, all firm personnel assigned to the engagement must sign and accept a non-disclosure and confidentiality agreement. An example of the WVCPRB Confidentiality Agreement is included as *Attachment 4*.

3.2 Vendor should provide documentation of similar work performed in the successful performance of information security and network vulnerability assessments in compliance with the *National Institute of Standards and Technology Special Publication 800-37¹* please document such references on **Attachment 1**.

4 MANDATORY REQUIREMENTS:

4.1 Mandatory Contract Services Requirements and Deliverables: Contract Services must meet or exceed the mandatory requirements listed below.

4.1.1 Primary persons responsible for the engagement must have a minimum of 5 years of experience in security design and testing of Microsoft .Net, Microsoft SQL Server, and Cisco Systems Networking. As part of the solicitation response, please provide copies of professional certifications which support this requirement and provide the pertinent reference information on *Attachment 2*. Perform the Information Security and Network Vulnerability Assessment in accordance with the National Institute of Standards and Technology Standards referenced in Section 3.3.

4.1.2 Prioritize and rank the discovered vulnerabilities using the **Common Vulnerability Scoring System (CVSS)**. This will include at a minimum:

4.1.2.1 Evaluation of the security policy and procedures

4.1.2.2 A scan of external entry points into the network

4.1.2.3 A review of all of the devices on the network with static IP addresses

4.1.2.4 A review of the server, firewall, and IDS configurations

4.1.2.5 Provide Post-Assessment Remediation Services if prime contractor cannot address the identified vulnerabilities.

4.1.3 For each assessment, provide a written report, including at a minimum, the following:

¹ Reference included as Exhibit B.

REQUEST FOR QUOTATION
Information Security and Network Vulnerability Assessment
WV Consolidated Public Retirement Board

- 4.1.3.1 Executive Summary
- 4.1.3.2 Summary of Target Environment
- 4.1.3.3 Scope (including systems assessed and method used)
- 4.1.3.4 Findings (in social engineering, data loss prevention, firewall architecture and policy, and endpoint assessment)
- 4.1.3.5 Recommendations (including “quick wins” and strategic recommendations)
- 4.1.3.6 Support or cross-reference all observed deficiencies and associated recommendations to one or more of the following standards or guidelines: *National Institute of Standards and Technology Special Publication 800-53*², or *SANS Consensus Audit Guidelines*³.
- 4.1.3.7 Appendix (including evidence and screenshots).
- 4.1.4 Firewall Architecture and Policy Review
 - 4.1.4.1 Perform external automated vulnerability scanning using a vulnerability scanning solution approved by the Security Content Automation Protocol (SCAP) to identify Internet-exposed weaknesses at the network and host level.⁴
 - 4.1.4.2 Use Expert interview, paper analysis, and direct observation to identify deficiencies in firewall policy, architecture, and administration.
 - 4.1.4.3 Quantify the Internet attack surface and provide specific recommendations to reduce and manage risks from the Internet vector.
- 4.1.5 Endpoint Assessment
 - 4.1.5.1 Perform automated host-based scanning against a sample of 15 desktop and laptop systems to identify weaknesses that facilitate remote desktop compromise.

² Reference provided as Exhibit C.

³ Reference provided as Exhibit D.

⁴ Reference provided as Exhibit E.

REQUEST FOR QUOTATION
Information Security and Network Vulnerability Assessment
WV Consolidated Public Retirement Board

- 4.1.5.2 Identify ways to optimize currently deployed technologies which monitor, detect, and respond to endpoint exploit and compromise.
 - 4.1.5.3 Provide a vendor-agnostic roadmap for closing discovered endpoint gaps and aligning CPRB with endpoint security best practices within 18 months of the assessment.
 - 4.1.6 Data Loss Prevention Gap Analysis
 - 4.1.6.1 Use Expert interview, paper analysis, and direct observation to audit how CPRB exchanges confidential data with external parties, and identify weaknesses.
 - 4.1.6.2 Identify ways to optimize currently deployed technologies to monitor, detect, and respond to data loss caused by stolen or lost mobile and portable storage devices.
 - 4.1.6.3 Provide a vendor-agnostic roadmap for closing discovered gaps and aligning CPRB with data loss prevention best practices within 18 months of the assessment.
 - 4.1.7 Collaborate with the CPRB Guidance Team to develop and deliver executive presentations of the assessment and its results.
 - 4.1.8 Provide documented evidence of the performance of a vulnerability assessment and/or penetration test on a government entity or corporation that has the minimum of 5,000 employees. Evidence of this should be in the form of a list of the Vendor's clients meeting this requirement with the total number of employees for each client identified with the client name. The employee count should be the total number of employees in the entire organization (federal agency, state government, county government, corporation, etc.), including all divisions, agencies, sections, etc. and may be rounded to the nearest hundred. (For example, the State of West Virginia has approximately 30,000 employees.)
 - 4.1.9 As part of the Solicitation, provide a signed attestation and confirmation of the following on *Attachment 3*:
 - 4.1.9.1 Confirm that neither the vendor nor any of the vendor's employees, agents, independent contractors, or subcontractors have been convicted of, pled guilty to, pled nolo contendere or were named as an unindicted co-conspirator to any felony.

REQUEST FOR QUOTATION
Information Security and Network Vulnerability Assessment
WV Consolidated Public Retirement Board

- 4.1.9.2 Confirm that there is no concluded or pending litigation against the vendor or vendor employees related to a contracted engagement.
- 4.1.9.3 Identify key staffs which would be assigned to the project and affirm that those individuals are full-time employees of the vendor.
- 4.1.9.4 Verify that neither the vendor nor any officer or employee have given any remuneration or anything of value directly or indirectly to CPRB or any of its Retirement Board members, officers, employees, or contracted consultants.
- 4.1.9.5 Verify that neither the vendor, nor any officer, principal or employee have given any remuneration or anything of value as a finder's fee, cash solicitation fee, or fee for consulting, lobbying or otherwise, in connection with this Solicitation.
- 4.1.9.6 Verify that within the past five years neither the vendor, nor any officer or employee of the vendor have been a defending party in a legal proceeding before a court related to the provision of the services.
- 4.1.9.7 Verify that within the past five years neither the vendor, nor any officer or employee been the subject of a governmental regulatory agency inquiry, investigation, or charge.
- 4.1.9.8 Verify that neither the vendor, any officer of the vendor, nor any owner of a twenty percent (20%) interest or greater in the vendor has filed for bankruptcy, reorganization, a debt arrangement, moratorium, or any proceeding under any bankruptcy or insolvency law, or any dissolution or liquidation proceeding.
- 4.1.9.9 Verify that neither the vendor, nor any officer, principal or employee who shall perform work under the contract has a possible conflict of interest (e.g. employment with the State of West Virginia).
- 4.1.9.10 Verify that the vendor does not have any active managed security service provider contract(s) with any State of West Virginia agency.
- 4.1.9.11 Provide a statement of whether there are any pending Securities Exchange Commission investigations involving the Vendor, and if

REQUEST FOR QUOTATION
Information Security and Network Vulnerability Assessment
WV Consolidated Public Retirement Board

such are pending or in progress, an explanation providing relevant details and an attached opinion of counsel as to whether the pending investigation(s) will impair the Vendor's performance in a contract under this Solicitation.

5 CONTRACT AWARD:

5.1 Contract Award: The Contract is intended to provide Agency with a purchase price for the Contract Services. The Contract shall be awarded to the Vendor that provides the Contract Services meeting the required specifications for the lowest overall total cost as shown on the Pricing Pages.

Vendor's who wish to respond to a Centralized Request for Quotation (CRFQ) online may submit information through the State's wvOASIS Vendor Self Service (VSS). Vendors should download the Exhibit "A": Proposal Form/Pricing Page as well as any other required documents that are attached separately to the CRFQ and published to the VSS. Vendors must complete these forms with their prices information and other required information per the specifications and include it as attachments to their online response with an Attachment Type of "Pricing". The Pricing Page attachments (Pricing) are then downloaded buy the Buyer during the scheduled bid opening for bid evaluation.

If unable to respond online please submit the Exhibit "A" Proposal Form/Pricing Pages and all other required documentation with your bid prior to the scheduled bid opening date.

5.1.1 Evaluation will be based on Total Cost; Items one (1) through five (5), award will be for the Total Cost of the five (5) Assessments Items one through five.

5.1.2 Total for the Assessments Items 1 through 5 are Firm Fixed Price.

5.2 Pricing Page: Vendor should complete the Pricing Page Exhibit "A" by entering the Unit Coast for each of the 5 Assessments .Vendor should complete the Pricing Page/Pricing Section in full as failure to complete the Pricing Page/Section in full in its entirety may result in Vendor's bid being disqualified.

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

6 PERFORMANCE: Vendor and agency shall agree upon a schedule for performance of contract services and contract services deliverables, unless such a schedule is already included herein by agency. In the event that this contract is designated as an open-end contract, vendor shall perform in accordance with the release orders that may be issued against this contract.

REQUEST FOR QUOTATION
Information Security and Network Vulnerability Assessment
WV Consolidated Public Retirement Board

- 7 **PAYMENT:** Payments will be based upon the Agency acceptance at the completion of the deliverables described in the Mandatory Requirements Section 4 of this Request for Quotation. Each of the five periodic assessments will have an independent payment point in accordance with the payment procedures of the state of West Virginia.
- 8 **TRAVEL:** Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on vendor's bid, but such costs will not be paid by the agency separately.
- 9 **FACILITIES ACCESS:** Performance of contract services may require access cards and/or keys to gain entrance to agency's facilities. In the event that access cards and/or keys are required:
 - 9.1 Vendor must identify principal service personnel which will be issued access cards and/or keys to perform service.
 - 9.2 Vendor will be responsible for controlling cards and keys and will pay replacement fee, if the cards or keys become lost or stolen.
 - 9.3 Vendor shall notify Agency immediately of any lost, stolen, or missing card or key.
 - 9.4 Anyone performing under this Contract will be subject to Agency's security protocol and procedures.
 - 9.5 Vendor shall inform all staff of Agency's security protocol and procedures.
- 10 **VENDOR DEFAULT:**
 - 10.1 The following shall be considered a vendor default under this Contract.
 - 10.1.1 Failure to perform Contract Services in accordance with the requirements contained herein.
 - 10.1.2 Failure to comply with other specifications and requirements contained herein.
 - 10.1.3 Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.
 - 10.1.4 Failure to remedy deficient performance upon request.
 - 10.2 The following remedies shall be available to Agency upon default.

REQUEST FOR QUOTATION
Information Security and Network Vulnerability Assessment
WV Consolidated Public Retirement Board

10.2.1 Cancellation of the Contract.

10.2.2 Cancellation of one or more release orders issued under this Contract.

10.2.3 Any other remedies available in law or equity.

11 MISCELLANEOUS:

11.1 Contract Manager: During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager: Rick Anderson

Telephone Number: (651) 705-1249

Fax Number: (651) 430-2661

Email Address: rick.anderson@elert.com

SECTION 3: Attachment 1 – Vendor References

Please see Team Elert's completed Attachment 1 – Vendor References on the following page followed by complete reference write-ups.

REQUEST FOR QUOTATION

Information Security and Network Vulnerability Assessment

Attachment 1 – Vendor References

Reference No. 1	Department Health and Human Services
Name:	Steve Davis (301-443-9660)
Position:	Information Security Officer, OIT
Address:	5600 Fishers Lane, Rockville, MD 20857
Telephone Number:	Kim Lewis, 301-443-2750
Project Name:	IT Security Support
Project Description:	See pages 31 & 47 of Team Elert Response for detailed description.

Reference No. 2	National Railroad Passenger Corporation (Amtrak)
Name:	Ron Baklarz
Position:	CISO
Address:	10 G Street N.E., Washington DC 20002
Telephone Number:	202-906-4935
Project Name:	Network Vulnerability Assessment
Project Description:	See pages 32 & 48 of Team Elert Response for detailed description.

Reference No. 3	Department of Education / Office of Inspector General
Name:	Therese Campbell
Position:	Director
Address:	550 12th Street S.W., Washington DC 20202
Telephone Number:	202-245-7367
Project Name:	FISMA and IT Support Services
Project Description:	See pages 33 & 48 of Team Elert Response for detailed description.

Vendor References

Department Health and Human Services Health Resources and Services Administration (HRSA) IT Security Support	
Contact Information: Steve Davis, Chief Information Security Officer, OIT Phone: (301) 443-9660 Email: sdavis@hrsa.gov COTR: Steve Davis	Period of Performance: 2007-Present Contract Number: HSHS250200722014B Contract Type: Fixed Firm Price Contracting Point of Contact: Kimberly Lewis Phone: (301) 443-2750
Scope of Project: In November 2007, Team Elert was awarded a task order by HRSA to provide a wide range of technical assistance in conjunction with the agency's Information Security Program Plan. This included obtaining an independent assessment of HRSA's information systems; monitoring the security-related activities of these systems, and recommending changes that would enhance security across the entire spectrum of HRSA's IT infrastructure. This task was awarded competitively under a broad scope IT Security BPA issued earlier in 2007. This is a wide scope support task that covers among others the following areas: • Penetration Testing and Vulnerability Assessments • Information Systems Security Program Plan Implementation and Maintenance • IT Infrastructure Evaluation and Recommendation • Cyber Protection and Surveillance • Incident Response Support • Information Systems Security Policy Development and Implementation • Support in BTS, Departmental and OIG Initiatives • Security Awareness and Training • Risk Assessment and Compliance Management Under the guidance of the agency's CISO, our team of on-site analysts and engineers, assisted by subject matter experts based in our headquarters, has been successfully helping HRSA in a diverse range of IT security issues including: • Revamping the agency set of IT security policies and procedures. • Conducting an agency wide network inventory in order to establish an updated security baseline of knowledge about networks, systems and applications. • Evaluating the HRSA's security program against the Departmental "Secure One" initiative. • Assess and recommend Data at Rest (DAR) encryption solution. In a relatively short time, Team Elert managed to establish the confidence and trust of end users, system owners, and HRSA's network operations team. Our on-site staff and headquarters based subject matter experts proactively evaluate and recommend activities that enhance HRSA's IT Security Program performance. Consulting with and borrowing solution ideas from other Team Elert staff members on other projects help us to improve team effectiveness, reduce implementation time lines and ensures a consistent and reliable technical performance. As in all other Team Elert task orders, a senior official is directly responsible for all personnel, deliverable, and contractual issues. Our executive management team is routinely engaged in technical discussions with the client and is closely familiar with all task activities.	

National Railroad Passenger Corporation (Amtrak) Network Vulnerability Assessment and Security Support	
Contact Information: Amtrak 10 G Street, N.E., Washington, DC 20002 Project POC: Ron Baklarz, CISO Phone: 202-906-4935 Fax: 202-906-4427 E-mail: BaklarR@Amtrak.com	Period of Performance: 03/2006 -Present Contract Number: 2500010055
Scope of Project: Team Elert conducted a comprehensive network wide technical vulnerability assessment that encompasses the following elements: • External penetration testing. • Internal network vulnerability scans. • PCI vulnerability assessments and penetration testing. • Mobile application security review. • Host-based scans (representative samples). • Review of firewall, IDS, and router security configuration. • Web-application testing of Amtrak's major ticketing system and credit card processing application. • Wireless Scanning. • "War dialing" to identify un-authorized/insecure modem connections among Amtrak's 5000 phone lines. • "Social engineering" of selected technical service functions. • Physical security and operations security review of a large call center and the main Data Center. Prior to embarking on this extensive effort, Team Elert prepared a Test Plan and detailed schedule. The Test Plan was submitted to Amtrak's review and was approved prior to beginning this effort. All activities are tightly coordinated with the Director of Information Security and the respective systems maintainers.	

Department of Education (ED) Office of the Inspector General (OIG) FISMA Audit Support Services	
Contact Information: ED 550 12 th Street Southwest, Washington, DC 20202 Project POC: Therese Campbell Phone: (202) 245-7367 E-mail: Therese.Campbell@ed.gov	Period of Performance: 06/2012-Present Contract Number: ED-OIG-12-A-0018
Scope of Project: Team Elert currently is a holder of an ED OIG Blanket Purchase Agreement (BPA) Task Order supporting the ED OIG. We have three full-time employees (FTE) on-site assisting in the annual FISMA audit and other cyber security tasks. We perform internal control reviews of the major categories outlined in FISMA by following strict audit standards and guidelines. We are responsible for performing the interviews and examinations to determine if controls are in place and the documentation of these results in work-papers. Additionally, Team Elert performs the vulnerability and penetration testing in support of these audits. Most recently we performed an internal/external penetration test on 2 class-B networks. This consisted of running network, host, database, web, and other scans. Team Elert also frequently advises the OIG on technical security questions and concerns.	

SECTION 4: Attachment 2 – Vendor Primary Staff References

Please see Team Elert's completed Attachment 2 – Vendor Primary Staff References on the following page.

REQUEST FOR QUOTATION

Information Security and Network Vulnerability Assessment

Attachment 2 – Vendor Primary Staff References

Reference No. 1	Gus Fritschie
Name:	Department of Health & Human Services
Position:	CIO & Project Manager
Address:	
Telephone Number:	
Project Name:	IT Security Support
Project Description:	See attached resume and overview.
Duties Performed:	See attached references.

Reference No. 2	Rizwan Ahmed
Name:	Amtrak
Position:	Security Consultant
Address:	
Telephone Number:	
Project Name:	Network Vulnerability Assessment
Project Description:	See attached resume and overview.
Duties Performed:	See attached references.

Reference No. 3	M. Wahid Mohiuddin
Name:	Department of Education/Office of Inspector General
Position:	Security Engineer
Address:	
Telephone Number:	
Project Name:	FISMA Audit & Security Assessment
Project Description:	See attached resume and overview.
Duties Performed:	See attached references.

Gus Fritschie, CISSP, CAP, CEH

QUALIFICATION SUMMARY

Mr. Fritschie has been involved in the field of information security for over 10 years. He began his career in information technology (IT) as a system administrator for a growing financial company. It was there that he gained a fundamental understanding of all aspects of IT, including network security.

Mr. Fritschie then joined the information security consulting practices of KPMG and Deloitte & Touche. He led and performed numerous vulnerability assessments and penetration tests in support of financial audits, the Government Information Security Reform Act (GISRA – now the Federal Information Security Management Act [FISMA]), and other compliance-related efforts. Clients included Fortune 500 companies, civilian agencies, and the Department of Defense (DOD).

Since joining SeNet as a Senior Security Engineer, Mr. Fritschie has led several large-scale projects. Some projects included enterprise-wide vulnerability assessments for multiple government and commercial clients, management of Certification and Accreditation (C&A) efforts, and Web application penetration tests. He currently serves as SeNet's Director of Engineering and Security Assessments. As such, he is responsible for all technical deliverables and projects for the company.

Mr. Fritschie has proven work performance with organizations and clients such as the Department of Health and Human Services (HHS), Department of Agriculture (USDA), Department of Labor (DOL), Department of the Interior (DOI), Government Printing Office (GPO), and Amtrak.

SKILLS

- Program and Project Management
- Enterprise Security Architecture (ESA)
- **Secure Configurations:** National Institute of Standards and Technology (NIST) checklists, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and Center for Internet Security (CIS) benchmarks for applications, networks, and database platforms
- **Networking:** Transmission Control Protocol (TCP)/Internet Protocol (IP), firewalls, Virtual Private Network (VPNs), and Cisco routers and switches
- **Operating Systems:** Microsoft Windows 2008/2003/2000/NT/Vista/XP, RedHat, UNIX, IBM AIX and z/OS Mainframe
- **Security Tools:** Nessus, Nikto, ISS Internet Scanner, Metasploit, Nmap, L0phtcrack, SARA, Wireshark, Aircrack-ng, Kismet, DISA Security Readiness Review (SRR) Scripts, WebInspect, AppScan, AppDetective, and Snort
- **Desktop Applications:** Microsoft Office Suite – Outlook, Visio, and Project
- **Certification and Accreditation:** Implementing certification and accreditation (C&A) activities of information systems, and performing security assessments and production of C&A documentation, including:
 - System Categorization (FIPS 199)
 - Privacy Impact Assessment (PIA)
 - Privacy Threshold Analysis (PTA)
 - Configuration Management Plan (CMP)
 - Information Technology Contingency Plan (ITCP)
 - Information Technology Disaster Recovery Plan (ITDRP)
 - System Security Plan (SSP)
 - Security Assessment Report (SAR)
 - Risk Assessment (RA)

- Security Controls Compliance Matrix (SCCM)
- Plan of Action and Milestones (POA&M)

PROFESSIONAL EXPERIENCE AND ACCOMPLISHMENTS

SeNet International Corporation, Fairfax, VA

2003 to Present

Chief Technology Officer

Mr. Fritschie manages and leads security teams performing vulnerability assessments for government and commercial agencies. The assessments involve performing wireless, network, and mainframe vulnerability and penetration testing. Mr. Fritschie performs C&A testing and conducts testing on Web applications during the development, pre-production, and production phases. Mr. Fritschie develops vulnerability/penetration testing methodologies. He conducts security reviews and risk assessments using Federal guidelines set forth in the Federal Information System Controls Audit Manual (FISCAM), Federal Information Processing Standard (FIPS) publications, Office of Management and Budget (OMB) guidelines (127 and 130), and FISMA.

Health Resources and Services Administration (HRSA)

In addition to serving as the project manager for a five-person SeNet Team at HRSA, Mr. Fritschie has performed a variety of technical tasks. He led the C&A efforts for HRSA's general support system (GSS) and over six other major applications (MAs). Mr. Fritschie architected and engineered a security architecture review and presented the results to the Chief Information Officer (CIO) and Chief Information Security Officer (CISO). He was also responsible for the oversight and final delivery of a penetration test that SeNet performed for HRSA. Mr. Fritschie is often asked by HRSA's CISO for guidance and advice on a variety of security topics.

Bureau of Indian Affairs (BIA)

For BIA, Mr. Fritschie performed multiple roles: security team lead, security engineer, and he had responsibilities at the program level. As the security team lead, Mr. Fritschie was a subject matter expert (SME) who provided C&A life cycle support and consulting services. He developed detailed security test and evaluation (ST&E) plans for BIA systems. He led the C&A process for BIA MAs and GSSs throughout the system development life cycle (SDLC). He developed the C&A schedule and lead client meetings. He developed detailed System Security Plans (SSPs) utilizing NIST Special Publication (SP) 800-53 security controls. He conducted interviews with key stakeholders and validated and audited existing security control assessments (SCAs) of existing MAs and GSSs. He developed ST&E Plans for MAs and GSSs. He was responsible for managing a team of eight security engineers and analysts.

Amtrak

Mr. Fritschie's experience with Amtrak goes back to 2000 when he worked for KPMG and was a member of the team that performed one of the first penetration tests on Amtrak's network. Because of his past experience at Amtrak, SeNet was awarded an enterprise vulnerability assessment contract in 2006, which Mr. Fritschie led and managed. Due to the success of SeNet's and Mr. Fritschie's work, SeNet was awarded an additional three-year contract to perform security assessments. This project involved the following tasks:

- Database Security Review
- External and Internal Vulnerability Assessment
- Web Application and Wireless Assessment
- Software Control and Data Acquisition (SCADA) Assessment
- Router/Switch and Firewall Assessment

Mr. Fritschie was responsible for the quality and content of the final report, and briefed the CIO and his executive staff on the results and recommendations. Amtrak's CISO views Mr. Fritschie's opinions and thoughts on InfoSec as valuable and often reaches out to him for advice.

National Finance Center (NFC)

For this large client, Mr. Fritschie has performed a variety of tasks both in the Washington DC area and at NFC headquarters in New Orleans. Mr. Fritschie and his team provided technical support during numerous C&As of NFC systems.

Mr. Fritschie also led a “least functionality assessment,” which was initiated by the NFC CIO in response to an Office of the Inspector General (OIG) audit. This task involved reviewing a number of settings across NFC’s environment to verify that they were in compliance with CM-7 from NIST SP 800-53. A series of least functionality baselines were created, and then scans were conducted and analyses performed to see whether the settings were in compliance. Mr. Fritschie also led a firewall assessment team to evaluate the security posture of these devices.

Occupational Safety and Health Administration (OSHA)

Mr. Fritschie performed numerous ST&Es on OSHA’s systems at the request of the OIG. These tests were technical in nature and focused on identifying security vulnerabilities at the operating system, database, and application levels. He noted findings in an ST&E report and made specific recommendations on how to mitigate the findings.

Mr. Fritschie also provided OSHA with network operations support. He served as SeNet security team lead and managed three security engineers/analysts. Responsibilities included:

- Managing the security team projects and personnel
- Managing the firewall and Intrusion Detection System (IDS)
- Managing antivirus and patch management systems
- Performing security assessments of the OSHANET and compliance testing
- Evaluating/recommending security enhancements for the OSHANET to Directorate of Information Technology (DIT) management
- Interfacing with security vendors on behalf of DIT management
- Attending vendor-sponsored security events
- Providing daily/weekly status of daily operations and ongoing projects to management
- Attending regularly scheduled team meetings, active directory (AD) meetings, and weekly meetings with management

United States Department of Agriculture (USDA)

In addition to his support for NFC, Mr. Fritschie has provided security testing expertise to the USDA to support the C&A process for a number of USDA components, such as:

- Animal and Plant Health Inspection Service (APHIS)
- Departmental Administration (DA)
- Office of the Chief Information Officer (OCIO)
- Agricultural Marketing Service (AMS)
- OIG

He created and oversaw the majority of testing that Team Elert performed and was responsible for the quality and results documented in the Security Assessment Report (SAR). He also performed risk assessments and created and assisted in Plan of Actions and Milestones (POA&M) development. The C&A documentation followed USDA templates and standards, and was completed in Cyber Security Assessment and Management (CSAM).

Government Printing Office (GPO)

Mr. Fritschie conducted a vulnerability assessment for the GPO. The scope of this task followed established Government guidelines (e.g., OMB A-130 Appendix III, NIST SP 800-26 *Self Assessment Guide for Information Technology Systems*, NIST SP 800-30 *Risk Management Guide*, CIO Council *Federal Information Technology Security Assessment Framework*), and covered the following components:

- Internal network infrastructure components – routers, hubs, and switches
- Internal network support servers – Domain Name System (DNS), e-mail, management, and security
- Internal IT resources – file and print servers, and database servers
- Database and intranet applications
- Mainframe access control measures

Deloitte & Touché Information Security Services, McLean, VA**2002 to 2003****Senior Security Consultant**

- Performed network security reviews that focused on internal and external penetration testing, including war-dialing and network architectural assessments.
- Managed Web application testing and security assessments using a variety of tools and methods.
- Performed a review of a major health care provider to test compliance with a Health Insurance Portability and Accountability Act (HIPAA) security rule. This involved assessing the current security state and determining the controls that needed to be in place to adhere to the standards and implementation specifications detailed in the HIPAA security rule. Performed a gap analysis and delivered recommendations to the client.
- Lead technical member of an audit of a major governmental organization. Focus areas included wireless security, NT and UNIX security, IDS, and VPN architectures.
- Assisted in the development and creation of proposals.

KPMG Risk and Advisory Services, Washington, DC**2000 to 2002****Senior Security Consultant**

- Provided internal and external penetration tests/vulnerability assessments for a number of Fortune 500 companies and government agencies.
- Formulated work papers (specific to the OIG) as a result of internal and external government penetration engagements. Delivered reports and presentations related to these engagements.
- Provided C&A for secure systems, enterprise security architecture, risk and vulnerability assessments, and security policy and procedures development.
- Participated in and led “tiger team” penetration attacks to test computer security. These attacks were designed to determine the level of risk from internal and external threats to information systems owned by government and private sector organizations. Targets of the attacks included mainframe computers, local area networks (LANs), wide area networks (WANs), distributed client/server computers, dial-up communication lines, and Internet connections.
- Created audit work plans on UNIX and Windows firewalls, routers, and Web servers for a government financial organization to be used by bank examiners across the country.
- Developed and instructed a course on network security for various KPMG LLP clients. It included network security policies, tools, and techniques used in performing network vulnerability testing.
- Performed firewall assessment reviews on a variety of platforms, including Check Point and Cisco PIX.
- Conducted security reviews and risk assessments using Federal guidelines set forth by the FISCAM, FIPS PUBs, OMB guidelines (127 and 130), GISRA, as well as the DOD Trusted Computer System Criteria. Also performed reviews related to HIPAA compliance.
- Assisted in designing a network architecture for an international banking organization.

- Implemented a solution that allowed customers and employees to securely access a company's intranet and extranet. This was accomplished with a reverse proxy server using Secure Socket Layer (SSL) and Light Directory Access Protocol (LDAP) for authentication.
- Assisted in the architectural/security review of a governmental organization's Directory Service implementation. The implementation involved Netscape Directory Server along with the use of iPlanet Directory Access Routers (iDARs). Developed and executed a test plan to ensure that controls were in place to mitigate the risks.
- Performed wireless security reviews and provided guidance regarding implementations related to the 802.11b protocol.

EDUCATION

B.A., Geography, Mary Washington College

CERTIFICATIONS AND TRAINING

- Certified Information Systems Security Professional, 2002
- Certification and Accreditation Professional, 2007
- NSA INFOSEC Assessment Methodology, 2006
- CompTIA Security+, 2007
- Solaris Certified Security Administrator, 2003
- System Administration in INFOSEC, NSTI No. 4013, 2004
- Certified Cisco Network Administrator, 2002
- Cisco Secure PIX Firewall Administrator, 2003
- Check Point Certified Systems Engineer, 2002
- Check Point Certified Security Administrator, 2002
- Microsoft Certified Systems Engineer, 2000
- Certified Ethical Hacker, 2010

CLEARANCES

OPM Public Trust

Rizwan Ahmed, SECURITY+, CEH, MCSE

QUALIFICATION SUMMARY

Ten plus years' experience in the computer field maintaining various desktop support disciplines concerning LAN/WAN environment. Ensuring the integrity and protection of networks, systems, and applications by technical enforcement of organizational security policies through monitoring of vulnerability scanning devices. Detect intrusions on the networks using Arc Sight and RSA Net witness. Analyze network traffic and IDS alerts to assess, prioritize and differentiate between potential intrusion attempts and false alarms. Vulnerability scans and penetration testing performed on commercial and Federal networks.

SKILLS

- **Security Tools:** FireEye, RedSeal, Netwitness, Arc Sight ESM & Logger, SMS Tipping Point, Tenable Security Center, Symantec Risk Automation Suite, Wireshark, Alien Vault, Secure Fusion, NetIQ, Snort, Security Onion, IBM Tivoli Endpoint (TEM)
- **Forensics Tools:** Guidance Encase Enterprises, AccessData FTK (Forensics Toolkit), Kali Linux, SANs SIFT Workstation
- **Penetration Testing Tools:** Metasploit, Core Impact, Nessus, Nmap, IBM Security AppScan, Burp Suite
- **Encryption Tools:** Pointsec, Bitlocker, PGP, Guardian Edge, Safend & Dell Credant Encryption
- **Operating Systems:** Windows 8/7/Vista/XP/2000 Professional & Enterprise, Microsoft Windows NT/2000/2003/2008 Server, Macintosh OS9 and OSX, Linux & Ubuntu all Distribution
- **Software Packages:** Microsoft Office XP/2003/2007/2010, Symantec Ghost, NetBotz Advanced View, Secure ZIP
- **Enterprise Tools:** Lumension Patch Management, MacAfee ePolicy Orchestrator, Symantec Endpoint protection Manager, BellArc, LANDesk, SharePoint
- **Ticketing Systems:** HHS Risk vision, Service Now

PROFESSIONAL EXPERIENCE AND ACCOMPLISHMENTS

Senet International Information Security Analyst/Engineer

September 2009 to Present

Iowa Lottery

Performed a security architecture review. This involved both internal and external vulnerability scans, firewall testing, and analysis of their network. The finished product was a report that outlined vulnerabilities and recommendations for the customer to mitigate those findings.

Health Resources and Services Administration (HRSa)

Performed the following services as a Network Security Analyst:

- Provided contracting services at HSRA in Rockville, MD.
- Responsible for hardware and software applications to secure baseline configuration using Bell arc and LANDesk.
- Used tenable security center to scan Windows & Linux operating system using the DISA STIGs audit polices.
- Responsible for software application scanning using IBM app Scan and also involved in application SDLC process.
- In addition to application scans using IBM App Scan, provided detailed vulnerability and remediation report.
- Responsible for daily monitoring of Arc sight for the enterprise log management.
- Responsible for daily monitoring of RSA Net witness application.

- Responsible for Incident response calls, involved in forensics processing as directed HR or when malware found in the network.
- Responsible for Monthly Security Dashboard for CISO & CIO.
- Responsible for handling Malware detected over the network. Analyzed threat and submitted report to the Branch chief for further action and remediation.
- Responsible for the daily monitoring of Tipping Point IDS/IPS.
- Responsible for Security Applications & Servers for any new updates and troubleshooting.
- Responsible for Penn testing of internal and external s web site and applications for the agency.
- Responsible for Vulnerability Scans of the network on a weekly and monthly basis using Tenable Security Center.
- Asset Management Documented any newly discovered IPs on the network and add those IPs to the Tenable Security Center Repository.
- Managed CSIRC Ticketing system "Risk Vision" in support of incident reporting.
- Managed agency ticketing system "Service Now" in support incident reporting.
- HRSA SME for Nessus Scanner and Tenable Security Center use and deployment.
- Supported Forensics process with Encase, FTK & SIFT Workstation solutions.
- Responsible for Threat Monitoring using Fire Eye & Tipping Point.
- Managed Tipping Point, Arc Sight, Net witness, Tenable Security Center, IBM AppScan and HRSA SOC mailbox.
- Set up the test lab environment for upcoming security scanners and applications.
- Responsible for maintaining the test lab.
- Successfully tested and deployed the Safend encryption and port control software successfully deployed and managed PGP Full Disk Encryption to over 2500 desktops.
- Managed and troubleshoot Facebook laptops for HRSA.
- Helps the risk assessment team with general support system (GSS) and major application (MA) certification and accreditation activities.
- Successfully tested enterprise products like Splunk, Guardian Edge, Alien Vault, and Pointsec.
- Worked with Guardian Edge Hard drive encryption, PGP, Encase and Arc Sight testing.

Management Systems Services, Inc.**December 2007 to September 2009****Senior Desktop Support***Health Resources and Services Administration (HRSA)*

Performed the following services as Senior Desktop Support:

- Provided contracting services at HSRA Federal Government, Rockville, MD.
- Was responsible for technical support for 1000+ users in Microsoft Windows environments.
- Managed all aspects of hardware and software, including installation, configuration, and maintenance.
- Upgraded/migrated PC hardware and operating systems.
- Provided one-on-one training to users for a new system.
- Provide basic hardware support by maintaining the network and computer equipment. This included simple fault diagnosis on the LAN and workstation, and control of day-to-day network operations.
- Implemented Norton Ghosting Solution for fast recovery (creating image files, etc.).

Raysat US, Tyson's Corner, VA**February 2005 to December 2007****Senior Support Engineer**

Performed the following services as Senior Support Engineer:

- Maintained and supported enterprise TCP/IP heterogeneous data network composed of MS Windows/Mac.
- Provided support for hardware- and software-related issues.
- Performed end-to-end connectivity and network troubleshooting.
- Performed day-to-day Windows 2000/NT administration such as user accounts, logon scripts, e-mail accounts, directory services, file system shares, and permissions.
- Responsible for vendor management and procurement of LAN/WAN hardware and upgrades.

- Trained employees in network procedures as well as in the use of hardware and software.
- Implemented Norton Ghosting Solution for fast recovery (creating image files, etc.).
- Applied patches and upgrades for existing servers and applications.
- Troubleshoot VPN for remote access.
- Installed network cards, high-speed cable modems, and HP printer support.
- Programmed batch files to facilitate ease of use to new computer user.

Computer Zone, Springfield, VA**April 2002 to February 2005****Desktop Support/Help Desk**

Performed the following services as Desktop Support/Help Desk:

- Installed, configured, and troubleshoot workstations and servers. Provided basic hardware support by maintaining the network and computer equipment. This included simple fault diagnosis on the LAN and workstation, and control of day-to-day network operations. Coordinated others doing installation and troubleshooting.
- Installed and configured Cisco routers, switches, and hubs. Configured switches and hubs on Cisco routers using Microsoft Windows 2000 Server and Windows NT 4.0 Server as the operating system.
- Monitored the event viewer in Windows NT 4.0 Server for any critical errors.
- Configured TCP/IP in Windows 2000, Windows NT, and Windows 95.
- Installed network printers using a common print solution and also set up network printers in a heterogeneous environment of Windows NT, Windows 95, and Windows 2000 Professional.
- Performed hands-on installation and troubleshooting of Pentium II/III/IV-level PCs.

Career Technology, Falls Church, VA**January 2001 to March 2003****Desktop Support/Helpdesk**

Performed the following services as Desktop Support/Help Desk:

- Designed and implemented local area networks (LANs) and wide area networks (WANs) according to client requirements evaluated after thorough study of floor maps and traffic-load calculations.
- Managed structured cable installation.
- Installed and configured a Windows 2000 Server on a LAN.
- Proposed the required equipment for the best performance.
- Installed network equipment such as hubs, switches, and routers.
- Configured server and workstation operating systems.
- Configured DNS, DHCP, and WINS services.
- Provided troubleshooting support and reconfiguration of corporate customers' LANs, primarily based on Windows NT operating systems.
- Performed migration from Windows NT 4.0 Domain to Windows 2000 (Active Directory). Maintained and supported Active Directory Services using Group Policy.

HSBC Bank, Karachi, Pakistan**February 2002 to November 2000****Desktop Support/Helpdesk****EDUCATION**

B.S., Commerce (Karachi University, Pakistan 2011)

B.S. Network Security (Strayer University, 2013)

CERTIFICATIONS AND TRAINING

- Complete hands-on Windows 7 & 8, Windows XP Professional, and Windows Vista
- MCSE 4.0, 2000, 2003 (Microsoft Certified Systems Engineer)
- A+ Certified Training
- MCDST Microsoft Certified Desktop Support Technician
- Dell Certified Technician
- CompTIA Security +
- CEH (Certified Ethical Hacker)

M. Wahid Mohiuddin, CEH, CICP, MCTS, CompTIA Security+

QUALIFICATION SUMMARY

Mr. Mohiuddin is an experienced security engineer with a thorough understanding of Information Assurance (IA) and Certification and Accreditation (C&A) processes. He has over seven years of IT experience with five years in network administration and two years in Information Security. He is an effective team player able to foster excellent relationships with team members, management, and clients. Mr. Mohiuddin has extensive experience in information system security design, implementation, and continuous monitoring to ensure confidentiality, availability, integrity, as well as efficient system performance. In addition to outstanding process and decision-making skills, he also possesses excellent communication and interpersonal skills and is able to easily communicate security-related concepts to both technical and non-technical staff. His additional qualifications include design, installation, management, and troubleshooting telecommunication systems and network software and hardware, maximizing the end-user experience while prioritizing IT security and information system efficiency.

Specifically, he has:

- Strong knowledge and experience with performing information security systems vulnerability testing, analysis and responses, as well as management reporting.
- Experience with performing penetration testing on entire network infrastructures inclusive of network boundaries, databases, applications, local area network (LAN) computers, and LAN/wide-area network (WAN) servers.
- Detailed knowledge of security tools, National Institute of Standards and Technology (NIST) standards, technologies, and industry best practices.
- Extensive knowledge of computer security procedures and protocol, and expert knowledge of federal copyright laws.
- Proven proficiency in the analysis, design, implementation, testing, and monitoring of network media, devices, and the entire network infrastructure while ensuring confidentiality, availability, and integrity of the information systems and business processes.
- Strong knowledge of information security concepts in relation to attack patterns, intrusion detection, firewalls, demilitarized zones (DMZs), administrative policies, backup, recovery, computer forensics, and common vulnerabilities.
- Experience with performing architectural design, implementation, and administration for in MS SharePoint technologies while ensuring the confidentiality, availability, and integrity of data.
- Extensive experience in the field of desktop support, local area network (LAN) administration, and help desk support.
- Excellent communication skills, interpersonal skills, technical documentation skills, and negotiation skills.

SKILLS

- **Security Technologies:** SonicWALL, eEye Retina, Snort, Wireshark, SolarWinds, AppsecInc AppDetective, IBM Rational Appscan, HP WebInspect, Nmap, Nessus, Nikto, Burp Proxy, Metasploit, IP Scanner, Kismet, Aircrack-ng, Backtrack/Kali penetration testing tools, Anti-virus tools (Norton, Symantec, McAfee, Ghost, etc.), Veritas NetBackup
- **Operating Platforms:** UNIX-based systems (Solaris, Linux) and Windows (all flavors), MAC, IBM WebSphere
- **Hardware:** HP Proliant GL-series servers, SonicWALL NSA 2400/4500, Cisco Catalyst 2960 switches, Dell and HP workstations/laptops
- **Languages:** C++, .NET, MySQL, Visual Basic
- **Client Scripting:** HTML, JScript, VBScript

- **Protocols:** TCP/IP, UDP, SNMP, LDAP, IPSec, FTP, SMTP, SSL
- **Services:** DHCP, WINS, DNS, SSH, VPN, VLAN, Terminal Services, Active Directory, IIS
- **Software Packages:** MS Office 2013, Microsoft Visio 2013, Microsoft Project
- **Tools:** Microsoft SharePoint, MS Office 2013, Microsoft Visio 2013, Adobe Professional Suite, Microsoft Project, Visual SourceSafe, Active Directory
- **Certifications:** CEH, CICP, CompTIA Security+, CCNA, MCP, MCTS

PROFESSIONAL EXPERIENCE AND ACCOMPLISHMENTS

SeNet International, Inc., Fairfax, VA
Information Security Engineer

June 2011 – Present

Mr. Mohiuddin performs vulnerability assessments and penetration tests using tools such as HP WebInspect, AppDetective, Nessus, Nikto, and Threat Vulnerability Assessment (TVA) matrix table development confirming to NIST and FISMA standards for government and commercial agencies. These assessments involve wireless, network, and mainframe vulnerability and penetration testing. He deploys open source and proprietary software and tools to perform the penetration testing for multiple environments, including but not limited to Windows, UNIX, Linux, mainframe, database, and Web application architectures. He assists in certification and accreditation (C&A) testing.

His tasks further include:

- Preparation of security test plans, external reconnaissance analyses, and presentation of reports on security vulnerabilities.
- Performing security risk assessments and conducting security briefings on sensitive cyber security matters.
- Performing database vulnerability assessment utilizing AppDetective on commercial and government database in compliance with CIS and FISMA standards. Database flavors included various versions of DB2, SQL Server, and Oracle.
- Configuring the technical aspects of cyber security to meet the appropriate standards and compliance requirements.
- Defining firewall, intrusion detection systems (IDS), intrusion prevention systems (IPS) policies and their implementation plans.
- Enforcing strong authentication and strict VPN policies employing a combination of IPSec and SSL security controls to prevent unauthorized access to the internal network.
- Reviewing IT audit logs to detect malicious activities.
- Assisting with Certification and Accreditation (C&A) testing.
- Drafting the patch management policy using NIST SP 800-40 guideline (*Procedure for Handling Security Patches*). Periodically executed vulnerability assessment scans using automated tools (Nessus, Nmap, Nikto, etc.) to ensure compliance of information system resources with the organization's technical security standard manual (TSSM).
- Configuration and management of Snort- a network based IDS solution, for perimeter and host intrusion detection system on critical servers.
- Managing cyber security awareness programs and activities while advising resource owners on the formation of appropriate security policies.
- Design and implementation a centralized patch management solution for corporate desktops and servers.
- Design and implementation of Windows 7 desktop security policy using Group Policy Object (GPO).
- Preparing security-related awareness and training materials, and conducting drills and seminars.
- Drafting the Business Continuity Plan and Disaster Recovery Policy in accordance with security policy and management guidelines.
- Interacting with users and responding to security incidents in coordination with the Information Security Officer (ISO) as a member of the corporate security team.

Systems Administrator**June 2011 – July 2012**

- Installation and management of CISCO ASA Firewall by setting up access rules, enforcing content filtering policies, NAT policies and ensure secure network traffic. Applied both inbound and outbound access lists on corporate firewall as well as static, conduit statements and created NAT pools for private IP addresses.
- Installation and management of Active Directory policies on Windows Server 2008 based servers thereby enforcing organizational policies based on user roles and responsibilities based on Access Control Lists.
- Configuration and administration of DNS BIND.
- Migration of Microsoft Exchange Server 2010 with Mobile Integration Services and Windows Server Updates Services (WSUS). Setup and administration of corporate mail relay services using postfix, postgrey on Debian systems.
- Installation, configuration and administration of SharePoint 2010 Professional Content Management System and corporate project management portal.
- Setup and administration of corporate website employing WordPress technology.
- Administration of corporate technology infrastructure which included a combination of UNIX, VMWare, Windows based servers and workstations.
- Successful organization wide migration from Windows XP to Windows 7 on all corporate hardware.
- Administration and organization wide implementation of strict antivirus, and IPS policies utilizing Symantec Endpoint Protection (SEP).
- Archiving backup data using Symantec Backup Exec in coordination with batch file scripting to generate automated backups periodically. Executed quarterly recovery tests.
- Inventory management of all corporate IT assets, purchased software licensing, and tracked licensing compliance.
- Auditing user password in compliance with the organization's password complexity requirements.
- System/network documentation, standard operating procedures (SOPs), and implementing corporate IT policies.
- Resolution of hardware, software and system issues. Analyze performance of the system and ensure the performance objective and availability of the requirements.
- Maintaining corporate network security policy, addressing server security issues, and timely application of appropriate security patches and upgrades.

AHCC, Rockville, MD**July 2008 – May 2011****Network Administrator**

At AHCC, Mr. Mohiuddin performed the following functions:

- Installed and maintained security infrastructure, including IPS, IDS, log management, and security assessment systems. Assess threats, risks, and vulnerabilities from emerging security issues.
- Conducted technical risk evaluation of hardware, software, and installed systems and networks. Assisted with testing of installed systems to ensure protection strategies are properly implemented and working as intended.
- Configured and managed Blackberry Enterprise Server (BES).
- Established a strong network architecture by implementing a highly defensive DMZ, employing several state-of-the art authentication mechanisms and security measures.
- Hardened firewall access rules by analyzing network traffic based on Snort® packet capture logs and Sonicwall® Intrusion Detection logs.
- Installed and configured Microsoft Exchange Server 2003 including email routing and setup, security policies, monitoring and maintenance.
- Managed phone system based on IP telephony (VoIP), and LAN based peer-to-peer call establishment.

- Responsible towards development and implementation of organizational security policy to cover all aspects of confidentiality, integrity and availability.
- Responsible towards all software and hardware upgrades, patches implementation, infrastructure related research and development.

St Joseph Mercy Hospital, Auburn Hills, MI
Infrastructure Support Specialist

January 2008 – July 2008

Mr. Mohiuddin performed the following functions:

- Installed, maintained, and troubleshot new server hardware and software infrastructure, network connectivity problems, and day-to-day operations.
- Supported a network of over 2,000 NT and 1000 Windows nodes, and over 200 NT servers.
- Conducted technical research on system upgrades to determine feasibility, cost, and compatibility with current infrastructure.
- Troubleshot and resolved hardware, software, and connectivity problems, including user access and component configuration.
- Worked with system and network engineers to reset and troubleshoot servers, routers, and switches.
- Interacted with clients to resolve basic help desk issues in a timely, professional manner.
- Analyzed Intrusion Detection and Ethereal logs to detect any network vulnerabilities or misuse.
- Analyzed and monitored network performance. Diagnosed and corrected problems in current networking topology.
- Implemented TCP/IP and related services such as DHCP/DNS/WINS.
- Tested gateways and firewalls using ping and tracert to troubleshoot packet loss and connectivity issues, and NAT translation.
- Installed CAT5 cables for T1 circuits, 250-ft.+ cable runs, line testing, and synchronization as well as analyzed existing cable layout.
- Analyzed performance of multicast traffic and the behavior of DHCP over cable network using Wireshark.
- Created and maintained Windows 2000 and XP ghost images as a method to reduce time and improve the efficiency of future system setups and rebuilds.

EDUCATION

M.B.A., Loyola University, Baltimore, MD (expected graduation July 2016)

B.S. Information Technology, Baker College, Auburn Hills, MI

Associate's Degree in General Sciences, Oakland Community College, Royal Oak, MI

CERTIFICATIONS

- Certified Ethical Hacker (CEH)
- Core Impact Certified Professional (CICP)
- CompTIA Security+, and Network+
- Cisco Certified Network Associate (CCNA)
- Microsoft Certified Technology Specialist (MCTS)
- Microsoft Certified Professional (MCP)

Rehan Bashir, CISSP, CAP, MCSE

QUALIFICATION SUMMARY

Mr. Bashir is an Information Security Analyst with extensive training in certification and accreditation (C&A) and information technology (IT).

SKILLS

- **Secure Configurations:** National Institute of Standards and Technology (NIST) checklists, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and Center for Internet Security (CIS) benchmarks for applications, networks, and database platforms
- **Security Tools:** Check Point Firewall, Snort IDS, Trend Micro Enterprise Security Solutions, Big Fix Patch Management, SecEdit, HFNetChk Pro, Nessus Vulnerability Scanner, Nmap, Nikto Web Security Scanner; Dsniff; Ethereal; NetIQ Security Manager, Juniper Netscreen Secure Sockets Layer (SSL) Virtual Private Network (VPN); ISS Internet Security Scanner; WebSense Content Filtering; Attack Toolkit; Paros Proxy Web application scanner; Network Security Toolkit (NST), Cyber Security Assessment and Management (CSAM)
- **Databases and Operating Systems:** MS Windows 2007/2003/2000/NT/XP
- **Desktop Applications:** Microsoft Office Suite – Word, Outlook, Excel, Visio, and Project

PROFESSIONAL EXPERIENCE AND ACCOMPLISHMENTS

SeNet International Corporation, Fairfax, VA
Senior Security Engineer

2006 to Present

Bureau of Indian Affairs (BIA) – Department of the Interior (DOI)

Mr. Bashir performs C&A on BIA major applications (MAs) and general support systems (GSSs) in accordance with NIST Special Publication (SP) 800-37. He conducts Internal Control Reviews (ICRs) on BIA's MAs and GSSs to meet the annual self-security assessment requirement mandated by Federal Information Security Management Act (FISMA) of 2002. He also supports the Office of Information and Privacy (OIP) by providing responses to the department's Office of the Chief Information Officer (OCIO) date-sensitive data calls. He performs technical vulnerability assessments (TVAs) using Nessus, Nmap, Microsoft Baseline Security Analyzer (MBSA), and more on MAs and GSSs, and analyzes and documents the results in security test and evaluation (ST&E) reports.

Mr. Bashir also performs security control testing on BIA systems using NIST SP 800-53 guidelines. He updates the existing System Security Plans (SSPs) based on NIST SP 800-18. He reviews current documented security policies and procedures, and updates the risk assessment (RA) in accordance with NIST SP 800-30. He assesses and determines the security categorization of systems based on Federal Information Processing Standard (FIPS) 199 and NIST SP 800-60. In addition, he assists the Active Directory (AD) team for AD security implementation.

DataWiz Corporation, Chantilly, VA
Information Security Analyst

2003 - 2006

Mine Safety and Health Administration (MSHA) – Department of Labor (DOL)

Working as an information security analyst in direct support of the Information Security Officer (ISO) at MSHA, Mr. Bashir was actively involved in designing the security policy, configuration, and implementation of a Windows 2003 AD migration project.

His duties included the following:

- Prepared C&A packages for both MAs and GSSs.
- Performed system categorization using FIPS 199 and NIST SP 800-60, testing of security controls as defined in NIST SP 800-53, and produced SSPs adhering to NIST SP 800-18.

- Developed and updated the SSP, Disaster Recovery Plan (DRP) and Contingency Plan (CP). Executed the Security Control Assessments (SCAs) on MSHA MAs and GSSs.
- Participated in client interviews as part of the RA, system categorization, and SCA.
- Drafted the technical, management, and operational security policies for MSHA in compliance with FISMA requirements.
- Conducted the table-top exercise to test and verify the CPs, and updated the plans accordingly.
- As part of day-to-day operations, coordinated with OCIO to meet the department's annual security tasks.
- Coordinated with the system owner to mitigate or remove identified weaknesses in the Plans of Actions and Milestones (POA&Ms) and submitted them to OCIO for review on a quarterly basis.
- Generated security alerts to users and technical staff as published by the United States Computer Emergency Readiness Team (US-CERT), the SysAdmin, Audit, Network, Security Institute (SANS), and other security vendors.
- Coordinated the MSHA security audits with the Office of Inspector General (OIG), prepared responses to OIG audit reports once the identified weaknesses were mitigated, and reported back to OIG.
- Performed an RA on a MSHA E-Gov System by using open source Web application testing tools (Paros, Nmap, and WebScarab).
- Updated the incident response and reporting manual.
- Coordinated the implementation and verification of security controls as specified in NIST SP 800-53.
- Coordinated the effort of MSHA's employees security awareness training program

Occupational Safety and Health Administration (OSHA) – DOL

As information security engineer, Mr. Bashir was responsible for administering and managing the agency's firewall. He created and modified the security policies for the firewall as needed and reviewed firewall logs on daily basis. His duties also included the following:

- Administered the agency-wide antivirus solution (Trend Micro).
- Designed and implemented the Windows XP desktop security policy using Group Policy Object (GPO).
- Implemented the hardware and software inventory software on all desktops and servers.
- Designed and implemented the centralized patch management solution for 2,500 desktops and servers.
- Drafted the patch management policy using NIST SP 800-40 guideline (Procedure for Handling Security Patches). Periodically executed vulnerability assessment scans using automated tools (Nessus, N-Stealth, Nikto, etc.) to check the compliance of information system resources with the agency's technical security standard manual (TSSM).
- Audited the user's passwords in compliance with the agency's password complexity requirements.
- Tested the agency's in-house developed business application for security controls.
- Configured the network intrusion detection, Snort, for perimeter and host intrusion detection system (NetIQ security manager) on critical servers.
- As a member of the OSHA's security team, interacted with users and responded to the security incidents in coordination with Information Security Officer (ISO).

NetSol USA, Vienna, VA

2001 - 2003

Systems Network Engineer

Mr. Bashir maintained the availability of company computer resources, including servers, workstations, laptops, printers, and multimedia equipment. Mr. Bashir also performed the following:

- Administered multi-server Windows 2000 local area network (LAN), workstations, and end-users.
- Recommended, evaluated, and purchased IT assets.
- Maintained inventory of IT assets, purchased software licensing, and tracked licensing compliance.
- Implemented Internet proxy/firewall and monitoring solutions.
- Administered and maintained Microsoft Exchange Server and user accounts.

- Maintained system tape backups and implemented disaster recovery planning (DRP).
- Maintained all servers, workstations, and printers.
- Provided Help Desk/end-user support for hardware, software, and Windows operating systems.
- Designed and maintained corporate intranet and Internet sites.
- Produced system/network documentation, standard operating procedures (SOPs), and IT policies.
- Maintained network security policy, addressed server security issues, and applied appropriate security patches and upgrades.

National Engineers Training Services, Lahore, Pakistan

1998 - 2001

Mr. Bashir's duties included:

- Installing, configuring and administering Microsoft IIS server (NT 4.0).
- Administering Domain Name Servers (DNSs – NT 4.0).
- Building secure file transfer protocol (FTP) servers.
- Administering general desktop support and assisting with Web development and Microsoft Exchange Server administration.
- Researching, acquiring, and configuring new network and server hardware systems.
- Providing continued operations and security of various network components, including Cisco 2500 routers, Cisco Catalyst 1900m and 2900 switches; and implementing the virtual local area networks (VLANs) for the segregation and security of the company's network.

EDUCATION

M.S., Computer Science, Askari College of Business and Computer Science, Lahore, Pakistan

CERTIFICATIONS AND TRAINING

- Certified Information System Security Professional (CISSP)
- Certification and Accreditation Professional (CAP)
- Microsoft Certified Systems Engineer (MCSE)
- Microsoft Certified Professional (MCP) – Windows 2000 Professional
- Certified Internet Web Master (CIW)
- NSTISSI No. 4013 (NSA)
- Information Systems Security Engineering Professional (ISSEP) – currently pursuing

CLEARANCES

OPM Public Trust Level 6

Gus Fritschie	
CISSP, CAP	
Member Since: 20 Nov 2002	Member Number: [REDACTED]

Certification Status									
Certification Awarded: 20 Nov 2002 				AMF Status Current Cycle Start Date: 01 Dec 2014 End Date: 30 Nov 2017 ☐ Pay \$85.00 by 30 Nov 2015		CPEStatus ☐ On Track			
#	Year	Begin	Due Date	Status	Amt	Group A	Group B	Total	
						Earned	Min	Earned	Earned
1	01 Dec 2014	30 Nov 2015			\$85	0.00	20	0.00	0.00
2	01 Dec 2015	30 Nov 2016			\$85	0.00	20	0.00	0.00
3	01 Dec 2016	30 Nov 2017			\$85	0.00	20	0.00	0.00
Credited to Date:					\$0	0.00	0.00	0.00	
Required for Renewal:					\$255	80	--	120	

Certification Awarded: 17 Apr 2007 				AMF Status Current Cycle Start Date: 01 May 2013 End Date: 30 Apr 2016 ☐ Pay \$65.00 by 30 Apr 2015		CPEStatus ☐ On Track			
#	Year	Begin	Due Date	Status	Amt	Group A	Group B	Total	
						Earned	Min	Earned	Earned
1	01 May 2013	30 Apr 2014		Paid	\$65	56.00	10	18.00	74.00
2	01 May 2014	30 Apr 2015			\$65	0.00	10	0.00	0.00
3	01 May 2015	30 Apr 2016			\$65	0.00	10	0.00	0.00
Credited to Date:					\$65	76.00*	18.00	94.00*	
Required for Renewal:					\$195	40	--	60	

* - Totals include rollover credits that are not included in yearly values.

Member Services Information	
Please contact your regional office for answers to your CPE credit or AMF payment questions:	
(ISC)² Member Support 311 Park Place Blvd. Suite 400 Clearwater, FL 33759 USA Ph: 1-866-331-ISC2 (4722) 1-727-785-0189	(ISC)² EMEA Second Floor 6 Hays Lane London SE1 2HB United Kingdom Ph: +44 (0)203.283.4383 Fx: +44 (0)203.283.4384
(ISC)² Asia-Pacific Suite 514, 5/F, South Tower World Finance Centre Harbour City, Kowloon Hong Kong Ph: +852.2850.6951 Fx: +852.2850.6959	(ISC)² Japan Yotsuya Business Garden 209 1-6-1 Wakaba Shinjuku-ku Tokyo 160-0011 Japan Ph: +81.3.5366.4824 Fx: +81.3.5366.4702 https://www.isc2.org/japan/

Links to more information

For detailed information regarding CPE requirements:
<https://www.isc2.org/CPE-requirements.aspx>

To view current CPE Guidelines and policies:
[https://www.isc2.org/uploadedFiles/\(ISC\)2_Member_Content/CPEs/cpe_guidelines.pdf](https://www.isc2.org/uploadedFiles/(ISC)2_Member_Content/CPEs/cpe_guidelines.pdf)

International Information Systems Security Certification Consortium

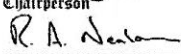
The (ISC)² Board of Directors hereby awards

Rehan Bashir

the credential of

Certified Information Systems Security Professional

Having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.


Chairperson

Recording Secretary



ANSI
ISO/IEC 17024

Certificate Number

June 2015

Expiration Date

Certified Since 2003

(ISC)²



Certificate of Completion

This certificate is awarded to

Rehan Bashir

In recognition of successfully completing training requirements for Advanced Training Standards for Systems Administration in INFOSEC NSTISSI No. 4013

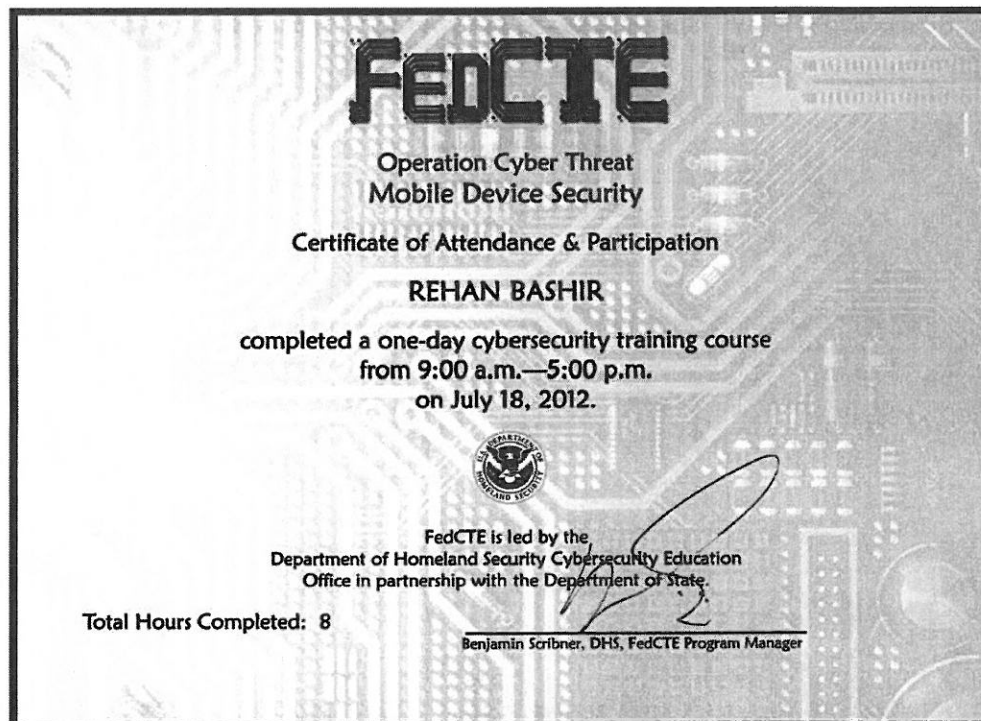
Signature

Dr. G.P. Singh, CEO
Karta Technologies, Inc.
Information Assurance Courseware Certified Institution

Date

July 7, 2004

Karta
The "Can Do" Company



SECTION 5: Attachment 3 – Attestation and Confirmations

Please see Team Elert's completed Attachment 3 – Attestation and Confirmations on the following pages.

REQUEST FOR QUOTATION

Information Security and Network Vulnerability Assessment

Attachment 3 – Attestation and Confirmations

Provide confirmation to the following statements, sign and submit this Attachment as part of the RFQ submission:

Statement	Confirmed (Yes/No)
Confirm that neither the vendor nor any of the vendor's employees, agents, independent contractors, or subcontractors have been convicted of, pled guilty to, pled nolo contendere or were named as an unindicted co-conspirator to any felony.	Yes
Confirm that there is no concluded or pending litigation against the vendor or vendor employees related to a contracted engagement.	Yes
Identify key staffs which would be assigned to the project and affirm that those individuals are full-time employees of the vendor.	Yes
Verify that neither the vendor nor any officer or employee have given any remuneration or anything of value directly or indirectly to CPRB or any of its Retirement Board members, officers, employees, or contracted consultants.	Yes
Verify that neither the vendor, nor any officer, principal or employee have given any remuneration or anything of value as a finder's fee, cash solicitation fee, or fee for consulting, lobbying or otherwise, in connection with this RFQ.	Yes
Verify that within the past five years neither the vendor, nor any officer or employee of the vendor have been a defending party in a legal proceeding before a court related to the provision of the services.	Yes
Verify that within the past five years neither the vendor, nor any officer or employee been the subject of a governmental regulatory agency inquiry, investigation, or charge.	Yes
Verify that neither the vendor, any officer of the vendor, nor any owner of a twenty percent (20%) interest or greater in the vendor has filed for bankruptcy, reorganization, a debt arrangement, moratorium, or any proceeding under any bankruptcy or insolvency law, or any dissolution or liquidation proceeding.	Yes
Verify that neither the vendor, nor any officer, principal or employee who shall perform work under the contract has a possible conflict of interest (e.g. employment with the State of West Virginia).	Yes
Verify that the vendor does not have any active managed	Yes

REQUEST FOR QUOTATION

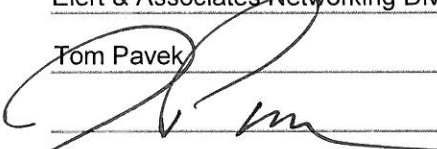
Information Security and Network Vulnerability Assessment

Attachment 3 – Attestation and Confirmations

Statement	Confirmed (Yes/No)
security service provider contract(s) with any State of West Virginia agency.	Yes
Confirm there are no pending Securities Exchange Commission investigations involving the Vendor, and if such are pending or in progress, an explanation providing relevant details and an attached opinion of counsel as to whether the pending investigation(s) will impair the Vendor's performance in a contract under this Solicitation.	Yes

Company: Elert & Associates Networking Division, Inc.

Printed Name: Tom Pavek

Signature: 

Title: Senior Vice President

Date: 01/19/2015

SECTION 6: Attachment 4 – Confidentiality and Non-Disclosure Statement

Please see Team Elert's completed Attachment 4 – Confidentiality and Non-Disclosure Statement on the following page.

**Consolidated Public Retirement Board
Confidentiality and Non-disclosure Statement**

Protecting confidentiality and understanding the sensitive nature of information recorded at the Consolidated Public Retirement Board (CPRB) becomes the responsibility of every person. We must strictly adhere to a policy of non-disclosure of any information relating to our clients, and every state employee or contract worker working inside of or with our office must sign and abide by this confidentiality statement.

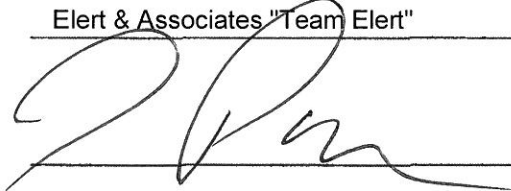
At no time, shall any state employee or contract worker who is working inside or with the CPRB discuss or distribute personal information regarding any client of this agency. This personal information includes, but is not limited to, client or employee salaries, medical history, pension specific information, social security numbers, or any other identifying numbers, addresses, banking information, telephone numbers, or any other data or information excluded from protection by the WV Freedom of Information Act.

"I, Tom Pavek the (title) Senior Vice President of

(company) Elert & Associates Networking Division, Inc. understand the sensitive nature and the confidentiality of the client/employee information stored at the West Virginia Consolidated Public Retirement Board. All employees of this company therefore acknowledge and agree that personal client/employee information and any other related data is to be treated as confidential information which is not a matter of public record. All employees of the above named company therefore agree not to permit distribution or engage in discussion of this information to any person. I understand that, if at any time I am approached by an outside individual, agency or media representative, I shall direct their queries to the Executive Director of the West Virginia Consolidated Public Retirement Board."

Print Name: Tom Pavek

Company: Elert & Associates "Team Elert"

Signature: 

Date: 01/19/2015

SECTION 7: Exhibit A - Pricing Page & RFQ Signed Documents

Please see Team Elert's completed Exhibit A – Pricing Page and Request For Quotation signed document on the following pages.

**Exhibit A
Pricing Page**

Information Security and Network Vulnerability Assessment service for CPRB

Eiert & Associates

Item	Item Description	Description	Unit of Measure	Unit Cost	Quantity Needed	Extended Cost
1	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 1	per Complete Assessment	\$18,200	1	\$18,200 0.00-
2	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 2	per Complete Assessment	\$27,160	1	\$27,160 0.00-
3	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 3	per Complete Assessment	\$27,160	1	\$27,160 0.00-
4	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 4	per Complete Assessment	\$29,720	1	\$29,720 0.00-
5	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 5	per Complete Assessment	\$32,280	1	\$32,280 0.00-
TOTAL of Assessments						\$134,520 0.00-

Assessment Cost are firm fixed for each complete Assessments

* Contrat Award will be for Total of Assessments *



Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
10 - Consulting

Proc Folder: 15921

Doc Description: Addendum2 for CRFQ CPR15*1

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2015-01-09	2015-01-22 13:30:00	CRFQ 0203 CPR1500000001	3

BID RECEIVING LOCATION

BID CLERK

DEPARTMENT OF ADMINISTRATION

PURCHASING DIVISION

2019 WASHINGTON ST E

CHARLESTON

WV 25305

US

VENDOR

Vendor Name, Address and Telephone Number:

Elert & Associates

140 Third Street South

Stillwater, MN 55082

651-705-1249 (Rick Anderson)

FOR INFORMATION CONTACT THE BUYER

Cindy L Adkins

(304) 558-3570

cindy.l.adkins@wv.gov

Signature X

Tom Pavsek

FEIN # 41-1826380

DATE 01/19/2015

All offers subject to all terms and conditions contained in this solicitation

INVOICE TO		SHIP TO	
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE		CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE	
CHARLESTON	WV24304	CHARLESTON	WV 25304
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	network security and vulnerability assessment	0.00000	LS	\$18,200	\$18,200

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO		SHIP TO	
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE		CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE	
CHARLESTON	WV24304	CHARLESTON	WV 25304
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	network security and vulnerability assessment	0.00000	LS	\$27,160	\$27,160

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO		SHIP TO	
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE		CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE	
CHARLESTON	WV24304	CHARLESTON	WV 25304
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	network security and vulnerability assessment	0.00000	LS	\$27,160	\$27,160

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO		SHIP TO	
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE		CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE	
CHARLESTON	WV24304	CHARLESTON	WV 25304
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	network security and vulnerability assessment	0.00000	LS	\$29,720	\$29,720

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO		SHIP TO	
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE		CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE	
CHARLESTON	WV24304	CHARLESTON	WV 25304
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	network security and vulnerability assessment	0.00000	LS	\$32,280	\$32,280

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

CPR1500000001	Document Phase Final	Document Description Addendum2 for CRFQ CPR15*1	Page 4 of 4
---------------	--------------------------------	---	-----------------------

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

SECTION 8: Vendor Preference Certificate

Please see Team Elert's completed Vendor Preference Certificate on the following page.

State of West Virginia

VENDOR PREFERENCE CERTIFICATE

Certification and application* is hereby made for Preference in accordance with **West Virginia Code**, §5A-3-37. (Does not apply to construction contracts). **West Virginia Code**, §5A-3-37, provides an opportunity for qualifying vendors to request (at the time of bid) preference for their residency status. Such preference is an evaluation method only and will be applied only to the cost bid in accordance with the **West Virginia Code**. This certificate for application is to be used to request such preference. The Purchasing Division will make the determination of the Vendor Preference, if applicable.

1. Application is made for 2.5% vendor preference for the reason checked:

- ☐ Bidder is an individual resident vendor and has resided continuously in West Virginia for four (4) years immediately preceding the date of this certification; **or**,
☐ Bidder is a partnership, association or corporation resident vendor and has maintained its headquarters or principal place of business continuously in West Virginia for four (4) years immediately preceding the date of this certification; **or** 80% of the ownership interest of Bidder is held by another individual, partnership, association or corporation resident vendor who has maintained its headquarters or principal place of business continuously in West Virginia for four (4) years immediately preceding the date of this certification; **or**,
☐ Bidder is a nonresident vendor which has an affiliate or subsidiary which employs a minimum of one hundred state residents and which has maintained its headquarters or principal place of business within West Virginia continuously for the four (4) years immediately preceding the date of this certification; **or**,

2. Application is made for 2.5% vendor preference for the reason checked:

- ☐ Bidder is a resident vendor who certifies that, during the life of the contract, on average at least 75% of the employees working on the project being bid are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or**,

3. Application is made for 2.5% vendor preference for the reason checked:

- ☐ Bidder is a nonresident vendor employing a minimum of one hundred state residents or is a nonresident vendor with an affiliate or subsidiary which maintains its headquarters or principal place of business within West Virginia employing a minimum of one hundred state residents who certifies that, during the life of the contract, on average at least 75% of the employees or Bidder's affiliate's or subsidiary's employees are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or**,

4. Application is made for 5% vendor preference for the reason checked:

- ☐ Bidder meets either the requirement of both subdivisions (1) and (2) or subdivision (1) and (3) as stated above; **or**,

5. Application is made for 3.5% vendor preference who is a veteran for the reason checked:

- ☐ Bidder is an individual resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard and has resided in West Virginia continuously for the four years immediately preceding the date on which the bid is submitted; **or**,

6. Application is made for 3.5% vendor preference who is a veteran for the reason checked:

- ☐ Bidder is a resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard, if, for purposes of producing or distributing the commodities or completing the project which is the subject of the vendor's bid and continuously over the entire term of the project, on average at least seventy-five percent of the vendor's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years.

7. Application is made for preference as a non-resident small, women- and minority-owned business, in accordance with West Virginia Code §5A-3-59 and West Virginia Code of State Rules.

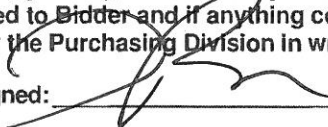
- ☒ Bidder has been or expects to be approved prior to contract award by the Purchasing Division as a certified small, women- and minority-owned business.

Bidder understands if the Secretary of Revenue determines that a Bidder receiving preference has failed to continue to meet the requirements for such preference, the Secretary may order the Director of Purchasing to: (a) reject the bid; or (b) assess a penalty against such Bidder in an amount not to exceed 5% of the bid amount and that such penalty will be paid to the contracting agency or deducted from any unpaid balance on the contract or purchase order.

By submission of this certificate, Bidder agrees to disclose any reasonably requested information to the Purchasing Division and authorizes the Department of Revenue to disclose to the Director of Purchasing appropriate information verifying that Bidder has paid the required business taxes, provided that such information does not contain the amounts of taxes paid nor any other information deemed by the Tax Commissioner to be confidential.

Under penalty of law for false swearing (West Virginia Code, §61-5-3), Bidder hereby certifies that this certificate is true and accurate in all respects; and that if a contract is issued to Bidder and if anything contained within this certificate changes during the term of the contract, Bidder will notify the Purchasing Division in writing immediately.

Bidder: Elert & Associates

Signed: 

Tom Pavek

Date: 01/19/2015

Title: Senior Vice President

SECTION 9: Purchasing Affidavit

Please see Team Elert's completed Purchasing Affidavit on the following page.

STATE OF WEST VIRGINIA
Purchasing Division**PURCHASING AFFIDAVIT**

MANDATE: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

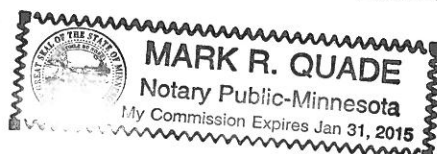
"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceeds five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (W. Va. Code §61-5-3) that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:Vendor's Name: Elet & AssociatesAuthorized Signature: _____ Date: 01/19/2015State of MinnesotaCounty of Washington, to-wit:Taken, subscribed, and sworn to before me this 19th day of January, 2015.

My Commission expires _____, 20____.

AFFIX SEAL HERE**NOTARY PUBLIC***Purchasing Affidavit (Revised 07/01/2012)*

SECTION 10: Addendum Acknowledgement Form & Signature Pages

Please see Team Elert's completed Addendum Acknowledgement Form and signature pages for the RFQ, Addendum 1, and Addendum 2 on the following pages.

ADDENDUM ACKNOWLEDGEMENT FORM

SOLICITATION NO.: CRFQ0203 CPR1500000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

☒ Addendum No. 1	☐ Addendum No. 6
☒ Addendum No. 2	☐ Addendum No. 7
☐ Addendum No. 3	☐ Addendum No. 8
☐ Addendum No. 4	☐ Addendum No. 9
☐ Addendum No. 5	☐ Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Elert & Associates
Company

Authorized Signature

Tom Pavek

01/19/2015

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

SOLICITATION NUMBER: CRQS CPR1500000002

Addendum Number: 01

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

- ☒ Modify bid opening date and time
- ☐ Modify specifications of product or service being sought
- ☐ Attachment of vendor questions and responses
- ☐ Attachment of pre-bid sign-in sheet
- ☐ Correction of error
- ☐ Other

Description of Modification to Solicitation:

Addendum issued to publish and distribute the following information to the vendor community. Bid opening is being moved to allow Agency time to address the Vendor questions that were presented. An Addendum will be published at a latter date to address these questions and the Agency responses.

Bid Opening was: 01/06/15 at 1:30 PM. EST
Bid Opening Now: 1/15/15 at 1:30 PM. EST.

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.
2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

SOLICITATION NUMBER: CRQS CPR1500000002

Addendum Number: 02

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

- ☒ Modify bid opening date and time
- ☐ Modify specifications of product or service being sought
- ☐ Attachment of vendor questions and responses
- ☐ Attachment of pre-bid sign-in sheet
- ☐ Correction of error
- ☐ Other

Description of Modification to Solicitation:

Addendum Issued to publish and distribute the following information to the vendor community.

1. Vendor submitted questions and Agency's responses.
2. Bid opening Changed from: 01/15/15 at 1:30 PM. EST
Bid Opening Now: 01/22/15 at 1:30 PM. EST.

No other Changes.

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.
2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.



Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
10 — Consulting

Proc Folder: 15921

Doc Description: Information Security and Network Vulnerability Assessment

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2014-12-05	2015-01-06 13:30:00	CRFQ 0203 CPR1500000001	1

BID RECEIVING LOCATION

BID CLERK

DEPARTMENT OF ADMINISTRATION

PURCHASING DIVISION

2019 WASHINGTON ST E

CHARLESTON

WV 25305

US

VENDOR

Vendor Name, Address and Telephone Number:

Elert & Associates

140 Third Street South

Stillwater, MN 55082

651-705-1249

FOR INFORMATION CONTACT THE BUYER

Guy Nisbet

(304) 558-2596

guy.l.nisbet@wv.gov

Signature X

Tom Pavek FEIN # 41-1826380

DATE 01/19/2015

All offers subject to all terms and conditions contained in this solicitation



Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
10 - Consulting

Proc Folder: 15921

Doc Description: Addendum1for CRFQ CPR15*1

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2014-12-29	2015-01-15 13:30:00	CRFQ 0203 CPR1500000001	2

BID RECEIVING LOCATION

BID CLERK

DEPARTMENT OF ADMINISTRATION

PURCHASING DIVISION

2019 WASHINGTON ST E

CHARLESTON

WV 25305

US

VENDOR

Vendor Name, Address and Telephone Number:

Elert & Associates

140 Third Street South

Stillwater, MN 55082

651-705-1249

FOR INFORMATION CONTACT THE BUYER

Guy Nisbet

(304) 558-2596

guy.l.nisbet@wv.gov

Signature X

Tom Pavek FEIN # 41-1826380

DATE 01/19/2015

All offers subject to all terms and conditions contained in this solicitation



Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
10 — Consulting

Proc Folder: 15921

Doc Description: Addendum2 for CRFQ CPR15*1

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2015-01-09	2015-01-22 13:30:00	CRFQ 0203 CPR1500000001	3

BID RECEIVING LOCATION

BID CLERK

DEPARTMENT OF ADMINISTRATION

PURCHASING DIVISION

2019 WASHINGTON ST E

CHARLESTON

WV 25305

US

VENDOR

Vendor Name, Address and Telephone Number:

Elert & Associates

140 Third Street South

Stillwater, MN 55082

651-705-1249

FOR INFORMATION CONTACT THE BUYER

Guy Nisbet

(304) 558-2596

guy.l.nisbet@wv.gov

Signature X

Tom Pavek FEIN # 41-1826380

DATE 01/19/2015

All offers subject to all terms and conditions contained in this solicitation

SECTION 11: Certification and Signature Page

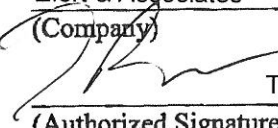
Please see Team Elert's Certification and Signature Page on the following page.

CERTIFICATION AND SIGNATURE PAGE

By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

Elert & Associates

(Company)

 Tom Pavek, Sr. Vice President

(Authorized Signature) (Representative Name, Title)

651-430-2772 / 651-430-2661 / 01/19/2015

(Phone Number) (Fax Number) (Date)