



801 International Parkway | 5th Floor | Lake Mary, Florida 32746 | Tel: (407) 562 1864 | Fax: (407) 562 2001

January 19, 2010

State of West Virginia
Department of Administration
Purchasing Division
Building 15
2019 Washington Street East
Charleston, WV 25305-0130

Re: Statewide Contract for Technical Services
RFQ No.: ITECH10

To Whom It May Concern:

Attached, please find a copy of our proposal for ITECH10. I sent in the original draft on January 10, 2010, but then learned there were two addendum to the original RFQ. As such, we are resubmitting one original and two copies of our proposal identified as Version 2. Please note that we submitted the required No Debt Affidavit with our original document and did not have a copy to submit with the revised proposal. Please use the signed No Debt Affidavit that was submitted with Version 1 of our proposal.

If you have any questions, please do not hesitate to contact me. We look forward to working with the State of West Virginia.

Sincerely,

A handwritten signature in black ink, appearing to read "Thomas Welch", written in a cursive style.

Thomas Welch
President and CEO

RECEIVED

2010 JAN 20 AM 10:02

WV PURCHASING
DIVISION



Proposal for
Statewide Contract for Technical Services
RFQ No.: ITECH10

Prepared for:

State of West Virginia
Department of Administration
Purchasing Division
Building 15
2019 Washington Street East
Charleston, WV 25305-0130

January 19, 2010
(Version 2)

Prepared by:

Bullzi Security, Inc.
801 International Parkway
Suite 500
Lake Mary, Florida 32746

This proposal or quotation includes data that shall not be disclosed outside the State of West Virginia ("State"), and shall not be duplicated, used, or disclosed — in whole or in part — for any purpose other than to evaluate this proposal or quotation. If, however, a contract is awarded to this offeror or quoter as a result of — or in connection with — the submission of this document, the State shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the State's right to use information contained in this document if it is obtained from another source without restriction. The data subject to this restriction is contained in all sheets.

© 2010 by Bullzi Security Inc. All rights reserved.

Statement of Confidentiality and Validity

Bullzi Security Inc. has prepared this document for the sole purpose and exclusive use of the State of West Virginia. Due to the confidential nature of the material in this proposal, Bullzi Security requests this document and its contents not be discussed, disclosed, or divulged without the prior written consent of Bullzi Security.

Copyright Notice

This document is proprietary and does not exist in the public domain. This copyright notice is attached only to provide protection in the event of inadvertent publication. No part of this publication may be copied without the express written permission of Bullzi Security.

Copyright © 2010 Bullzi Security, Inc.
All rights reserved.



COVER LETTER

Bullzi Security, Inc.
801 International Parkway
Suite 501
Lake Mary, Florida 32746

January 10, 2010

State of West Virginia
Department of Administration
Purchasing Division
Building 15
2019 Washington Street East
Charleston, WV 25305-0130

Re: Statewide Contract for Technical Services
RFQ No.: ITECH10

To Whom It May Concern:

Bullzi Security, Inc. is pleased to submit this bid to the State of West Virginia for the Statewide Contract for Technical Services (RFQ No.: ITECH10). Thomas Welch will be the primary contact to speak on behalf of Bullzi Security.

Contact Information: Thomas Welch
Tel: (407)562-1864
Cell: (973)809-5509
Fax: (407)562-2001
e-mail: twelch@bullzisecurity.com

Bullzi Security meets or exceeds all of the mandatory requirements of this RFQ. If you have any questions, please do not hesitate to contact me. We look forward to working with the State of West Virginia.

Sincerely,

Thomas Welch
President and CEO



TABLE OF CONTENTS

| | |
|---|----|
| <i>Cover Letter</i> | 3 |
| <i>Table of Contents</i> | 4 |
| <i>Section I</i> | 5 |
| <i>Corporate Description</i> | 5 |
| <i>Section II</i> | 8 |
| <i>Qualifications and Experience of the Company</i> | 8 |
| <i>Supplemental Staffing for</i> | 8 |
| <i>Computer Systems and Network Security</i> | 8 |
| 2.1 Experience..... | 8 |
| 2.2 Resumes..... | 9 |
| 2.3 References for Supplemental Staffing for Computer Systems and Network Security..... | 10 |
| <i>Section III</i> | 12 |
| <i>Qualifications and Experience of the Company</i> | 12 |
| <i>Attachment 4</i> | 12 |
| <i>Internet/Intranet and Electronic Commerce Security Development and Implementation</i> | 12 |
| 3.1 Experience..... | 12 |
| 3.2 Certifications..... | 14 |
| 3.3 Resumes..... | 15 |
| 3.4 References for Internet/Intranet and Electronic Commerce Security Development and Implementation..... | 16 |
| <i>Section 4</i> | 18 |
| <i>Other Documents</i> | 18 |
| <i>Appendix A</i> | 19 |
| <i>Resumes</i> | 19 |
| <i>Appendix B</i> | 30 |
| <i>Addendum Acknowledgment</i> | 30 |

SECTION I
CORPORATE DESCRIPTION

- 1) Bullzi Security, Inc.
801 International Parkway
Suite 500
Lake Mary, Florida 32746
Contact Number: (407)562-1864
Fax Number: (407)562-2001

Federal ID Number: 20-1840083

Website: www.bullzisecurity.com
www.sendsecure.com
www.wiselearningsolutions.com

- 2) Contact Name: Thomas Welch
P.O. Box 11398
Southport, NC 28461
Contact Number: (973)809-5509

- 3) The Company was formed on Oct. 25, 2004, as the merger of Welch and Welch Investigations, Inc. (formed in June 1988), Secure Enterprise Software, Inc. (formed in June 2002) and WISE Learning Solutions, Inc. (formed in 2004). On January 1, 2006, the company had 7 full-time employees. Today, we have over 30 employees and contractors.

- 4) Company History

Bullzi Security is an information security consulting and education company with operations in Florida, North Carolina and New Jersey. Bullzi Security's administration will be coordinated out of our Lake Mary, Florida office, while routine company management will be coordinated by service line managers who meet regularly to ensure efficient resource utilization.

Bullzi Security provides the information security consulting services, such as security assessments, penetration testing, regulatory compliance programs, policy development and security mitigation measures. The information that is possessed by companies today, is their greatest asset, and as we have seen lately, is subject to unauthorized access, breaches, loss of data, etc. The business world must be ready to protect this information and be prepared to detect and respond to cyber attacks. Bullzi Security conducts risk assessments or vulnerability testing of its client's information systems, providing an

analysis of the organization's vulnerabilities from a physical security, IT security, document security and personnel security prospective.

Bullzi Security will use proprietary techniques, based on industry standards (ISO-17799) as well as the most reliable, up-to-date automated security assessment tools, to generate security profiles of essential information systems. The vulnerability testing service focuses on the client's IT exposures. With the recent rash of breaches and unauthorized access that have made the news, along with federal mandates such as Healthcare Insurance Portability and Accountability Act (HIPAA); North American Electric Reliability Council (NERC); the Gramm-Leach-Bliley Act (GLBA) and the Sarbanes-Oxley Act (SOX), Bullzi Security is set to launch a marketing campaign focusing on the protection of one's information.

Figure 1, below, identifies the products and services that will be offered by Bullzi Security.

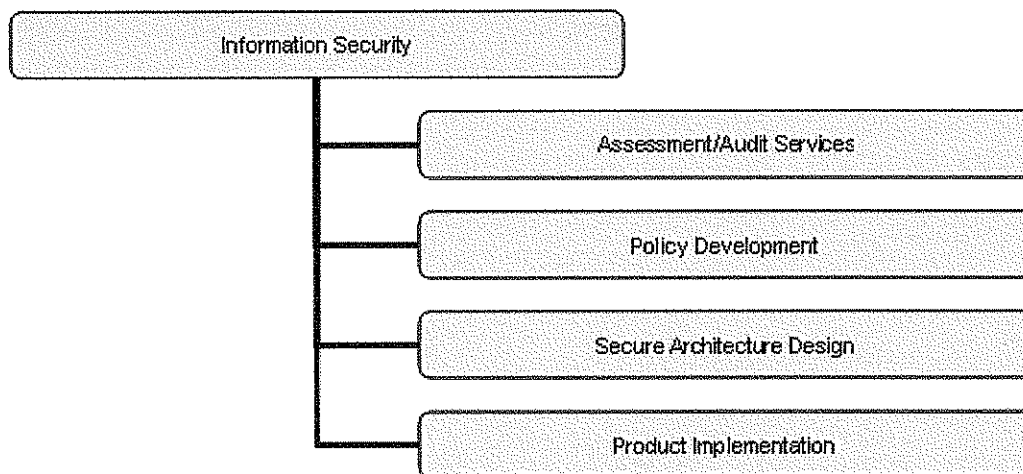


Figure 1 – Information Security Products and Services

In addition to its information security consulting business, Bullzi Security also provides security education company, WISE Learning Solution LLC ("WISE"). WISE is a wholly-owned subsidiary of Bullzi Security, Inc.

WISE Learning Solutions LLC (WISE)

WISE Learning Solutions LLC (a Nevada limited liability company) is an eLearning company that was originally founded in October 2004 by Thomas W. Welch, Michael D. Welch and Michael H. Welch as WISE Learning Solutions, Inc. WISE, which is an acronym for Web-based Information Security Education, provides web-based security training solutions that use multimedia technology (e.g. audio, graphics, animation, video and text).

The WISE flagship product, Information Security Awareness, was designed to meet the mandated training requirements of many to today's regulatory programs, such as the

Healthcare Insurance Portability and Accountability Act (HIPAA); North American Electric Reliability Council (NERC); the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley Act (SOX) and others. The WISE courses were created due to a void in the industry for this type of training. Traditional classroom-based training simply is not scalable and is logistically difficult to implement.

The Information Security Awareness program is currently offered in five languages (English, French, Spanish, Brazilian Portuguese and Japanese). Other languages, such as Serbian and Chinese, are expected to be available in the second fiscal quarter of 2006. Italian, Russian and German are slated for release later this year.

The WISE Information Security Awareness program educates system users on the value of corporate assets, acceptable use of the Internet, how to handle e-mail attachments and forty-four other topics related to safe computing. In addition to awareness training, WISE has completed, or is in the process of completing, training programs that address privacy, secure coding practices, anti-money laundering, physical security, information security engineering, identity theft, computer forensics, and more.

Figure 2, below, identifies the products and services offered by WISE.

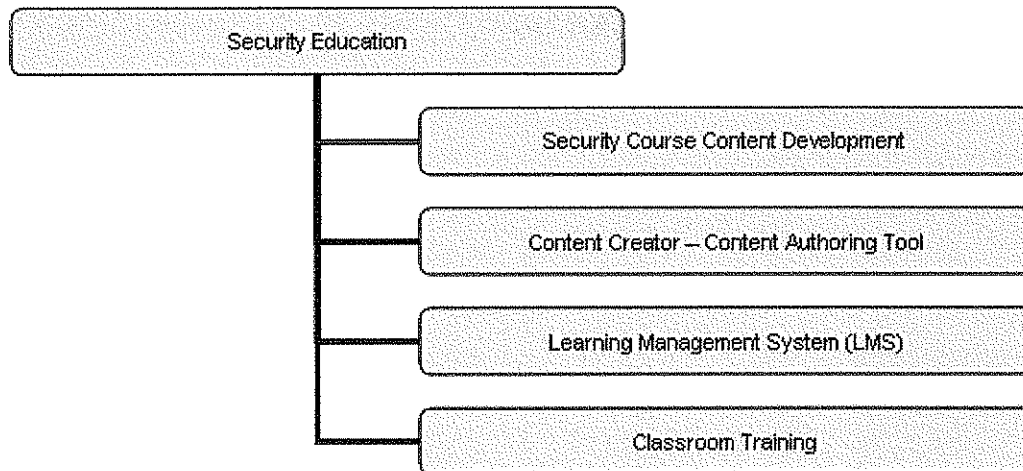


Figure 2 – Security Education Products and Services

SECTION II

QUALIFICATIONS AND EXPERIENCE OF THE COMPANY
SUPPLEMENTAL STAFFING FOR
COMPUTER SYSTEMS AND NETWORK SECURITY

Category: Computer Systems and Network Security

Description: Includes, but is not limited to; analysis, assessment, planning, firewalls, virtual private networks, design and review, virus, on all levels and all software platforms.

2.1 Experience

Providing information security and privacy services is well within the competencies of Bullzi Security. Through our consulting services and integrated delivery systems, Bullzi Security helps to minimize the threats to its clients' information systems and communication networks. Bullzi Security brings a unique set of skills and experience to ensure each client receives the most comprehensive, cost-effective information security services available. As an end-to-end information security solutions provider, Bullzi Security offers its clients the full breadth of information security products and services including:

- Information Security Consulting and Technology Planning
- Information Security Assessments and Audits
- Information Security and Privacy Policy Review and Development
- Information Security and Privacy Training and Awareness Programs
- Secure Architecture Design
- Security Products Implementation and Integration
- Managed Security Services (Firewalls and Intrusion Detection Systems)
- Computer Incident Response Team (CIRT) w/24 Hour Rapid Response
- Investigative and Forensic Services

Bullzi Security is an expert in the information security field. We have the experience, expertise, credentials, and professionalism to meet or exceed the expectations of the State. The Bullzi Security team has been working together for the past ten years. The team of professional security consultants has conducted hundreds of assessments for our clients, from various industry segments, such as government, higher education, healthcare, banking and finance, Fortune 500 companies, etc.

2.2 Resumes

The security engineers on the Bullzi Security team, identified in Table 3.3-1, have come from numerous areas within the Information Technology (IT) industry, such as system administration, network administration, programming, investigation and forensic analysis. Only qualified, senior level security engineers will be assigned to this engagement. The resumes for the engineers that will be assigned to this project can be found in Appendix A.

| Task | Company | Name |
|--------------------------------------|-----------------|------------------|
| Security assessments (web-based) | Bullzi Security | Michael Welch |
| Security assessments (network-based) | Bullzi Security | Alex Solomonovic |
| Risk and Security Management | Bullzi Security | Thomas Welch |

Table 2.2-1 Project Staffing Table

As a security company whose reputation is based on its clients' trust, Bullzi Security recognizes the importance of fostering that trust. One of the key ways in which Bullzi Security does this is by going through extraordinary lengths to ensure that it hires only the best people, with trustworthy backgrounds. Each and every security consultant is required to go through an extensive background check as a condition of employment. The background check consists of the following:

- Civil Litigation, includes lawsuits past, present and ongoing
- Criminal Background check via National Crime Information Computer
- Credit check via the Credit Bureau

Additionally, each security engineer signs a company Non-disclosure agreement (NDA) stating that he/she will not divulge information learned about a particular client. Once the project is complete, Bullzi Security burns a copy of the report on CD. Once the State confirms receipt of a readable copy of the CD, the assessment information is deleted from the Bullzi Security systems.

2.3 References for Supplemental Staffing for Computer Systems and Network Security

| | |
|--|--|
| <i>Company Name</i> | <i>West Virginia Health Care Authority</i> |
| <i>Contact Name</i> | John Grey |
| <i>Contact Phone Number and E-mail</i> | (304) 348-2250 jgrey@hcawv.org |
| <i>Project Dates, Duration and Value</i> | Information Security Assessment: 2002 Duration: 19 days Project Value: \$42K Follow-up Security Assessment: 2004 Duration: 5 days Project Value: \$12K |
| <i>Brief Description of Project</i> | Security Assessments, HIPAA Assessment and ISO 17799 Review |
| <i>Staff Assigned</i> | Thomas Welch, Alex Solomonovic, Michael Welch |
| <i>Consultants Role</i> | The consultants assigned to this project conducted information security assessments, which included a review of the clients compliance with the HIPAA and ISO standards. This included a review of administrative, physical and technical controls. The technical review required the use of a number of 3 rd party software packages such as nessus, nmap, Solar Winds, WebInspect, etc. |

| | |
|--|--|
| <i>Company Name</i> | <i>Union Center National Bank</i> |
| <i>Contact name</i> | Barbara Leibman |
| <i>Contact Phone Number and E-mail</i> | (908)206-2956 BLIEBMAN@ucnb.com |
| <i>Project Dates, Duration and Value</i> | October 2002 – 2008 Duration: 20 days / year Project Value: \$40K |
| <i>Brief Description of Project</i> | Security Assessments, Security Product Implementation |
| <i>Staff Assigned</i> | Thomas Welch, Alex Solomonovic, Michael Welch |
| <i>Consultants Role</i> | The consultants assigned to this project conducted information security assessments, which included a review of the clients compliance with the GLB Act. The assessment included a review of administrative, physical and technical controls. The technical review required the use of a number of 3 rd party software packages such as nessus, nmap, Solar Winds, WebInspect, etc. |

| | |
|--|--|
| <i>Company Name</i> | <i>McDonald Information Services</i> |
| <i>Contact name</i> | Rich Rager |
| <i>Contact Phone Number and E-mail</i> | (201)659-2600 rich@callmis.com |
| <i>Project Dates, Duration and Value</i> | June 2005 – Current Duration: 30 days (conducted annually) Project Value: \$60K |
| <i>Brief Description of Project</i> | Policy Development, Security Assessments and PCI/ISO Reviews, Vendor Selection Assistance |
| <i>Staff Assigned</i> | Thomas Welch, Alex Solomonovic |
| <i>Consultants Role</i> | The consultants assigned to this project conducted information security assessments, which included a review of the clients compliance with the Payment Card Industry Data Security Standard (PCI DSS) and the ISO 27002 standard. This included a review of administrative, physical and technical controls. The technical review required the use of a number of 3 rd party software packages such as nessus, nmap, Solar Winds, WebInspect, etc. |

SECTION III

QUALIFICATIONS AND EXPERIENCE OF THE COMPANY

ATTACHMENT 4

**INTERNET/INTRANET AND ELECTRONIC COMMERCE SECURITY DEVELOPMENT
AND IMPLEMENTATION**

3.1 Experience

Providing information security and privacy services is well within the competencies of Bullzi Security. Through our consulting services and integrated delivery systems, Bullzi Security helps to minimize the threats to its clients' information systems and communication networks. Bullzi Security brings a unique set of skills and experience to ensure each client receives the most comprehensive, cost-effective information security services available. As an end-to-end information security solutions provider, Bullzi Security offers its clients the full breadth of information security products and services including:

- Information Security Consulting and Technology Planning
- Information Security Assessments and Audits
- Information Security and Privacy Policy Review and Development
- Information Security and Privacy Training and Awareness Programs
- Secure Architecture Design
- Security Products Implementation and Integration
- Managed Security Services (Firewalls and Intrusion Detection Systems)
- Computer Incident Response Team (CIRT) w/24 Hour Rapid Response
- Investigative and Forensic Services

Bullzi Security is an expert in the information security field. We have the experience, expertise, credentials, and professionalism to meet or exceed the expectations of the State. The Bullzi Security team has been working together for the past ten years. The team of professional security consultants has conducted hundreds of assessments for our clients, from various industry segments, such as government, higher education, healthcare, banking and finance, Fortune 500 companies, etc.

From the perspective of a large project in the government sector, Bullzi Security' lead security consultant, Thomas Welch, designed the first public law enforcement network for the Kansas Bureau of Investigation (KBI). This was the first state in the United States to transmit National Crime Information Center (NCIC) and Central Criminal History (CCH) records across the Internet in a secure mode. The KBI replaced all 590 frame and point-to-point circuits, from all local and county agencies, with a Virtual Private Network

(VPN) over the Internet. Mr. Welch conducted the analysis and wrote the final Security Architecture Report, which ultimately resulted in FBI approval.

When conducting assessments, the Bullzi Security team follows the ISO 17799 and NIST security standards. From an assessment perspective, the Bullzi Security team has the experience and knowledge to conduct technology audits from a number of perspectives. This includes:

- Physical Security Audits
- Personnel Security Audits
- Documentation Reviews (Policy, Procedures, Standards, Topology Diagrams)
- Technical Assessments, including but not limited to:
 - External Penetration Testing
 - Internal Host and LAN Assessments
 - Application Assessments
 - Workstation Assessments
 - Wireless LAN Assessments
 - Firewall & Router Assessments

The Bullzi Security team has a number of key advantages over other companies. One of these advantages is our incident response and forensic experience. Based on our examination of various incidents and crime scenes, we are better able to help protect our clients' sites and identify hidden vulnerabilities. Additionally, the Bullzi Security team is comprised of security professionals who have expertise in the following disciplines:

- ISO 17799 Knowledge
- Policy and Standards Development
- Security Assessments
- PKI/LDAP/X.500
- Biometrics
- Incident Response/Forensics
- Firewall Design
- Intrusion Detection System
- Virus Protection
- Content Filtering
- URL Filtering
- Encryption
- Two-Factor Authentication
- Physical Security
- RADIUS Servers

All of the security engineers have access to these specialty experts whenever needed. In addition, State technical staff has the option of being involved in all aspects of the assessment. This interaction will allow for extensive "knowledge transfer" from the Bullzi Security staff to the State IT staff. All authorized individuals from State's IT staff have the option of participating in the entire testing process. Additionally, all tools and techniques will be discussed and explained.

Many times the same security vulnerabilities exist on numerous systems throughout the network, thus the Bullzi Security team will work closely with State's IT staff and educate them on how to remedy many of the standard deficiencies discovered during the scanning process. This process of knowledge transfer will allow the State IT staff to become more knowledgeable in security issues, thereby more independent on future assessments.

The strength of the Bullzi Security team is in its people and methodologies. Information Security is an esoteric field, comprised of many disciplines.

3.2 Certifications

The Bullzi Security team members have the following certifications and training.

Industry Certifications:

Bullzi Security has security consultants who hold the following industry certifications:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Protection Professional (CPP)
- Certified Fraud Investigator (CFI)

All of the Bullzi Security team members that are named in this proposal currently have their CISSPs.

Product Certifications:

Bullzi Security has security consultants certified in the following product sets:

- Certified Checkpoint Security Engineer (CCSE)
- Certified Checkpoint Security Administrator (CCSA)
- Certified Nokia Security Administration (IPSO and VRRP)
- Cisco Certified Network Associate (CCNA)
- Certified Entrust PKI Administrator & Engineer
- Tripwire Certified

Bullzi Security also has security consultants that are experts in the following product sets:

- Assessment Tools – Nessus, nmap, Web Inspect, Saint, Solar Winds, and numerous others
- Forensic Tools – Encase, The Coroners Toolkit, Expert Witness
- Anti-virus Products – F-Secure, eSafe, TrendMicro, Symantec, MacAfee
- Hacking/Security Tools – IophtCrack, SuperSniff, AntiSniff, Back Oriface 2000
- Authentication Tools – ActivCard, RADIUS, RSA Security Dynamics Tokens and ACE Server
- Operating System Security Administration – Windows NT, Windows 2000, Linux Solaris, Cisco Routers
- Programming expertise in several programming languages as well as web based technologies.
- Wireless Technologies (802,11b, CDPD, RAM, Circuit Switched Cellular)

3.3 Resumes

The security engineers on the Bullzi Security team, identified in Table 3.3-1, have come from numerous areas within the Information Technology (IT) industry, such as system administration, network administration, programming, investigation and forensic analysis. Only qualified, senior level security engineers will be assigned to this engagement. The resumes for the engineers that will be assigned to this project can be found in Appendix A.

| Task | Company | Name |
|--------------------------------------|-----------------|------------------|
| Security assessments (web-based) | Bullzi Security | Michael Welch |
| Security assessments (network-based) | Bullzi Security | Alex Solomonovic |
| Risk and Security Management | Bullzi Security | Thomas Welch |

Table 3.3-1 Project Staffing Table

As a security company whose reputation is based on its clients' trust, Bullzi Security recognizes the importance of fostering that trust. One of the key ways in which Bullzi Security does this is by going through extraordinary lengths to ensure that it hires only the best people, with trustworthy backgrounds. Each and every security consultant is required to go through an extensive background check as a condition of employment. The background check consists of the following:

- Civil Litigation, includes lawsuits past, present and ongoing
- Criminal Background check via National Crime Information Computer
- Credit check via the Credit Bureau

Additionally, each security engineer signs a company Non-disclosure agreement (NDA) stating that he/she will not divulge information learned about a particular client. Once the project is complete, Bullzi Security burns a copy of the report on CD. Once the State confirms receipt of a readable copy of the CD, the assessment information is deleted from the Bullzi Security systems.

3.4 References for Internet/Intranet and Electronic Commerce Security Development and Implementation

| | |
|--|--|
| <i>Company Name</i> | <i>West Virginia Health Care Authority</i> |
| <i>Contact Name</i> | John Grey |
| <i>Contact Phone Number and E-mail</i> | (304) 348-2250 jgrey@hcawv.org |
| <i>Project Dates, Duration and Value</i> | Information Security Assessment: 2002 Duration: 19 days Project Value: \$42K Follow-up Security Assessment: 2004 Duration: 5 days Project Value: \$12K |
| <i>Brief Description of Project</i> | Security Assessments, HIPAA Assessment and ISO 17799 Review |
| <i>Staff Assigned</i> | Thomas Welch, Alex Solomonovic, Michael Welch |
| <i>Consultants Role</i> | The consultants assigned to this project conducted information security assessments, which included a review of the clients compliance with the HIPAA and ISO standards. This included a review of administrative, physical and technical controls. The technical review required the use of a number of 3 rd party software packages such as nessus, nmap, Solar Winds, WebInspect, etc. |

| | |
|--|--|
| <i>Company Name</i> | <i>Union Center National Bank</i> |
| <i>Contact name</i> | Barbara Leibman |
| <i>Contact Phone Number and E-mail</i> | (908)206-2956 BLIEBMAN@ucnb.com |
| <i>Project Dates, Duration and Value</i> | October 2002 – 2008 Duration: 20 days / year Project Value: \$40K |
| <i>Brief Description of Project</i> | Security Assessments, Security Product Implementation |
| <i>Staff Assigned</i> | Thomas Welch, Alex Solomonovic, Michael Welch |
| <i>Consultants Role</i> | The consultants assigned to this project conducted information security assessments, which included a review of the clients compliance with the GLB Act. The assessment included a review of administrative, physical and technical controls. The technical review required the use of a number of 3 rd party software packages such as nessus, nmap, Solar Winds, WebInspect, etc. |

| | |
|--|--|
| <i>Company Name</i> | <i>McDonald Information Services</i> |
| <i>Contact name</i> | Rich Rager |
| <i>Contact Phone Number and E-mail</i> | (201)659-2600 rich@callmis.com |
| <i>Project Dates, Duration and Value</i> | June 2005 – Current Duration: 30 days (conducted annually) Project Value: \$60K |
| <i>Brief Description of Project</i> | Policy Development, Security Assessments and PCI/ISO Reviews, Vendor Selection Assistance |
| <i>Staff Assigned</i> | Thomas Welch, Alex Solomonovic |
| <i>Consultants Role</i> | The consultants assigned to this project conducted information security assessments, which included a review of the clients compliance with the Payment Card Industry Data Security Standard (PCI DSS) and the ISO 27002 standard. This included a review of administrative, physical and technical controls. The technical review required the use of a number of 3 rd party software packages such as nessus, nmap, Solar Winds, WebInspect, etc. |

SECTION 4
OTHER DOCUMENTS

[PAGE INTENTIONALLY LEFT BLANK]

APPENDIX A
RESUMES

[PAGE INTENTIONALLY LEFT BLANK]

THOMAS WELCH, CPP, CISSP

PROFILE

Mr. Welch has over twenty-five years in the Information Systems business, ten of which he was directly responsible for the design and development of Public Safety related applications. Mr. Welch serves as Chief Executive Officer for Bullzi Security, an information security outsourcing and consulting firm. Mr. Welch has also served as a private investigator and information security consultant since 1988 and was President and CEO of Technological Investigative Services. Mr. Welch served as CIO of Paradigm4, a wireless systems integration company for three years. Prior to his career in the Information Systems business, Mr. Welch was a Crime Analyst for the City of Orange, New Jersey and a Public Safety Officer (cross-trained Police Officer and Firefighter) for the City of Coconut Creek, Florida. He attended Florida Atlantic University and has advanced training in computer crime investigations and computer forensics. Mr. Welch is a Certified Information System Security Professional (CISSP) and Certified Protection Professional (CPP). Mr. Welch is an author and frequent lecturer on computer security topics, including computer crime investigation and computer forensics.

Experience

Bullzi Security, Inc., 801 International Parkway, Suite 500, Lake Mary, Florida 32746, serves as Chief Executive Officer from September 4, 2001 to present. Responsibilities include running a professional services organization that provides end-to-end information security solutions for, both, government and corporate clients. Services include preventive measures such as Information Security policy creation, security training, secure architecture design, security assessments including vulnerability analysis and penetration testing, implementation of security products such as firewalls, PKI, two-factor authentication, intrusion detection systems, kernel hardening, managed security services, etc.

JAWZ Inc., 353C Route 46 West, Fairfield, New Jersey 07004, served as Vice President – Enterprise Security Solutions from January 1, 2000 to August 31, 2001. Responsibilities included business development for major client relationships such as Bullzi Security, Intermedia, HP, Bell Canada (and subsidiaries), etc. Prior to his move to business development, Mr. Welch served as VP – Global Security Group, where he was responsible for managing a group of 60 information security professionals that provided end-to-end information security solutions for, both, government and corporate clients. Services included preventive measures such as Information Security policy creation, secure architecture design, security assessments including vulnerability analysis and penetration testing, implementation of security products such as firewalls, PKI, two-factor authentication, intrusion detection systems, kernel hardening, managed security services, etc. In addition to these preventive services, Mr. Welch's group provided Computer Incident Response Team (CIRT) response, high-tech crime investigations, computer forensics, and training.

Secure Data Technologies Corporation., 353C Route 46 West, Fairfield, New Jersey 07004, served as Chief Executive Office from January 1, 1999 to December 31, 1999, at which time the company was purchased by JAWS Technologies Inc. Mr. Welch was principal and founder of Secure Data Technologies Corp., an information security outsourcing and consulting company. Secure Data Technologies Corp also provided investigative services, computer forensics, and high-tech crime training.

Paradigm4, Inc., 363 Route 46 West, Fairfield, New Jersey 07004, served as Senior Vice President and CIO from January 1, 1996 to June 1, 1998. Mr. Welch is also a principal in Paradigm4, Inc., a wireless systems integration company. He was responsible for the company's overall technical architecture, which included the design, development and implementation of all wireless networking components. Mr. Welch was also responsible for all corporate security, including physical and information security.

Welch and Welch Investigations, Inc., P.O. Box 95, Glenwood, New Jersey 07418, served as President and CEO from June 8, 1988 to present. Primary duties involve civil/criminal investigations with an emphasis on computer crime investigations and computer forensics, consulting related to information security and law enforcement automation; and education and training related to information security and computer crime investigations. Mr. Welch consults to the business community and law enforcement groups on system analysis, design and planning; system vulnerabilities and security deficiencies; internal computer crime investigations.

SI3, Inc., 271 Route 46 West, Suite F109, Fairfield, New Jersey 07004, served as Vice President of Operations (50% Owner) from June 1989 to February 1993. Mr. Welch was principally responsible for development of all application software. Primary duties included the management of both the organization and customer-based projects. SI3 specialized in the design and development of Command and Control computer systems for government. This included Computer-Aided Dispatching (StateD), Records Management, and Message Switching applications. Mr. Welch managed a staff of eighteen (18) programmers, technicians and marketing support representatives, in addition to over twenty major projects.

Mr. Welch was directly responsible for company and Project-based security, which included designing major Command and Control systems that were required to run 24 hours/day, seven days/week, with no down time. This included the use of distributed, fault-tolerant and/or remote hot-standby systems. Contingency planning was one of the most crucial aspects of the system design. Part of the overall design included advanced communications networks to provide the linkage between the distributed systems. Mr. Welch was responsible for securing these networks, by using Access Control Security, encryption, dial-back modem devices, and Caller-ID verification. Mr. Welch is also familiar with other physical security measures, such as TEMPEST and Biometrics. Since many of these Command and Control systems had access to other highly secure networks, such as the National Crime Information Center, Mr. Welch was required to design and implement application level security, which would control and/or limit user access to various levels of the system.

Mr. Welch left SI3, Inc. in February 1993, when he sold the company to Systemhouse, Inc.

Computil Corp., 1040 Route 46 West, Clifton, New Jersey, served as Director of Operations from February 1988 to June 1989. Primary duties included the analysis, design, coding for Command and Control systems and included the supervision and management of ten (10) programmers and technicians. (See duties identified under SI3, Inc.)

Compu-Key Corp., 376 Hollywood Ave., Fairfield, New Jersey, served as Program Manager from August 1986 to February 1988. Primary duties included the analysis, design, coding for Command and Control systems. These duties included the supervision and management of two programmers and two technicians. (See duties identified under SI3, Inc.)

City of Orange Police Department, Orange Police Department, Orange, New Jersey, served as Crime Analyst from August 1985 to May 1986. Primary duties included the analysis of raw data to create Crime Trend Analysis and Distribution Analysis Reports. Additional duties consisted of designing a PC-based system to automate the crime analysis functions, in addition to leading an in-house Committee in the selection of a computer system for Dispatch Operations and Records Management.

City of Coconut Creek Police Department, Coconut Creek Municipal Center, Lyons Road, Coconut Creek, Florida, served as a Police Officer for the Coconut Creek Public Safety Department from July 1982 to November 1984. Conducted preliminary investigations of all criminal acts, including homicide, thefts, frauds, and other problems involving security.
Citations - Meritorious Police Duty, 1984.

Major Achievements

- Author of the Computer Crime Investigation and Computer Forensics chapter of Auerbach's Handbook of Information Security Management.
- Author of the TIS's Computer-based training (CBT) on Computer Crime Investigation and Computer Forensics. This is a 100-hour, self-paced course highlighting issues that deal with CIRT, high-tech crime investigations and computer forensics.
- Designed a secure environment for the Kansas Bureau of Investigation (KBI) – Criminal Justice network. This solution included a number of information security mechanisms, such as firewalls, IDS, two-factor authentication, policy development and awareness training. The KBI is the first state in the United States to use the Internet to transmit criminal justice data to the FBI. This design received FBI approval in August 1998.
- Lead designer for the New York City E9-1-1/StateD System
- Major speaking engagements, presentations and tutorials:
 - ✓ Testified as an expert on hacking and computer security before the New Jersey State Commission of Investigation – Computer Crime Hearings (1999)
 - ✓ Sea Girt Police Academy - Computer Crime Investigation
 - ✓ Technology for Information Security Conference (TISC) '97 – Computer Forensics and Investigation
 - ✓ Technology for Information Security Conference (TISC) '96 – Computer Crime Investigations Workshop
 - ✓ Somerset County Police Academy – Computer Seizure and Analysis
 - ✓ Mid-Atlantic and Great Lake Organized Crime and Law Enforcement Network (MAGLOCLEN) – Internet Crime and Underground Bulletin Boards
 - ✓ Network Security '96 – Computer Crime: Investigative Techniques
 - ✓ CSI '95 Annual Security Conference – Computer Crime Investigation
- Conducted security assessments for major corporations and governmental agencies that included business level risk assessments which includes technical assessments of the clients architecture (i.e. vulnerability scans, attack and penetration, etc.), policy development, awareness training and the implementation of security products.
- Managed the design and development of the New York City Fire Departments second generation StateD system - STARFIRE II.
- Original author of SI3's Computer-Aided Dispatch and Records Management system, which is currently installed in over fifteen (15) Police and Fire agencies, including the City of Newark.
- Co-designer of the first, secure law enforcement network that permitted CJIS transactions over the Internet. This design, which included firewalls, virtual private networks, intelligent intrusion detection systems, and several levels of authentication, culminated in a report that was submitted to the FBI and later approved.
- Designed and installed an Agent Tracking System for the New York Operations of the Federal Bureau of Investigations.
- Spearheaded the software development effort for the City of Newark "Scofflaw" project, using the Motorola hand-held terminals and the Motorola Data Radio Network.
- Designed and installed an integrated networking switch to the National Crime Information Center and the Department of Motor Vehicles, utilizing Stratus Fault Tolerant hardware.

Information Systems Expertise

Mr. Welch's experience with various hardware platforms include:

- PC, HP 9000, Sun Ultra, Stratus, IBM RS/6000, DG AViiON, DEC 5000/240, Convergent Technologies B38 NGEN, Unisys A3, Unisys B1990, and IBM System 36

Mr. Welch's experience with various software includes:

- MS Windows (3.1, 95, 98, NT), UNIX, VOS, MS-DOS, BTOS/CTOS, X-Windows(Motif), "C", C++, Pascal, Fortran, LINK (4GL), Forte`
- Informix, Oracle, Ingres, Sybase, ISAM

Mr. Welch's experience with various information security products includes:

- Check Point firewalls, Entrust, EnCase, Expert Witness, Coroners Toolkit, Axent Security Suite, ActivCard, F-Secure, Security Dynamics SecurID, ISS Security Suite (IDS and Scanning Tools), Tripwire, nmap

Mr. Welch's experience with computer-based security systems include:

- UNIX and NT O/S Security (Access Control, File Management and Auditing), Kerberos, RSA Encryption, Firewalls, various virus detection and mitigation applications, PC Access, NTP, SATAN, Tripwire, COPS, Cracker

Education

Broward Community College, Coconut Creek, Florida, 1984. Associate of Arts (AA).

Florida Atlantic University, Boca Raton, Florida, 1985. Major - Computer Science.

Certificate of Compliance in Law Enforcement, State of Florida, Criminal Justice Standards and Training (Police Academy - 1982).

Academic Honors - graduated first in academy class.

Specialized Law Enforcement Courses and Seminars:

Line Supervision for Law Enforcement Officers

Progressive Patrol Administration

Executive/VIP Protection Course

Investigative Technology Course

Credit Card Fraud Investigation Course

Criminal History Records Seminar

Fingerprint Techniques

Computer Security

Licenses and Certifications

New Jersey Private Investigator License (1988)

Florida Private Detective License (1988)

New York State Private Investigator License (1995)

Certified Protection Professional (CPP) - 1995

Certified Information Systems Security Professional (CISSP) – 1996

Certified Fraud Investigator (CFI) – 1998

Certified Checkpoint Security Engineer (CCSE) – 1998

Certified Checkpoint Security Administrator (CCSA) – 1998

ALEX SOLOMONOVIC, CISSP

PROFILE

Mr. Solomonovic has over twelve years of experience in information technology. During the last six years, he has focused on large integration projects, and secure network design and development of full scale Managed Security Services.

Experience

Bullzi Security, Inc., 801 International Parkway, Suite 500, Lake Mary, Florida 32746, serves as Director of Security Technology from September 4, 2001 to present. Responsible for security technology evaluation, recommendation and integration as well as the company's technical architecture, products, and service capabilities both internally and externally. Also, responsible for secure network design solutions and network architecture reviews.

JAWZ Inc., 353C Route 46 West, Fairfield, New Jersey 07004, served as Director, Security Architecture from January 1, 2000 to August 31, 2001. Responsibilities included designed, implemented and managed JAWZ Managed Security Services operation based at Fairfield, NJ office, CheckPoint FW-1/VPN-1 turnkey solution for the client, consulting and support, ISS RS 3.2 & 5.x fully managed solution, 24/7 monitoring and reporting, pre-sales support of high profile security projects (involving Fortune 100 clients) regarding network security review and secure network design using best known practices and best of breed security products.

Secure Data Technologies Corp., 353C Route 46 West, Fairfield, New Jersey 07004, served as Director, Information Security from January 1, 1999 to December 31, 1999. Responsibilities included implementation of network security products based on customer security requirements: CheckPoint VPN-1 (on NT and Nokia IPSO platforms), Entrust PKI, ActivCard Server (token & smartcard authentication). Working closely with customers on improving their LAN/WAN design and recommending and specifying products and equipment to secure and upgrade existing or design & install new networks.

Paradigm4, Inc., 363 Route 46 West, Fairfield, New Jersey 07004, served as Information Security Officer from December 9, 1996 to December 31, 1998. Responsibilities included administration of multi-domain NT 4.0 LAN/WAN environment and supporting 150+ internal users and providing II and III level of support for customers. Managing CheckPoint 3.0b/4.0 FW-1 firewalls. Managing Netscape Mail Server 3.6 for NT with 150+ users, Tally auditing system, ELRON-Internet Manager monitoring application. Designed and implemented security policy for entire company at multiple locations including testing for user & system compliance with the policy. Participated on various projects in designing secure network solution for customers. Overlooked network and physical security for entire company in multiple geographical locations.

Significant Projects

General Electric – GEIS/GEIO, Gaithersburg, MD (2000)

Over the period of six months, provided security consulting on a wide variety of topics and issues, attendance of hundreds of internal process, design and readiness review meetings, assisted GEIS System Integrity group with Windows NT related security issues, Nokia 440/650 Firewall appliance support and assistance in redesigning CheckPoint FW-1/VPN-1 implementation and consolidation of the rulebases, ISS Real Secure 3.2/5.0 IDS system design and initial rollout. Delivered internal IDS ISS RS training for GEIS System Integrity, Firewall Security groups and members of GE Europe System Integrity Team.

Township of Union, NJ - Network Security Integration (1999)

Performed complete assessment of 150+ node network in multiple departments/locations. Presented detailed report, including recommendations for security policy development and general network upgrades, security awareness training, physical security and access control, PC H/W and network infrastructure upgrade. After report acceptance implemented security policy changes, specified, ordered, installed and configured new computer room equipment. Reviewed and corrected security settings and permissions, verified that latest patches, service packs and drivers are installed; performed software compliance audit, unified naming conventions for users and organization units, reorganized file/directory structure in entire network. Established strong password requirements. Standardized on NT 4.0 WS OS on client side, installed and integrated CheckPoint/Nokia VPN-1 (RL50) firewall appliance into existing layout and configured WWW and Imail servers on DMZ.

State of Kansas - KBI (1998)

Together with other two members of Paradigm4 information security team, designed the solution that complies with current FBI policy that states that federal criminal information cannot be transmitted over the Internet, unless the state can provide sufficient assurances that adequate security is in place to safeguard the data. Paradigm4 developed and implemented CJIS applications and message switches to make KBI NCIC2000 compliant. This design effort, which included the development of a secure architecture, virtual private networks, firewalls, intelligent network intrusion detection and several levels of authentication, resulted in a report that was submitted to the FBI and later approved. This paved the way to send the first law enforcement transactions over the Internet in the history of the FBI.

City of New York - CityTime Project (1997-98)

Responsible for network security design and integration of multiple departmental LANs into WAN environment with connection to project vendors extranet as a part of ongoing project that includes redesign and integration of the whole City of New York Office of Payroll Administration network.

Information Systems Expertise

- Network security design and architecture, including design and implementation of CheckPoint FW systems, IIS RS 3.2 and 5.x IDS systems, VPN solutions, designing company security policies, firewall rule base.
- Installation and "hardening" NT 3.51/4.0 Server as a preparation to install WWW, FTP or Email server applications on DMZ network segment.
- In depth knowledge of DOS, Windows9X, MS Office 97/2000, NT 4.0 Workstation, NT 4.0 Server administration, RAS.
- Network design and testing (TCP/IP, SMTP, POP3, FTP, TELNET, DNS, RIP, Ethernet, Fast Ethernet, manageable hubs/switches, RAID, DAT, DLT, UPS).
- Installation and configuration of Cisco Fast Ethernet Catalyst 2924XL switches, 1600 & 1700 Cisco routers and Proteon GT series routers.
- Basic knowledge of Solaris 2.6 and BSD UNIX required for CP FW-1 and VPN-1 installation, configuration and maintenance.
- Extensive hardware experience with PCs and peripherals, incl. notebooks, MDC units, analog and CDPD modems.

Installation, configuration, management and maintenance of tools and applications:

- CheckPoint FW-1/VPN-1 on NT 4.0, IPSO (Nokia) platform and Intrusion.Com appliance
- ISS Internet Scanner 6.X & ISS RS 3.2 and 5.x network/OS/Server Sensor and WS MGMT.
- ELRON Internet Manager 4.X & Tally Systems.
- Netscape Messaging Server 3.6, MS Exchange 5.5, IPSwitch-Imail Server 5.7/6.1, MS IIS 4.0, PC AW 8.0/9.0.

- Entrust Enterprise PKI 4.0 and ActivCard 3.1 server on NT platform
- Visio Professional/Enterprise 5.0 & 2000
- Tripwire HQ 1.0 and Connector 1.0

Training, Certifications and Memberships

TechLink - Windows NT 4.0 Administration (March 1997)
CSI - Windows NT Security (June 1997)
OpenRoute Networks - Proteon GT Router configuration course (Apr. 1998)
CSI - Advanced Windows NT Security (Aug. 1998)
CSI - Comprehensive Intrusion Detection (Aug. 1998)
CheckPoint - CCSA, CCSE 3.0b (Sept. 1998)
Certified Entrust PKI 4.0 Administrator & Engineer (July 1999)
Nokia FW – HA VRRP & Nokia Security Administrator (March 2000)
Certified ISS Database, Internet Scanner 6.X & ISS RealSecure 3.2 Engineer – ICE (April 2000)
Cisco Certified Network Associate - CCNA (February 2001)
CheckPoint Certified Security Administrator – CCSA2000 (March 2001)
Member of Computer Security Institute (1996-present)

MICHAEL WELCH, CISSP, CISM

PROFILE

Mr. Welch has over eleven years in the Information Security business. Mr. Welch has conducted over 100 security architecture reviews, Business Risk Assessments (Gap Analysis), attack and penetration tests, network and host assessments and firewall reviews. Mr. Welch has implemented firewalls, intrusion detection systems and file integrity systems into network infrastructures. Mr. Welch has reviewed and developed security policies and procedures to ensure that they followed industry best practices, as well as, assisted in the development of a HIPAA Compliance program. Mr. Welch has been responsible for full project life cycle of security architecture reviews, penetration assessments, and Business Risk Assessments. Mr. Welch has been involved in creating Security Best Practices Baselines for various technologies which include: Windows NT4, Windows 2000 (Professional and Server), Internet Information Server 4 and 5, Solaris 8, Linux 7, Checkpoint Firewall on NT4 and Solaris, and Apache Web Server. Mr. Welch has conducted security awareness training; created an advanced hacking course; developed a Computer Based Training course on Computer Crime Investigations and Forensics; and assisted in training security consultants in performing Business Risk Assessments.

Experience

Bullzi Security, Inc. 801 International Parkway, Suite 500, Lake Mary, Florida 32746, serves as Director of Risk Management from January 1st, 2002 to Present. Responsibilities include developing and maintaining the risk management division of Bullzi Security. The prime focus will be on Business Risk Assessments focused on HIPAA and GLB compliance, following the Common Criteria and BS7799 guidelines to help organizations mitigate risk to an acceptable level. Mr. Welch other areas of focus will be on Attack and Penetration, Vulnerability Assessments, and Fraud Detection and Prevention.

Vigilinx, 53 Wateview Boulevard, Parsippany, New Jersey, served as Manger of Risk Assessments from April 15th 2001 to December 31st, 2001. Managed and conducted Business Security Assessments and Attack & Penetration Tests. Business Security Assessments were geared to identify mission critical assets and mitigate risk to an acceptable level. This was done through interviews, policy and procedure reviews, walk-troughs and checklists. The Attack & Penetration Tests were focused on Application Assessment, Infrastructure Assessment and System Configurations to help customers to lower their risk to an acceptable level.

JAWZ Inc., 353C Route 46 West, Fairfield, New Jersey 07004, served as Senior Security Consultant from January 1, 2000 to April 14th, 2001. Responsibilities included supporting internal and external JAWZ clients globally. Conducted security architecture reviews, attack and penetration testing, network and host assessments; all phases of secure network architecture (design, implementation, testing). Integrated network equipment; such as firewalls (Checkpoint) and IDS systems (ISS Real Secure and Black Ice) into client networks.

Responsibilities included writing proposals and reports for clients, briefing clients on status of project and at the end of an assessment. Use MS Project for project management. Other duties included:

- Participated in the development of Advanced Hacking Course, which will be given at the University of Calgary. Designated as one of three instructors that will be teaching the course.
- Assisted in the development of an out-of-band logging server for JAWZ. Exported logs from firewalls, IDS systems and production servers.
- Assisted in development of JAWZ HIPAA Compliance program.
- Conducted GAP Analysis Assessments for Financial, Health, and Telecommunication Industries.
- Attended information security conferences (Blackhat, DefCon, SANs, and InfoSec World) to stay current with security topics.
- Represented JAWZ at trade shows/expos to demo hacking techniques and assist in pre-sales (Techno Security, NLETS, ASPcon).

- Secured NT, Linux and Solaris Servers for both internal and external clients using industry standard and best practices.

Secure Data Technologies Corporation, 353C Route 46 West, Fairfield, New Jersey 07004, served as E-commerce Manager from January 1, 1999 to December 31, 1999. Developed and maintained a 100-hour computer based training course on computer forensics and investigations. This course was designed for law enforcement and corporate security personnel and developed using Quest.

Other responsibilities for clients included:

- Maintained and administered internet/intranet sites.
- Administered mail servers and DNS servers.
- Performed security assessments onsite and remotely for customers.

Paradigm4, Inc., 363 Route 46 West, Fairfield, New Jersey 07004, served as Computer Programmer from January 1, 1997 to December 31st, 1998. Developed and maintained installation scripts using Install Shield for Paradigm4 client software. Lead developer of Computer Based Training for Kansas Bureau of Investigations and Florida Department of Law Enforcement on NCIC 2000. Trained end users of each organization on functionality of Computer Based Training. Assisted in the design of the Paradigm4 Accident Reporting System using Protogen and Visual Basic.

International Museum of Cartoon Art, Boca Raton, Florida, served as Operations Manager from April 1996 to December 31st, 1996. Responsibilities included the physical and operational security for museum. Worked with law enforcement and museum management in order to protect the multi-million dollar art as well as the visitors to the museum

Welch and Welch Investigations, 13 Stone Ridge Road, Vernon, New Jersey, servers as Intern Investigator from March 15th, 1993 to present. Responsibilities include the development of computer based trained on forensics and investigations.

Major Achievements

- Co-Author of the TIS's Computer-based training (CBT) on Computer Crime Investigation and Computer Forensics. This is a 100-hour, self-paced course highlighting issues that deal with CIRT, high-tech crime investigations and computer forensics.
- Conducted security assessments for major corporations and governmental agencies that included business level risk assessments which include technical assessments of the client's architecture (i.e. vulnerability scans, attack and penetration, etc.), policy development, awareness training and the implementation of security products.

Information Systems Expertise

Mr. Welch's experience with various hardware platforms include:

- Windows family (NT, WIN2K, 3.1, 95, 98), Solaris, Linux (Redhat)

Mr. Welch's experience with various information security assessment products includes:

- AppScan, WebInspect, Core Impact, ISS Internet Scanner, Database Scanner, Retina, Nessus, Enterprise Security Manager, Cerberus Internet Scanner, Network Associates Cybercop Scanner, Axent NetProwler, and various other freeware scanning utilities (nmap, whisker, iscan), L0pht Crack, SuperScan, Solarwinds, Web Cracker, Grinder, Legion, Ogre, Somarsoft, Visual Route, Teleport Pro, Black Widow, NT Admin Toolkit, Expert Witness, Sam Spade, Achilles
-

Mr. Welch's experience with various information security products includes:

- Check Point firewalls, Entrust, EnCase, Expert Witness, Coroners Toolkit, Axent Security Suite, ActivCard, F-Secure, RSA SecurID, ISS Security Suite (IDS and Scanning Tools), Snort, Tripwire, nmap

Mr. Welch's experience with computer-based security systems include:

- UNIX and NT O/S Security (Access Control, File Management and Auditing), Kerberos, RSA Encryption, Firewalls, various virus detection and mitigation applications, PC Access, NTP, SATAN, Tripwire, COPS, Cracker

Education

Utica College, NY. Economic Crime Management (04). Working on Masters Degree
George Washing University, Washington D.C., 1996. Major – BA - Criminal Justice.

Certifications

Certified Information Security Manager (CISM) - 2003
Certified Information Systems Security Professional (CISSP) – 2001
InfoSec Assessment Methodology (NSA) - 2000
Certified Checkpoint Security Administrator (CCSA) – 2000
Tripwire Certified – 2000

Memberships

International Information Systems Security Certification Consortium
American Society of Industrial Security
The Information Systems Audit and Control Association and Foundation
Association of Certified Fraud Examiners
Information Systems Security Association
High Technology Crime Investigation Association
Infraguard

ADDENDUM ACKNOWLEDGMENT

REQUISITION No.: ITECH10

I HEREBY ACKNOWLEDGE RECEIPT OF THE FOLLOWING CHECKED ADDENDUM(S) AND HAVE MADE THE NECESSARY REVISIONS TO MY PROPOSAL, PLAN AND/OR SPECIFICATIONS, ETC.

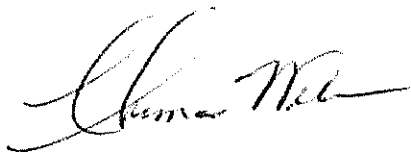
ADDENDUM NO'S:

- No.1 DATED DECEMBER 14, 2009
- No.2 DATED DECEMBER 29, 2009
- No.3 DATED JANUARY 11, 2009

I UNDERSTAND THAT FAILURE TO CONFIRM THE RECEIPT OF THE ADDENDUM(S) MAY BE CAUSE FOR REJECTION OF BIDS.

BULLZI SECURITY UNDERSTANDS THAT ANY VERBAL REPRESENTATION MADE OR ASSUMED TO BE MADE DURING ANY ORAL DISCUSSION HELD BETWEEN BULLZI SECURITY REPRESENTATIVES AND ANY STATE PERSONNEL IS NOT BINDING. IT IS FULLY UNDERSTOOD THAT ONLY THE INFORMATION ISSUED IN WRITING AND ADDED TO THE SPECIFICATIONS BY AN OFFICIAL ADDENDUM IS BINDING.

By: BULLZI SECURITY, INC



Thomas Welch, President and CEO

Dated: January 19, 2010



Proposal for
Statewide Contract for Technical Services
RFQ No.: ITECH10

Prepared for:

State of West Virginia
Department of Administration
Purchasing Division
Building 15
2019 Washington Street East
Charleston, WV 25305-0130

January 10, 2010
(Version 1)

Prepared by:

Bullzi Security, Inc.
801 International Parkway
Suite 500
Lake Mary, Florida 32746

RECEIVED

2010 JAN 12 PM 1:29

WV PURCHASING
DIVISION

This proposal or quotation includes data that shall not be disclosed outside the State of West Virginia ("State"), and shall not be duplicated, used, or disclosed — in whole or in part — for any purpose other than to evaluate this proposal or quotation. If, however, a contract is awarded to this offeror or quoter as a result of — or in connection with — the submission of this document, the State shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the State's right to use information contained in this document if it is obtained from another source without restriction. The data subject to this restriction is contained in all sheets.

© 2010 by Bullzi Security Inc. All rights reserved.

Statement of Confidentiality and Validity

Bullzi Security Inc. has prepared this document for the sole purpose and exclusive use of the State of West Virginia. Due to the confidential nature of the material in this proposal, Bullzi Security requests this document and its contents not be discussed, disclosed, or divulged without the prior written consent of Bullzi Security.

Copyright Notice

This document is proprietary and does not exist in the public domain. This copyright notice is attached only to provide protection in the event of inadvertent publication. No part of this publication may be copied without the express written permission of Bullzi Security.

Copyright © 2010 Bullzi Security, Inc.
All rights reserved.



COVER LETTER

Bullzi Security, Inc.
801 International Parkway
Suite 501
Lake Mary, Florida 32746

January 10, 2010

State of West Virginia
Department of Administration
Purchasing Division
Building 15
2019 Washington Street East
Charleston, WV 25305-0130

Re: Statewide Contract for Technical Services
RFQ No.: ITECH10

To Whom It May Concern:

Bullzi Security, Inc. is pleased to submit this bid to the State of West Virginia for the Statewide Contract for Technical Services (RFQ No.: ITECH10). Thomas Welch will be the primary contact to speak on behalf of Bullzi Security.

Contact Information: Thomas Welch
Tel: (407)562-1864
Cell: (973)809-5509
Fax: (407)562-2001
e-mail: twelch@bullzisecurity.com

Bullzi Security meets or exceeds all of the mandatory requirements of this RFQ. If you have any questions, please do not hesitate to contact me. We look forward to working with the State of West Virginia.

Sincerely,

Thomas Welch
President and CEO



TABLE OF CONTENTS

| | |
|--|----|
| <i>Cover Letter</i> | 3 |
| <i>Table of Contents</i> | 4 |
| <i>Section I</i> | 5 |
| <i>Corporate Description</i> | 5 |
| <i>Section II</i> | 8 |
| <i>Qualifications and Experience of the Company</i> | 8 |
| <i>Supplemental Staffing for</i> | 8 |
| <i>Computer Systems and Network Security</i> | 8 |
| 2.1 Experience..... | 8 |
| 2.2 Resumes..... | 9 |
| 2.3 References..... | 10 |
| <i>Section III</i> | 11 |
| <i>Qualifications and Experience of the Company</i> | 11 |
| <i>Attachment 4</i> | 11 |
| <i>Internet/Intranet and Electronic Commerce Security Development and Implementation</i> | 11 |
| 3.1 Experience..... | 11 |
| 3.2 Certifications..... | 13 |
| 3.3 Resumes..... | 14 |
| 3.4 References..... | 15 |
| <i>Section 4</i> | 16 |
| <i>Other Documents</i> | 16 |
| <i>Appendix A</i> | 17 |
| <i>Resumes</i> | 17 |
| <i>Appendix B</i> | 28 |
| <i>Addendum Acknowledgment</i> | 28 |

SECTION I
CORPORATE DESCRIPTION

- 1) Bullzi Security, Inc.
801 International Parkway
Suite 500
Lake Mary, Florida 32746
Contact Number: (407)562-1864
Fax Number: (407)562-2001

Federal ID Number: 20-1840083

Website: www.bullzisecurity.com
www.sendsecure.com
www.wiselearningsolutions.com

- 2) Contact Name: Thomas Welch
P.O. Box 11398
Southport, NC 28461
Contact Number: (973)809-5509

- 3) The Company was formed on Oct. 25, 2004, as the merger of Welch and Welch Investigations, Inc. (formed in June 1988), Secure Enterprise Software, Inc. (formed in June 2002) and WISE Learning Solutions, Inc. (formed in 2004). On January 1, 2006, the company had 7 full-time employees. Today, we have over 30 employees and contractors.

- 4) Company History

Bullzi Security is an information security consulting and education company with operations in Florida, North Carolina and New Jersey. Bullzi Security's administration will be coordinated out of our Lake Mary, Florida office, while routine company management will be coordinated by service line managers who meet regularly to ensure efficient resource utilization.

Bullzi Security provides the information security consulting services, such as security assessments, penetration testing, regulatory compliance programs, policy development and security mitigation measures. The information that is possessed by companies today, is their greatest asset, and as we have seen lately, is subject to unauthorized access, breaches, loss of data, etc. The business world must be ready to protect this information and be prepared to detect and respond to cyber attacks. Bullzi Security conducts risk assessments or vulnerability testing of its client's information systems, providing an

analysis of the organization's vulnerabilities from a physical security, IT security, document security and personnel security prospective.

Bullzi Security will use proprietary techniques, based on industry standards (ISO-17799) as well as the most reliable, up-to-date automated security assessment tools, to generate security profiles of essential information systems. The vulnerability testing service focuses on the client's IT exposures. With the recent rash of breaches and unauthorized access that have made the news, along with federal mandates such as Healthcare Insurance Portability and Accountability Act (HIPAA); North American Electric Reliability Council (NERC); the Gramm-Leach-Bliley Act (GLBA) and the Sarbanes-Oxley Act (SOX), Bullzi Security is set to launch a marketing campaign focusing on the protection of one's information.

Figure 1, below, identifies the products and services that will be offered by Bullzi Security.

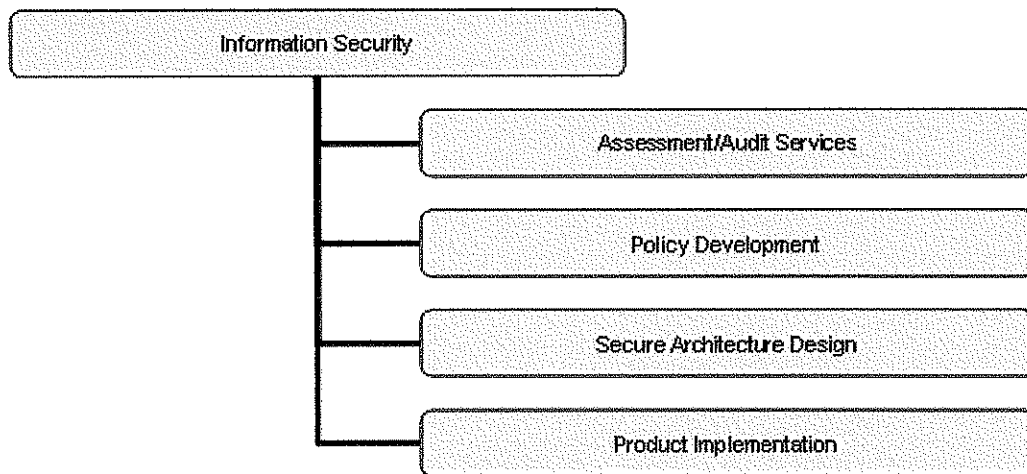


Figure 1 – Information Security Products and Services

In addition to its information security consulting business, Bullzi Security also provides security education services through its eLearning company, WISE Learning Solution LLC ("WISE"), which is a wholly-owned subsidiary of Bullzi Security, Inc.

WISE Learning Solutions LLC (WISE)

WISE Learning Solutions LLC (a Nevada limited liability company) is an eLearning company that was originally founded in October 2004 by Thomas W. Welch, Michael D. Welch and Michael H. Welch as WISE Learning Solutions, Inc. WISE, which is an acronym for Web-based Information Security Education, provides web-based security training solutions that use multimedia technology (e.g. audio, graphics, animation, video and text).

The WISE flagship product, Information Security Awareness, was designed to meet the mandated training requirements of many of today's regulatory programs, such as the

Healthcare Insurance Portability and Accountability Act (HIPAA); North American Electric Reliability Council (NERC); the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley Act (SOX) and others. The WISE courses were created due to a void in the industry for this type of training. Traditional classroom-based training simply is not scalable and is logistically difficult to implement.

The Information Security Awareness program is currently offered in five languages (English, French, Spanish, Brazilian Portuguese and Japanese). Other languages, such as Serbian and Chinese, are expected to be available in the second fiscal quarter of 2006. Italian, Russian and German are slated for release later this year.

The WISE Information Security Awareness program educates system users on the value of corporate assets, acceptable use of the Internet, how to handle e-mail attachments and forty-four other topics related to safe computing. In addition to awareness training, WISE has completed, or is in the process of completing, training programs that address privacy, secure coding practices, anti-money laundering, physical security, information security engineering, identity theft, computer forensics, and more.

Figure 2, below, identifies the products and services offered by WISE.

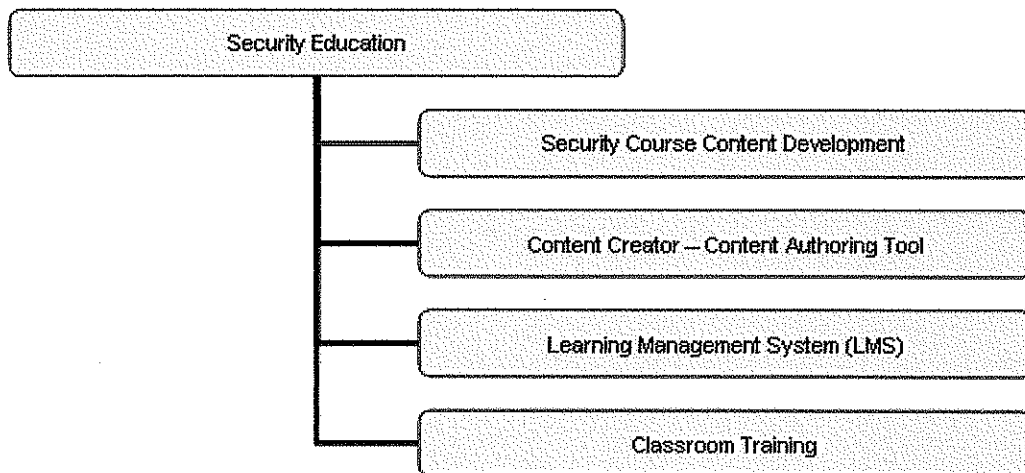


Figure 2 – Security Education Products and Services

SECTION II

QUALIFICATIONS AND EXPERIENCE OF THE COMPANY
SUPPLEMENTAL STAFFING FOR
COMPUTER SYSTEMS AND NETWORK SECURITY

Category: Computer Systems and Network Security

Description: Includes, but is not limited to; analysis, assessment, planning, firewalls, virtual private networks, design and review, virus, on all levels and all software platforms.

2.1 Experience

Providing information security and privacy services is well within the competencies of Bullzi Security. Through our consulting services and integrated delivery systems, Bullzi Security helps to minimize the threats to its clients' information systems and communication networks. Bullzi Security brings a unique set of skills and experience to ensure each client receives the most comprehensive, cost-effective information security services available. As an end-to-end information security solutions provider, Bullzi Security offers its clients the full breadth of information security products and services including:

- Information Security Consulting and Technology Planning
- Information Security Assessments and Audits
- Information Security and Privacy Policy Review and Development
- Information Security and Privacy Training and Awareness Programs
- Secure Architecture Design
- Security Products Implementation and Integration
- Managed Security Services (Firewalls and Intrusion Detection Systems)
- Computer Incident Response Team (CIRT) w/24 Hour Rapid Response
- Investigative and Forensic Services

Bullzi Security is an expert in the information security field. We have the experience, expertise, credentials, and professionalism to meet or exceed the expectations of the State. The Bullzi Security team has been working together for the past ten years. The team of professional security consultants has conducted hundreds of assessments for our clients, from various industry segments, such as government, higher education, healthcare, banking and finance, Fortune 500 companies, etc.

2.2 Resumes

The security engineers on the Bullzi Security team, identified in Table 3.3-1, have come from numerous areas within the Information Technology (IT) industry, such as system administration, network administration, programming, investigation and forensic analysis. Only qualified, senior level security engineers will be assigned to this engagement. The resumes for the engineers that will be assigned to this project can be found in Appendix A.

| Task | Company | Name |
|--------------------------------------|-----------------|------------------|
| Security assessments (web-based) | Bullzi Security | Michael Welch |
| Security assessments (network-based) | Bullzi Security | Alex Solomonovic |
| Risk and Security Management | Bullzi Security | Thomas Welch |

Table 2.2-1 Project Staffing Table

As a security company whose reputation is based on its clients' trust, Bullzi Security recognizes the importance of fostering that trust. One of the key ways in which Bullzi Security does this is by going through extraordinary lengths to ensure that it hires only the best people, with trustworthy backgrounds. Each and every security consultant is required to go through an extensive background check as a condition of employment. The background check consists of the following:

- Civil Litigation, includes lawsuits past, present and ongoing
- Criminal Background check via National Crime Information Computer
- Credit check via the Credit Bureau

Additionally, each security engineer signs a company Non-disclosure agreement (NDA) stating that he/she will not divulge information learned about a particular client. Once the project is complete, Bullzi Security burns a copy of the report on CD. Once the State confirms receipt of a readable copy of the CD, the assessment information is deleted from the Bullzi Security systems.

2.3 References

| | |
|--|---|
| <i>Company Name</i> | <i>West Virginia Health Care Authority</i> |
| <i>Contact Name</i> | John Grey |
| <i>Contact Phone Number and E-mail</i> | (304) 348-2250 jgrey@hcawv.org |
| <i>Project Dates, Duration and Value</i> | First Assessment: 2002 Duration: 19 days Project Value: \$42K Follow-up Assessment: 2004 Duration: 5 days Project Value: \$12K |
| <i>Brief Description of Project</i> | Security Assessments, HIPAA Assessment and ISO 17799 Review |
| <i>Staff Assigned</i> | Thomas Welch, Alex Solomonovic, Michael Welch |

| | |
|--|---|
| <i>Company Name</i> | <i>Union Center National Bank</i> |
| <i>Contact name</i> | Barbara Leibman |
| <i>Contact Phone Number and E-mail</i> | (908)206-2956 BLIEBMAN@ucnb.com |
| <i>Project Dates, Duration and Value</i> | October 2002 – 2008 Duration: 20 days / year Project Value: \$40K |
| <i>Brief Description of Project</i> | Security Assessments, Security Product Implementation |
| <i>Staff Assigned</i> | Thomas Welch, Alex Solomonovic, Michael Welch |

| | |
|--|--|
| <i>Company Name</i> | <i>McDonald Information Services</i> |
| <i>Contact name</i> | Rich Rager |
| <i>Contact Phone Number and E-mail</i> | (201)659-2600 rich@callmis.com |
| <i>Project Dates, Duration and Value</i> | June 2005 – Current Duration: 30 days Project Value: \$60K |
| <i>Brief Description of Project</i> | Policy Development, Security Assessments and ISO Reviews, Vendor Selection |
| <i>Staff Assigned</i> | Thomas Welch, Alex Solomonovic |

SECTION III

QUALIFICATIONS AND EXPERIENCE OF THE COMPANY

ATTACHMENT 4

**INTERNET/INTRANET AND ELECTRONIC COMMERCE SECURITY DEVELOPMENT
AND IMPLEMENTATION**

3.1 Experience

Providing information security and privacy services is well within the competencies of Bullzi Security. Through our consulting services and integrated delivery systems, Bullzi Security helps to minimize the threats to its clients' information systems and communication networks. Bullzi Security brings a unique set of skills and experience to ensure each client receives the most comprehensive, cost-effective information security services available. As an end-to-end information security solutions provider, Bullzi Security offers its clients the full breadth of information security products and services including:

- Information Security Consulting and Technology Planning
- Information Security Assessments and Audits
- Information Security and Privacy Policy Review and Development
- Information Security and Privacy Training and Awareness Programs
- Secure Architecture Design
- Security Products Implementation and Integration
- Managed Security Services (Firewalls and Intrusion Detection Systems)
- Computer Incident Response Team (CIRT) w/24 Hour Rapid Response
- Investigative and Forensic Services

Bullzi Security is an expert in the information security field. We have the experience, expertise, credentials, and professionalism to meet or exceed the expectations of the State. The Bullzi Security team has been working together for the past ten years. The team of professional security consultants has conducted hundreds of assessments for our clients, from various industry segments, such as government, higher education, healthcare, banking and finance, Fortune 500 companies, etc.

From the perspective of a large project in the government sector, Bullzi Security' lead security consultant, Thomas Welch, designed the first public law enforcement network for the Kansas Bureau of Investigation (KBI). This was the first state in the United States to transmit National Crime Information Center (NCIC) and Central Criminal History (CCH) records across the Internet in a secure mode. The KBI replaced all 590 frame and point-to-point circuits, from all local and county agencies, with a Virtual Private Network

(VPN) over the Internet. Mr. Welch conducted the analysis and wrote the final Security Architecture Report, which ultimately resulted in FBI approval.

When conducting assessments, the Bullzi Security team follows the ISO 17799 and NIST security standards. From an assessment perspective, the Bullzi Security team has the experience and knowledge to conduct technology audits from a number of perspectives. This includes:

- Physical Security Audits
- Personnel Security Audits
- Documentation Reviews (Policy, Procedures, Standards, Topology Diagrams)
- Technical Assessments, including but not limited to:
 - External Penetration Testing
 - Internal Host and LAN Assessments
 - Application Assessments
 - Workstation Assessments
 - Wireless LAN Assessments
 - Firewall & Router Assessments

The Bullzi Security team has a number of key advantages over other companies. One of these advantages is our incident response and forensic experience. Based on our examination of various incidents and crime scenes, we are better able to help protect our clients' sites and identify hidden vulnerabilities. Additionally, the Bullzi Security team is comprised of security professionals who have expertise in the following disciplines:

- | | |
|------------------------------------|------------------------------|
| ▪ ISO 17799 Knowledge | ▪ Intrusion Detection System |
| ▪ Policy and Standards Development | ▪ Virus Protection |
| ▪ Security Assessments | ▪ Content Filtering |
| ▪ PKI/LDAP/X.500 | ▪ URL Filtering |
| ▪ Biometrics | ▪ Encryption |
| ▪ Incident Response/Forensics | ▪ Two-Factor Authentication |
| ▪ Firewall Design | ▪ Physical Security |
| | ▪ RADIUS Servers |

All of the security engineers have access to these specialty experts whenever needed. In addition, State technical staff has the option of being involved in all aspects of the assessment. This interaction will allow for extensive "knowledge transfer" from the Bullzi Security staff to the State IT staff. All authorized individuals from State's IT staff have the option of participating in the entire testing process. Additionally, all tools and techniques will be discussed and explained.

Many times the same security vulnerabilities exist on numerous systems throughout the network, thus the Bullzi Security team will work closely with State's IT staff and educate them on how to remedy many of the standard deficiencies discovered during the scanning process. This process of knowledge transfer will allow the State IT staff to become more knowledgeable in security issues, thereby more independent on future assessments.

The strength of the Bullzi Security team is in its people and methodologies. Information Security is an esoteric field, comprised of many disciplines.

3.2 Certifications

The Bullzi Security team members have the following certifications and training.

Industry Certifications:

Bullzi Security has security consultants who hold the following industry certifications:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Protection Professional (CPP)
- Certified Fraud Investigator (CFI)

All of the Bullzi Security team members that are named in this proposal currently have their CISSPs.

Product Certifications:

Bullzi Security has security consultants certified in the following product sets:

- Certified Checkpoint Security Engineer (CCSE)
- Certified Checkpoint Security Administrator (CCSA)
- Certified Nokia Security Administration (IPSO and VRRP)
- Cisco Certified Network Associate (CCNA)
- Certified Entrust PKI Administrator & Engineer
- Tripwire Certified

Bullzi Security also has security consultants that are experts in the following product sets:

- Assessment Tools – Nessus, nmap, Web Inspect, Saint, Solar Winds, and numerous others
- Forensic Tools – Encase, The Coroners Toolkit, Expert Witness
- Anti-virus Products – F-Secure, eSafe, TrendMicro, Symantec, MacAfee
- Hacking/Security Tools – I0phtCrack, SuperSniff, AntiSniff, Back Oriface 2000
- Authentication Tools – ActivCard, RADIUS, RSA Security Dynamics Tokens and ACE Server
- Operating System Security Administration – Windows NT, Windows 2000, Linux Solaris, Cisco Routers
- Programming expertise in several programming languages as well as web based technologies.
- Wireless Technologies (802,11b, CDPD, RAM, Circuit Switched Cellular)

3.3 Resumes

The security engineers on the Bullzi Security team, identified in Table 3.3-1, have come from numerous areas within the Information Technology (IT) industry, such as system administration, network administration, programming, investigation and forensic analysis. Only qualified, senior level security engineers will be assigned to this engagement. The resumes for the engineers that will be assigned to this project can be found in Appendix A.

| Task | Company | Name |
|--------------------------------------|-----------------|------------------|
| Security assessments (web-based) | Bullzi Security | Michael Welch |
| Security assessments (network-based) | Bullzi Security | Alex Solomonovic |
| Risk and Security Management | Bullzi Security | Thomas Welch |

Table 3.3-1 Project Staffing Table

As a security company whose reputation is based on its clients' trust, Bullzi Security recognizes the importance of fostering that trust. One of the key ways in which Bullzi Security does this is by going through extraordinary lengths to ensure that it hires only the best people, with trustworthy backgrounds. Each and every security consultant is required to go through an extensive background check as a condition of employment. The background check consists of the following:

- Civil Litigation, includes lawsuits past, present and ongoing
- Criminal Background check via National Crime Information Computer
- Credit check via the Credit Bureau

Additionally, each security engineer signs a company Non-disclosure agreement (NDA) stating that he/she will not divulge information learned about a particular client. Once the project is complete, Bullzi Security burns a copy of the report on CD. Once the State confirms receipt of a readable copy of the CD, the assessment information is deleted from the Bullzi Security systems.

3.4 References

| | |
|--|---|
| <i>Company Name</i> | <i>West Virginia Health Care Authority</i> |
| <i>Contact Name</i> | John Grey |
| <i>Contact Phone Number and E-mail</i> | (304) 348-2250 jgrey@hcawv.org |
| <i>Project Dates, Duration and Value</i> | First Assessment: 2002 Duration: 19 days Project Value: \$42K Follow-up Assessment: 2004 Duration: 5 days Project Value: \$12K |
| <i>Brief Description of Project</i> | Security Assessments, HIPAA Assessment and ISO 17799 Review |
| <i>Staff Assigned</i> | Thomas Welch, Alex Solomonovic, Michael Welch |

| | |
|--|---|
| <i>Company Name</i> | <i>Union Center National Bank</i> |
| <i>Contact name</i> | Barbara Leibman |
| <i>Contact Phone Number and E-mail</i> | (908)206-2956 BLIEBMAN@ucnb.com |
| <i>Project Dates, Duration and Value</i> | October 2002 – 2008 Duration: 20 days / year Project Value: \$40K |
| <i>Brief Description of Project</i> | Security Assessments, Security Product Implementation |
| <i>Staff Assigned</i> | Thomas Welch, Alex Solomonovic, Michael Welch |

| | |
|--|--|
| <i>Company Name</i> | <i>McDonald Information Services</i> |
| <i>Contact name</i> | Rich Rager |
| <i>Contact Phone Number and E-mail</i> | (201)659-2600 rich@callmis.com |
| <i>Project Dates, Duration and Value</i> | June 2005 – Current Duration: 30 days Project Value: \$60K |
| <i>Brief Description of Project</i> | Policy Development, Security Assessments and ISO Reviews, Vendor Selection |
| <i>Staff Assigned</i> | Thomas Welch, Alex Solomonovic |

SECTION 4
OTHER DOCUMENTS

[PAGE INTENTIONALLY LEFT BLANK]

APPENDIX A
RESUMES

[PAGE INTENTIONALLY LEFT BLANK]

THOMAS WELCH, CPP, CISSP

PROFILE

Mr. Welch has over twenty-five years in the Information Systems business, ten of which he was directly responsible for the design and development of Public Safety related applications. Mr. Welch serves as Chief Executive Officer for Bullzi Security, an information security outsourcing and consulting firm. Mr. Welch has also served as a private investigator and information security consultant since 1988 and was President and CEO of Technological Investigative Services. Mr. Welch served as CIO of Paradigm4, a wireless systems integration company for three years. Prior to his career in the Information Systems business, Mr. Welch was a Crime Analyst for the City of Orange, New Jersey and a Public Safety Officer (cross-trained Police Officer and Firefighter) for the City of Coconut Creek, Florida. He attended Florida Atlantic University and has advanced training in computer crime investigations and computer forensics. Mr. Welch is a Certified Information System Security Professional (CISSP) and Certified Protection Professional (CPP). Mr. Welch is an author and frequent lecturer on computer security topics, including computer crime investigation and computer forensics.

Experience

Bullzi Security, Inc., 801 International Parkway, Suite 500, Lake Mary, Florida 32746, serves as Chief Executive Officer from September 4, 2001 to present. Responsibilities include running a professional services organization that provides end-to-end information security solutions for, both, government and corporate clients. Services include preventive measures such as Information Security policy creation, security training, secure architecture design, security assessments including vulnerability analysis and penetration testing, implementation of security products such as firewalls, PKI, two-factor authentication, intrusion detection systems, kernel hardening, managed security services, etc.

JAWZ Inc., 353C Route 46 West, Fairfield, New Jersey 07004, served as Vice President – Enterprise Security Solutions from January 1, 2000 to August 31, 2001. Responsibilities included business development for major client relationships such as Bullzi Security, Intermedia, HP, Bell Canada (and subsidiaries), etc. Prior to his move to business development, Mr. Welch served as VP – Global Security Group, where he was responsible for managing a group of 60 information security professionals that provided end-to-end information security solutions for, both, government and corporate clients. Services included preventive measures such as Information Security policy creation, secure architecture design, security assessments including vulnerability analysis and penetration testing, implementation of security products such as firewalls, PKI, two-factor authentication, intrusion detection systems, kernel hardening, managed security services, etc. In addition to these preventive services, Mr. Welch's group provided Computer Incident Response Team (CIRT) response, high-tech crime investigations, computer forensics, and training.

Secure Data Technologies Corporation., 353C Route 46 West, Fairfield, New Jersey 07004, served as Chief Executive Office from January 1, 1999 to December 31, 1999, at which time the company was purchased by JAWS Technologies Inc. Mr. Welch was principal and founder of Secure Data Technologies Corp., an information security outsourcing and consulting company. Secure Data Technologies Corp also provided investigative services, computer forensics, and high-tech crime training.

Paradigm4, Inc., 363 Route 46 West, Fairfield, New Jersey 07004, served as Senior Vice President and CIO from January 1, 1996 to June 1, 1998. Mr. Welch is also a principal in Paradigm4, Inc., a wireless systems integration company. He was responsible for the company's overall technical architecture, which included the design, development and implementation of all wireless networking components. Mr. Welch was also responsible for all corporate security, including physical and information security.

Welch and Welch Investigations, Inc., P.O. Box 95, Glenwood, New Jersey 07418, served as President and CEO from June 8, 1988 to present. Primary duties involve civil/criminal investigations with an emphasis on computer crime investigations and computer forensics, consulting related to information security and law enforcement automation; and education and training related to information security and computer crime investigations. Mr. Welch consults to the business community and law enforcement groups on system analysis, design and planning; system vulnerabilities and security deficiencies; internal computer crime investigations.

SI3, Inc., 271 Route 46 West, Suite F109, Fairfield, New Jersey 07004, served as Vice President of Operations (50% Owner) from June 1989 to February 1993. Mr. Welch was principally responsible for development of all application software. Primary duties included the management of both the organization and customer-based projects. SI3 specialized in the design and development of Command and Control computer systems for government. This included Computer-Aided Dispatching (StateD), Records Management, and Message Switching applications. Mr. Welch managed a staff of eighteen (18) programmers, technicians and marketing support representatives, in addition to over twenty major projects.

Mr. Welch was directly responsible for company and Project-based security, which included designing major Command and Control systems that were required to run 24 hours/day, seven days/week, with no down time. This included the use of distributed, fault-tolerant and/or remote hot-standby systems. Contingency planning was one of the most crucial aspects of the system design. Part of the overall design included advanced communications networks to provide the linkage between the distributed systems. Mr. Welch was responsible for securing these networks, by using Access Control Security, encryption, dial-back modem devices, and Caller-ID verification. Mr. Welch is also familiar with other physical security measures, such as TEMPEST and Biometrics. Since many of these Command and Control systems had access to other highly secure networks, such as the National Crime Information Center, Mr. Welch was required to design and implement application level security, which would control and/or limit user access to various levels of the system.

Mr. Welch left SI3, Inc. in February 1993, when he sold the company to Systemhouse, Inc.

Computil Corp., 1040 Route 46 West, Clifton, New Jersey, served as Director of Operations from February 1988 to June 1989. Primary duties included the analysis, design, coding for Command and Control systems and included the supervision and management of ten (10) programmers and technicians. (See duties identified under SI3, Inc.)

Compu-Key Corp., 376 Hollywood Ave., Fairfield, New Jersey, served as Program Manager from August 1986 to February 1988. Primary duties included the analysis, design, coding for Command and Control systems. These duties included the supervision and management of two programmers and two technicians. (See duties identified under SI3, Inc.)

City of Orange Police Department, Orange Police Department, Orange, New Jersey, served as Crime Analyst from August 1985 to May 1986. Primary duties included the analysis of raw data to create Crime Trend Analysis and Distribution Analysis Reports. Additional duties consisted of designing a PC-based system to automate the crime analysis functions, in addition to leading an in-house Committee in the selection of a computer system for Dispatch Operations and Records Management.

City of Coconut Creek Police Department, Coconut Creek Municipal Center, Lyons Road, Coconut Creek, Florida, served as a Police Officer for the Coconut Creek Public Safety Department from July 1982 to November 1984. Conducted preliminary investigations of all criminal acts, including homicide, thefts, frauds, and other problems involving security.
Citations - Meritorious Police Duty, 1984.

Major Achievements

- Author of the Computer Crime Investigation and Computer Forensics chapter of Auerbach's Handbook of Information Security Management.
- Author of the TIS's Computer-based training (CBT) on Computer Crime Investigation and Computer Forensics. This is a 100-hour, self-paced course highlighting issues that deal with CIRT, high-tech crime investigations and computer forensics.
- Designed a secure environment for the Kansas Bureau of Investigation (KBI) – Criminal Justice network. This solution included a number of information security mechanisms, such as firewalls, IDS, two-factor authentication, policy development and awareness training. The KBI is the first state in the United States to use the Internet to transmit criminal justice data to the FBI. This design received FBI approval in August 1998.
- Lead designer for the New York City E9-1-1/StateD System
- Major speaking engagements, presentations and tutorials:
 - ✓ Testified as an expert on hacking and computer security before the New Jersey State Commission of Investigation – Computer Crime Hearings (1999)
 - ✓ Sea Girt Police Academy - Computer Crime Investigation
 - ✓ Technology for Information Security Conference (TISC) '97 – Computer Forensics and Investigation
 - ✓ Technology for Information Security Conference (TISC) '96 – Computer Crime Investigations Workshop
 - ✓ Somerset County Police Academy – Computer Seizure and Analysis
 - ✓ Mid-Atlantic and Great Lake Organized Crime and Law Enforcement Network (MAGLOCLLEN) – Internet Crime and Underground Bulletin Boards
 - ✓ Network Security '96 – Computer Crime: Investigative Techniques
 - ✓ CSI '95 Annual Security Conference – Computer Crime Investigation
- Conducted security assessments for major corporations and governmental agencies that included business level risk assessments which includes technical assessments of the clients architecture (i.e. vulnerability scans, attack and penetration, etc.), policy development, awareness training and the implementation of security products.
- Managed the design and development of the New York City Fire Departments second generation StateD system - STARFIRE II.
- Original author of SI3's Computer-Aided Dispatch and Records Management system, which is currently installed in over fifteen (15) Police and Fire agencies, including the City of Newark.
- Co-designer of the first, secure law enforcement network that permitted CJIS transactions over the Internet. This design, which included firewalls, virtual private networks, intelligent intrusion detection systems, and several levels of authentication, culminated in a report that was submitted to the FBI and later approved.
- Designed and installed an Agent Tracking System for the New York Operations of the Federal Bureau of Investigations.
- Spearheaded the software development effort for the City of Newark "Scofflaw" project, using the Motorola hand-held terminals and the Motorola Data Radio Network.
- Designed and installed an integrated networking switch to the National Crime Information Center and the Department of Motor Vehicles, utilizing Stratus Fault Tolerant hardware.

Information Systems Expertise

Mr. Welch's experience with various hardware platforms include:

- PC, HP 9000, Sun Ultra, Stratus, IBM RS/6000, DG AViiON, DEC 5000/240, Convergent Technologies B38 NGEN, Unisys A3, Unisys B1990, and IBM System 36

Mr. Welch's experience with various software includes:

- MS Windows (3.1, 95, 98, NT), UNIX, VOS, MS-DOS, BTOS/CTOS, X-Windows(Motif), "C", C++, Pascal, Fortran, LINK (4GL), Forte`
- Informix, Oracle, Ingres, Sybase, ISAM

Mr. Welch's experience with various information security products includes:

- Check Point firewalls, Entrust, EnCase, Expert Witness, Coroners Toolkit, Axent Security Suite, ActivCard, F-Secure, Security Dynamics SecurID, ISS Security Suite (IDS and Scanning Tools), Tripwire, nmap

Mr. Welch's experience with computer-based security systems include:

- UNIX and NT O/S Security (Access Control, File Management and Auditing), Kerberos, RSA Encryption, Firewalls, various virus detection and mitigation applications, PC Access, NTP, SATAN, Tripwire, COPS, Cracker

Education

Broward Community College, Coconut Creek, Florida, 1984. Associate of Arts (AA).

Florida Atlantic University, Boca Raton, Florida, 1985. Major - Computer Science.

Certificate of Compliance in Law Enforcement, State of Florida, Criminal Justice Standards and Training (Police Academy - 1982).

Academic Honors - graduated first in academy class.

Specialized Law Enforcement Courses and Seminars:

Line Supervision for Law Enforcement Officers

Progressive Patrol Administration

Executive/VIP Protection Course

Investigative Technology Course

Credit Card Fraud Investigation Course

Criminal History Records Seminar

Fingerprint Techniques

Computer Security

Licenses and Certifications

New Jersey Private Investigator License (1988)

Florida Private Detective License (1988)

New York State Private Investigator License (1995)

Certified Protection Professional (CPP) - 1995

Certified Information Systems Security Professional (CISSP) - 1996

Certified Fraud Investigator (CFI) - 1998

Certified Checkpoint Security Engineer (CCSE) - 1998

Certified Checkpoint Security Administrator (CCSA) - 1998

ALEX SOLOMONOVIC, CISSP

PROFILE

Mr. Solomonovic has over twelve years of experience in information technology. During the last six years, he has focused on large integration projects, and secure network design and development of full scale Managed Security Services.

Experience

Bullzi Security, Inc., 801 International Parkway, Suite 500, Lake Mary, Florida 32746, serves as Director of Security Technology from September 4, 2001 to present. Responsible for security technology evaluation, recommendation and integration as well as the company's technical architecture, products, and service capabilities both internally and externally. Also, responsible for secure network design solutions and network architecture reviews.

JAWZ Inc., 353C Route 46 West, Fairfield, New Jersey 07004, served as Director, Security Architecture from January 1, 2000 to August 31, 2001. Responsibilities included designed, implemented and managed JAWZ Managed Security Services operation based at Fairfield, NJ office, CheckPoint FW-1/VPN-1 turnkey solution for the client, consulting and support, ISS RS 3.2 & 5.x fully managed solution, 24/7 monitoring and reporting, pre-sales support of high profile security projects (involving Fortune 100 clients) regarding network security review and secure network design using best known practices and best of breed security products.

Secure Data Technologies Corp., 353C Route 46 West, Fairfield, New Jersey 07004, served as Director, Information Security from January 1, 1999 to December 31, 1999. Responsibilities included implementation of network security products based on customer security requirements: CheckPoint VPN-1 (on NT and Nokia IPSO platforms), Entrust PKI, ActivCard Server (token & smartcard authentication). Working closely with customers on improving their LAN/WAN design and recommending and specifying products and equipment to secure and upgrade existing or design & install new networks.

Paradigm4, Inc., 363 Route 46 West, Fairfield, New Jersey 07004, served as Information Security Officer from December 9, 1996 to December 31, 1998. Responsibilities included administration of multi-domain NT 4.0 LAN/WAN environment and supporting 150+ internal users and providing II and III level of support for customers. Managing CheckPoint 3.0b/4.0 FW-1 firewalls. Managing Netscape Mail Server 3.6 for NT with 150+ users, Tally auditing system, ELRON-Internet Manager monitoring application. Designed and implemented security policy for entire company at multiple locations including testing for user & system compliance with the policy. Participated on various projects in designing secure network solution for customers. Overlooked network and physical security for entire company in multiple geographical locations.

Significant Projects

General Electric – GEIS/GEIO, Gaithersburg, MD (2000)

Over the period of six months, provided security consulting on a wide variety of topics and issues, attendance of hundreds of internal process, design and readiness review meetings, assisted GEIS System Integrity group with Windows NT related security issues, Nokia 440/650 Firewall appliance support and assistance in redesigning CheckPoint FW-1/VPN-1 implementation and consolidation of the rulebases, ISS Real Secure 3.2/5.0 IDS system design and initial rollout. Delivered internal IDS ISS RS training for GEIS System Integrity, Firewall Security groups and members of GE Europe System Integrity Team.

Township of Union, NJ - Network Security Integration (1999)

Performed complete assessment of 150+ node network in multiple departments/locations. Presented detailed report, including recommendations for security policy development and general network upgrades, security awareness training, physical security and access control, PC H/W and network infrastructure upgrade. After report acceptance implemented security policy changes, specified, ordered, installed and configured new computer room equipment. Reviewed and corrected security settings and permissions, verified that latest patches, service packs and drivers are installed; performed software compliance audit, unified naming conventions for users and organization units, reorganized file/directory structure in entire network. Established strong password requirements. Standardized on NT 4.0 WS OS on client side, installed and integrated CheckPoint/Nokia VPN-1 (RL50) firewall appliance into existing layout and configured WWW and Imail servers on DMZ.

State of Kansas - KBI (1998)

Together with other two members of Paradigm4 information security team, designed the solution that complies with current FBI policy that states that federal criminal information cannot be transmitted over the Internet, unless the state can provide sufficient assurances that adequate security is in place to safeguard the data. Paradigm4 developed and implemented CJIS applications and message switches to make KBI NCIC2000 compliant. This design effort, which included the development of a secure architecture, virtual private networks, firewalls, intelligent network intrusion detection and several levels of authentication, resulted in a report that was submitted to the FBI and later approved. This paved the way to send the first law enforcement transactions over the Internet in the history of the FBI.

City of New York - CityTime Project (1997-98)

Responsible for network security design and integration of multiple departmental LANs into WAN environment with connection to project vendors extranet as a part of ongoing project that includes redesign and integration of the whole City of New York Office of Payroll Administration network.

Information Systems Expertise

- Network security design and architecture, including design and implementation of CheckPoint FW systems, IIS RS 3.2 and 5.x IDS systems, VPN solutions, designing company security policies, firewall rule base.
- Installation and "hardening" NT 3.51/4.0 Server as a preparation to install WWW, FTP or Email server applications on DMZ network segment.
- In depth knowledge of DOS, Windows9X, MS Office 97/2000, NT 4.0 Workstation, NT 4.0 Server administration, RAS.
- Network design and testing (TCP/IP, SMTP, POP3, FTP, TELNET, DNS, RIP, Ethernet, Fast Ethernet, manageable hubs/switches, RAID, DAT, DLT, UPS).
- Installation and configuration of Cisco Fast Ethernet Catalyst 2924XL switches, 1600 & 1700 Cisco routers and Proteon GT series routers.
- Basic knowledge of Solaris 2.6 and BSD UNIX required for CP FW-1 and VPN-1 installation, configuration and maintenance.
- Extensive hardware experience with PCs and peripherals, incl. notebooks, MDC units, analog and CDPD modems.

Installation, configuration, management and maintenance of tools and applications:

- CheckPoint FW-1/VPN-1 on NT 4.0, IPSO (Nokia) platform and Intrusion.Com appliance
- ISS Internet Scanner 6.X & ISS RS 3.2 and 5.x network/OS/Server Sensor and WS MGMT.
- ELRON Internet Manager 4.X & Tally Systems.
- Netscape Messaging Server 3.6, MS Exchange 5.5, IPswitch-Imail Server 5.7/6.1, MS IIS 4.0, PC AW 8.0/9.0.

- Entrust Enterprise PKI 4.0 and ActivCard 3.1 server on NT platform
- Visio Professional/Enterprise 5.0 & 2000
- Tripwire HQ 1.0 and Connector 1.0

Training, Certifications and Memberships

TechLink - Windows NT 4.0 Administration (March 1997)
CSI - Windows NT Security (June 1997)
OpenRoute Networks - Proteon GT Router configuration course (Apr. 1998)
CSI - Advanced Windows NT Security (Aug. 1998)
CSI - Comprehensive Intrusion Detection (Aug. 1998)
CheckPoint - CCSA, CCSE 3.0b (Sept. 1998)
Certified Entrust PKI 4.0 Administrator & Engineer (July 1999)
Nokia FW – HA VRRP & Nokia Security Administrator (March 2000)
Certified ISS Database, Internet Scanner 6.X & ISS RealSecure 3.2 Engineer – ICE (April 2000)
Cisco Certified Network Associate - CCNA (February 2001)
CheckPoint Certified Security Administrator – CCSA2000 (March 2001)
Member of Computer Security Institute (1996-present)

MICHAEL WELCH, CISSP, CISM

PROFILE

Mr. Welch has over eleven years in the Information Security business. Mr. Welch has conducted over 100 security architecture reviews, Business Risk Assessments (Gap Analysis), attack and penetration tests, network and host assessments and firewall reviews. Mr. Welch has implemented firewalls, intrusion detection systems and file integrity systems into network infrastructures. Mr. Welch has reviewed and developed security policies and procedures to ensure that they followed industry best practices, as well as, assisted in the development of a HIPAA Compliance program. Mr. Welch has been responsible for full project life cycle of security architecture reviews, penetration assessments, and Business Risk Assessments. Mr. Welch has been involved in creating Security Best Practices Baselines for various technologies which include: Windows NT4, Windows 2000 (Professional and Server), Internet Information Server 4 and 5, Solaris 8, Linux 7, Checkpoint Firewall on NT4 and Solaris, and Apache Web Server. Mr. Welch has conducted security awareness training; created an advanced hacking course; developed a Computer Based Training course on Computer Crime Investigations and Forensics; and assisted in training security consultants in performing Business Risk Assessments.

Experience

Bullzi Security, Inc. 801 International Parkway, Suite 500, Lake Mary, Florida 32746, serves as Director of Risk Management from January 1st, 2002 to Present. Responsibilities include developing and maintaining the risk management division of Bullzi Security. The prime focus will be on Business Risk Assessments focused on HIPAA and GLB compliance, following the Common Criteria and BS7799 guidelines to help organizations mitigate risk to an acceptable level. Mr. Welch other areas of focus will be on Attack and Penetration, Vulnerability Assessments, and Fraud Detection and Prevention.

Vigilinx, 53 Wateview Boulevard, Parsippany, New Jersey, served as Manger of Risk Assessments from April 15th 2001 to December 31st, 2001. Managed and conducted Business Security Assessments and Attack & Penetration Tests. Business Security Assessments were geared to identify mission critical assets and mitigate risk to an acceptable level. This was done through interviews, policy and procedure reviews, walk-troughs and checklists. The Attack & Penetration Tests were focused on Application Assessment, Infrastructure Assessment and System Configurations to help customers to lower their risk to an acceptable level.

JAWZ Inc., 353C Route 46 West, Fairfield, New Jersey 07004, served as Senior Security Consultant from January 1, 2000 to April 14th, 2001. Responsibilities included supporting internal and external JAWZ clients globally. Conducted security architecture reviews, attack and penetration testing, network and host assessments; all phases of secure network architecture (design, implementation, testing). Integrated network equipment; such as firewalls (Checkpoint) and IDS systems (ISS Real Secure and Black Ice) into client networks.

Responsibilities included writing proposals and reports for clients, briefing clients on status of project and at the end of an assessment. Use MS Project for project management. Other duties included:

- Participated in the development of Advanced Hacking Course, which will be given at the University of Calgary. Designated as one of three instructors that will be teaching the course.
- Assisted in the development of an out-of-band logging server for JAWZ. Exported logs from firewalls, IDS systems and production servers.
- Assisted in development of JAWZ HIPAA Compliance program.
- Conducted GAP Analysis Assessments for Financial, Health, and Telecommunication Industries.
- Attended information security conferences (Blackhat, DefCon, SANs, and InfoSec World) to stay current with security topics.
- Represented JAWZ at trade shows/expos to demo hacking techniques and assist in pre-sales (Techno Security, NLETS, ASPcon).

- Secured NT, Linux and Solaris Servers for both internal and external clients using industry standard and best practices.

Secure Data Technologies Corporation, 353C Route 46 West, Fairfield, New Jersey 07004, served as E-commerce Manager from January 1, 1999 to December 31, 1999. Developed and maintained a 100-hour computer based training course on computer forensics and investigations. This course was designed for law enforcement and corporate security personnel and developed using Quest.

Other responsibilities for clients included:

- Maintained and administered internet/intranet sites.
- Administered mail servers and DNS servers.
- Performed security assessments onsite and remotely for customers.

Paradigm4, Inc., 363 Route 46 West, Fairfield, New Jersey 07004, served as Computer Programmer from January 1, 1997 to December 31st, 1998. Developed and maintained installation scripts using Install Shield for Paradigm4 client software. Lead developer of Computer Based Training for Kansas Bureau of Investigations and Florida Department of Law Enforcement on NCIC 2000. Trained end users of each organization on functionality of Computer Based Training. Assisted in the design of the Paradigm4 Accident Reporting System using Protogen and Visual Basic.

International Museum of Cartoon Art, Boca Raton, Florida, served as Operations Manager from April 1996 to December 31st, 1996. Responsibilities included the physical and operational security for museum. Worked with law enforcement and museum management in order to protect the multi-million dollar art as well as the visitors to the museum

Welch and Welch Investigations, 13 Stone Ridge Road, Vernon, New Jersey, servers as Intern Investigator from March 15th, 1993 to present. Responsibilities include the development of computer based trained on forensics and investigations.

Major Achievements

- Co-Author of the TIS's Computer-based training (CBT) on Computer Crime Investigation and Computer Forensics. This is a 100-hour, self-paced course highlighting issues that deal with CIRT, high-tech crime investigations and computer forensics.
- Conducted security assessments for major corporations and governmental agencies that included business level risk assessments which include technical assessments of the client's architecture (i.e. vulnerability scans, attack and penetration, etc.), policy development, awareness training and the implementation of security products.

Information Systems Expertise

Mr. Welch's experience with various hardware platforms include:

- Windows family (NT, WIN2K, 3.1, 95, 98), Solaris, Linux (Redhat)

Mr. Welch's experience with various information security assessment products includes:

- AppScan, WebInspect, Core Impact, ISS Internet Scanner, Database Scanner, Retina, Nessus, Enterprise Security Manager, Cerberus Internet Scanner, Network Associates Cybercop Scanner, Axent NetProwler, and various other freeware scanning utilities (nmap, whisker, iscan), L0pht Crack, SuperScan, Solarwinds, Web Cracker, Grinder, Legion, Ogre, Somarsoft, Visual Route, Teleport Pro, Black Widow, NT Admin Toolkit, Expert Witness, Sam Spade, Achilles

-

Mr. Welch's experience with various information security products includes:

- Check Point firewalls, Entrust, EnCase, Expert Witness, Coroners Toolkit, Axent Security Suite, ActivCard, F-Secure, RSA SecurID, ISS Security Suite (IDS and Scanning Tools), Snort, Tripwire, nmap

Mr. Welch's experience with computer-based security systems include:

- UNIX and NT O/S Security (Access Control, File Management and Auditing), Kerberos, RSA Encryption, Firewalls, various virus detection and mitigation applications, PC Access, NTP, SATAN, Tripwire, COPS, Cracker

Education

Utica College, NY. Economic Crime Management (04). Working on Masters Degree
George Washing University, Washington D.C., 1996. Major – BA - Criminal Justice.

Certifications

Certified Information Security Manager (CISM) - 2003
Certified Information Systems Security Professional (CISSP) – 2001
InfoSec Assessment Methodology (NSA) - 2000
Certified Checkpoint Security Administrator (CCSA) – 2000
Tripwire Certified – 2000

Memberships

International Information Systems Security Certification Consortium
American Society of Industrial Security
The Information Systems Audit and Control Association and Foundation
Association of Certified Fraud Examiners
Information Systems Security Association
High Technology Crime Investigation Association
Infraguard

APPENDIX B

ADDENDUM ACKNOWLEDGMENT

REQUISITION No.: ITECH10

I HEREBY ACKNOWLEDGE RECEIPT OF THE FOLLOWING CHECKED ADDENDUM(S) AND HAVE MADE THE NECESSARY REVISIONS TO MY PROPOSAL, PLAN AND/OR SPECIFICATIONS, ETC.

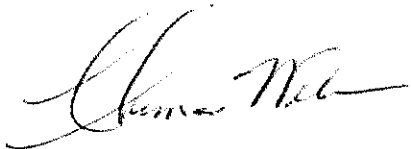
ADDENDUM NO'S:

No.1 DATED DECEMBER 14, 2009

I UNDERSTAND THAT FAILURE TO CONFIRM THE RECEIPT OF THE ADDENDUM(S) MAY BE CAUSE FOR REJECTION OF BIDS.

BULLZI SECURITY UNDERSTANDS THAT ANY VERBAL REPRESENTATION MADE OR ASSUMED TO BE MADE DURING ANY ORAL DISCUSSION HELD BETWEEN BULLZI SECURITY REPRESENTATIVES AND ANY STATE PERSONNEL IS NOT BINDING. IT IS FULLY UNDERSTOOD THAT ONLY THE INFORMATION ISSUED IN WRITING AND ADDED TO THE SPECIFICATIONS BY AN OFFICIAL ADDENDUM IS BINDING.

By: BULLZI SECURITY, INC



Thomas Welch, President and CEO

Dated: January 10, 2010

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

VENDOR OWING A DEBT TO THE STATE:

West Virginia Code §5A-3-10a provides that: 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 the debt owed is an amount greater than one thousand dollars in the aggregate.

PUBLIC IMPROVEMENT CONTRACTS & DRUG-FREE WORKPLACE ACT:

If this is a solicitation for a public improvement construction contract, the vendor, by its signature below, affirms that it has a written plan for a drug-free workplace policy in compliance with Article 1D, Chapter 21 of the *West Virginia Code*. The vendor **must** make said affirmation with its bid submission. Further, public improvement construction contract may not be awarded to a vendor who does not have a written plan for a drug-free workplace policy in compliance with Article 1D, Chapter 21 of the *West Virginia Code* and who has not submitted that plan to the appropriate contracting authority in timely fashion. For a vendor who is a subcontractor, compliance with Section 5, Article 1D, Chapter 21 of the *West Virginia Code* may take place before their work on the public improvement is begun.

ANTITRUST:

In submitting a bid to any agency for the state of West Virginia, the bidder offers and agrees that if the bid is accepted the bidder will convey, sell, assign or transfer to the state of West Virginia all rights, title and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the state of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the state of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to the bidder.

I certify that this bid is made without prior understanding, agreement, or connection with any corporation, firm, limited liability company, partnership or person or entity submitting a bid for the same materials, supplies, equipment or services and is in all respects fair and without collusion or fraud. I further certify that I am authorized to sign the certification on behalf of the bidder or this bid.

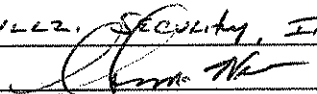
LICENSING:

Vendors must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agencies or political subdivision. Furthermore, the vendor must provide all necessary releases to obtain information to enable the Director or spending unit to verify that the vendor is licensed and in good standing with the above entities.

CONFIDENTIALITY:

The vendor agrees that he or she will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the agency's policies, procedures and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in <http://www.state.wv.us/admin/purchase/privacy/noticeConfidentiality.pdf>.

Under penalty of law for false swearing (*West Virginia Code* §61-5-3), it is hereby certified that the vendor affirms and acknowledges the information in this affidavit and is in compliance with the requirements as stated.

Vendor's Name: BULLZ SECURITY, INC.
Authorized Signature:  Date: 1/10/10