The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.


wvOASIS
Jump to: FORMS
Go
Home
Personalize
Accessibility
App Help
About
Welcome, Lu Anne Cottrill
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR) Dept: 0203 ID: ESR01221500000001756 Ver.: 1 Function: New Phase: Final
Modified by batch , 01/22/2015
Header
List View
General Information
Contact
Default Values
Discount
Document Information
Procurement Folder: 15921
Procurement Type: Central Contract - Fixed Amt
Vendor ID: 000000114262
Legal Name: SECURITY RISK SOLUTIONS INC
Alias/DBA:
Total Bid: $0.00
Response Date: 01/22/2015
Response Time: 9:56
SO Doc Code: CRFQ
SO Dept: 0203
SO Doc ID: CPR1500000001
Published Date: 1/9/15
Close Date: 1/22/15
Close Time: 13:30
Status: Closed
Solicitation Description: Addendum2 for CRFQ CPR15*1
Total of Header Attachments: 0
Total of All Attachments: 0

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

State Of West Virginia
Solicitation Response

Proc Folder : 15921
Solicitation Description : Addendum2 for CRFQ CPR15*1
Proc Type : Central Contract - Fixed Amt

Date issued	Solicitation Closes	Solicitation No	Version
	2015-01-22 13:30:00	SR 0203 ESR01221500000001756	1

VENDOR

000000114262

SECURITY RISK SOLUTIONS INC

FOR INFORMATION CONTACT THE BUYER
Guy Nisbet
(304) 558-2596
guy.l.nisbet@wv.gov

Signature X **FEIN #** **DATE**

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	network security and vulnerability assessment	0.00000	LS	$63,254.52	

Comm Code	Manufacturer	Specification	Model #
81111801			

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	network security and vulnerability assessment	0.00000	LS	$56,929.07	

Comm Code	Manufacturer	Specification	Model #
81111801			

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	network security and vulnerability assessment	0.00000	LS	$56,929.07	

Comm Code	Manufacturer	Specification	Model #
81111801			

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	network security and vulnerability assessment	0.00000	LS	$56,929.07	

Comm Code	Manufacturer	Specification	Model #
81111801			

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
5	network security and vulnerability assessment	0.00000	LS	$63,254.52	

Comm Code	Manufacturer	Specification	Model #
81111801			

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

Security Risk Solutions, Inc.
698 Fishermans Bend
Mount Pleasant, SC 29464
Tel:843-442-9104

SecurityRiskSolutions
.....managing information security risks in the real world

20th January, 2015

Department of Administration, Purchasing Division
2019 Washington Street East
P.O. Box 50130
Charleston, WV 25305-0130

Attn: Mr. Guy Nisbet, Senior Buyer

Proposal for State of West Virginia Consolidated Public Retirement Board Network Security and Vulnerability Assessment. Solicitation #: CPR1500000001

Dear Mr. Nisbet,

Security Risk Solutions, Inc. is pleased to submit this proposal for solicitation CPR1500000001. The following corporate information is provided in support of our proposal:

Corporate Name:	Security Risk Solutions, Inc. (SRS)
Economic Status:	SBA Small Business, Woman Owned Small Business
Preference Applied for:	Non-resident vendor certified as a small, women-owned, or minority-owned business under W. Va. CSR §148-22-9.
Authorized Representative and Contact Information	Johnathan Coleman, CISSP, CISM, CBRM, CRISC Principal, Security Risk Solutions, Inc. 698 Fishermans Bend, Mt. Pleasant, SC 29464, USA Tel: (843) 647-1556 Cell:(843) 442-9104 jc@securityrs.com
Incorporation Status	S-Corporation (South Carolina)
Years in Business:	Currently in 11th year. Original articles of organization dated December 2004.
D&B (D-U-N-S) Number:	192835390
TIN:	20-8133845
Security Clearance:	SRS maintains a DOD Top Secret Facility Clearance, Cage Code 41MQ0
GSA Schedule Contract Number:	GS-35F-0034W; SIN 132 51

In support of our proposal, we are pleased to make the following assertions:

1. At time of submitting, no addenda 1 and 2 have been issued. SRS acknowledges all information and terms provided by the addenda.
2. Upon award, Security Risk Solutions, Inc is both willing and able to perform the terms indicated in our proposal.
3. We hereby confirm acceptance of all Terms and Conditions as described, incorporated or referenced in the RFQ.
4. Our online Representations and Certifications Application (ORCA) are current and up-to date.
5. We are submitting a Fixed Price proposal.
6. Our proposal will remain in full force and effect for 180 days from bid open date.
7. SRS is hereby identifying itself as a non-resident small business and women-owned business for consideration to be provided the same preference made available to any resident vendor under W. Va. CSR §148-22-9.

Thank you for considering our offer. Should you require additional information, please contact me at 843-442-9104 or by e-mail at jc@securityrs.com.
Sincerely,

Johnathan Coleman, CISSP, CISM, CBRM, CRISC
Principal, Security Risk Solutions Inc.

Johnathan Coleman

State of West Virginia

Information Security and Network Vulnerability Assessment

WV Consolidated Public Retirement Board (CPRB)

Technical Proposal: Response to Solicitation #: CRFQ 0203 CPR1500000001

Submitted by

Security Risk Solutions, Inc.
698 Fishermans Bend
Mount Pleasant, SC 29464
(Tel) 843.647.1556
(Fax) 843.416.4881

Point of Contact: Johnathan Coleman, CISSP, CISM, CBRM, CRISC
Principal, Security Risk Solutions, Inc.
(Tel): 843.442.9104
jc@securityrs.com

VENDOR SIGNATURE: Johnathan Coleman _____ DATE: 21st January 2015

Table of Contents

1 Vendor Information 1
2 endor Qualifications 1
2.1 About our Team 1
2.2 Confidentiality Agreements 2
2.3 Similar Past Performance 3
3 Mandatory Requirements 7
3.1 Mandatory Contract Services Requirements and Deliverables 7
3.1.1 Relevant Staff Experience 7
3.1.2 Prioritize and rank the discovered vulnerabilities using the Common Vulnerability Scoring System (CVSS) 10
3.1.3 Evaluation of the security policy and procedures 11
3.1.4 Scan of external entry points into the network 11
3.1.5 Review of all of the devices on the network with static IP addresses: 14
3.1.6 A review of the server, firewall, and IDS configurations 15
3.1.7 Provide Post-Assessment Remediation Services if prime contractor cannot address the identified vulnerabilities 15
3.1.8 Written Reports 15
3.1.9 Firewall Architecture and Policy Review 16
3.1.10 Endpoint Assessment 17
3.1.11 Data Loss Prevention Gap Analysis 18
3.1.12 Collaborate with the CPRB Guidance Team to develop and deliver executive presentations of the assessment and its results. 19
3.1.13 Evidence of the performance of a vulnerability assessment and/or penetration test on a government entity or corporation that has the minimum of 5,000 employees: 20

Appendix A: Resumes for Personnel Proposed
Appendix B: Copies of Staff Certifications and Degrees
Attachment 1 - Vendor References
Attachment 2 – Vendor Primary Staff References
Attachment 3 – Attestation and Confirmations
Attachment 4 – Confidentiality Agreement
Attachment 5 – Vendor Preference Certificate
Attachment 6 – Purchasing Affidavit
Attachment 7 - Certification and Signature Page
Attachment 8 - Addendum Acknowledgement Form
Exhibit A – Pricing (see separate worksheet)

1 Vendor Information

The following information is provided in response to the requirements of the solicitation. Supporting information for the Primary Vendor (Prime Contractor) and subcontractors is shown in Table 1 below.

Table 1: Vendor Identification

	PRIME CONTRACTOR	SUBCONTRACTOR
Organization:	Security Risk Solutions, Inc. (SRS)	Athena Consulting Group, LLC (ACG)
Economic Status/ Preferences	• SBA Small Business. • Woman Owned Small Business (WOSB) • WV Preference as an out-of-state WOSB applied for.	• Small Business
Authorized Representative and Contact Information:	Johnathan Coleman, CISSP, CISM Principal, Security Risk Solutions 698 Fishermans Bend, Mt. Pleasant, SC 29464, USA Cell:(843) 442-9104 jc@securityrs.com	Doug Majewski CEO, Athena Consulting Group 4995 LacCross Road, Suite 1250 North Charleston, SC 29406 Tel: (804) 417 7699 chris.cotton@athenaconsultinggroup.com
Website	www.securityrisksolutions.com	www.athenaconsultinggroup.com
Incorporation:	S-Corporation (South Carolina)	Limited Liability Corporation (SC)
Date Founded:	31 December, 2004	24 December, 2004
D-U-N-S No:	192835390	171419257
TIN:	20-8133845	25-1915472

2 Vendor Qualifications

2.1 About our Team

Team Highlights

- **Highly qualified and certified team of Security Professionals with deep experience and understanding of Information Security, experienced in performing assessments for Federal and State Agencies**
- **Renowned and credentialed subject matter experts in IT Security, Privacy, and Risk Assessment**
- **Staff committed to this effort available from day one and ready to excel**
- **Team includes staff experienced with WV State Agencies and WVOT infrastructure, requiring little learning curve to adjust to organizational culture or technical environment**

Security Risk Solutions (SRS) Inc., is a small, woman owned business based in Mount Pleasant, SC. SRS is a vendor neutral consulting firm that specializes in Information Security Risk Management Services, with a particular expertise with Security Risk Assessments, Compliance, and mitigation planning. SRS recognizes the delicate balance and difficult challenges faced by organizations in trying to fulfill the business mission, yet still maintain regulatory requirements for security and implement security best practices in a cost effective manner. Our services focus not only on the

technical infrastructure, but also on the business processes and staff practices which play a crucial part in the effective implementation of any security, compliance or IT governance program. Service offerings include: Risk Management (Assessment and Analysis), Organizational Business Impact Analysis, Technical Vulnerability Assessments and Penetration Testing, Audit and Development of Corporate and Regulatory Compliance Programs, System Interoperability and Requirements Analysis, and Project Risk Management.

Our proposed team includes SRS as the prime contractor, and Athena Consulting Group LLC (ACG). SRS has been working with ACG for many years. Our team collectively provides deep subject matter expertise and experience working together as a cohesive unit to provide the absolute best value and highest quality of service. As prime contractor, SRS will provide all aspects of program management, leadership to the team, contract oversight, and will provide the overall technical and strategic subject matter expertise regarding IT security and Penetration Testing. Our current knowledge of the WV Offices/systems, WV Department of Administration, and WV Office of Technology Offices and personnel will be critical in ensuring that our implementation approach is appropriately and efficiently tailored to accommodate nuance and uniqueness that exists in every project. Our team's deep experience in penetration testing and technical vulnerability experience is proven through years of experience in performing these tasks in complex, sensitive, and mission critical networks. For example, our team has lead and conducted numerous "high stakes" technical vulnerability assessments on networks and systems for the Department of Defense, the Department of Health and Human Services, and the State of West Virginia.

Athena Consulting Group (ACG) is an Information Assurance, Program Management and Information Technology services firm focused on solutions with customer-centric support to the US Government, including the Department of Defense and Veteran's Affairs. With offices in Charleston, SC, Richmond, VA, and San Diego, CA, ACG is supporting customers worldwide. ACG offers end-to-end complete solutions, assuring high-end quality prior to and for the duration of projects. ACG receive and act in advance upon information regarding product releases, code-security, new vulnerabilities, and mitigation strategies. Technical and management staff personnel are industry experts with the ability to combine elegant and innovative technical solutions with best industry and business practices.

Security Risk Solutions, Inc., confirms its ability to provide all of the specific products and services specified in this proposal, on-time, on budget, and to the highest degree of excellence.

Date Founded:
As shown in
Table 1: Vendor Identification, SRS and ACG were founded in December 2004 and are in their eleventh year of business.

2.2 Confidentiality Agreements

Subsequent to contract award, but prior to the start of work, all firm personnel assigned to the engagement will sign and accept a non-disclosure and confidentiality agreement. All staff

proposed for this project have been subject to background investigations for positions of trustworthiness, and hold Department of Defense security clearances.

2.3 Similar Past Performance

The following examples provide documentation of similar work performed in the successful performance of information security and network vulnerability assessments in compliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37. Attachment 1 contains the necessary information for customer references.

The following past performance references are provided for consideration, all of which include testing and approaches consistent with and compliant with NIST SP 800-37.

Past Performance 1: WV PEIA/WV CHIP Security Risk Assessment
Services provided by SRS and ACG include all aspects of information security, including vulnerability assessments, penetration testing, physical security, IT related systems, policies and procedures, staff training, and third party interaction(s).

Past Performance 2: Cyber Security Inspections – US Navy
SRS and ACG provide support to the US Cyber Command (USCYBERCOM) Command Cyber Security Inspections (CSI) Stage II readiness team. Our team travels to sites selected for inspection by the US Navy Fleet Cyber Command (FLTCYBERCOM) Office of Compliance and Assessment (OCA) to assess the security of Navy networks through a comprehensive, graded inspection involving all Cyber Security areas, specifically: Leadership Management, Physical Security, Administration, Training, Network Configuration, Network Operations, and Human Factors and Command Operational Behavior. Navy Medicine Information Systems Support Activity (NAVMISSA) consists of 29 Major Medical Centers, Hospitals, and Ambulatory Clinics, 27 Major Information Systems, approximately 55,000 users and 86,000 end nodes.

Past Performance 3: Army National Guard Bureau DIACAP Support
SRS performs security Vulnerability Testing for the Army National Guard Electronic Security Systems program. Under this task, SRS provides support to the Space and Naval Warfare Systems Center, Atlantic and the Army National Guard Bureau by conducting security reviews, vulnerability testing, and supporting documentation for the ARNG ESS System DIACAP Accreditation, using NIST SP 800-37, NIST SP 800-53revision 4, Army Information Assurance requirements, and Department of Defense Security Standards.

Table 2: Past Performance 1: WV PEIA/ WV CHIP

Security Risk Solutions (SRS): State of West Virginia Public Employees Insurance Agency (PEIA) / West Virginia Children's Health Insurance Program (CHIP) Security Risk Assessment			
Contracting Organization	State of West Virginia Public Employees Insurance Agency (PEIA)	**Performance Period:**	March 2014 – April 3rd, 2015
Description and relevance to solicitation requirements:			
SRS was tasked with providing a multi-phase HIPAA Security Risk Assessment which included a Policies and Procedures Review, Network Discovery Topology Review, Internal / External Technical Vulnerability Assessment, Physical Security Review, Security Risk Management, Risk Analysis Training, , Mitigation Planning with Cost Estimates, and Program Management for the State of West Virginia PEIA and CHIP agencies. This support provided the Privacy Officer of the West Virginia Department of Administration, and the Directors of both PEIA and CHIP, with detailed levels of compliance with the HIPAA Security Rule and an overall risk assessment of the critical assets of each organization. During the project, a multi-disciplined workgroup was formed comprising of SRS, PEIA, and CHIP, as well as key members from the West Virginia Office of Technology. Exceptional program management skills combined with technical expertise were needed to bring together all key players into the assessment from each agency at the appropriate stage. During the first phase of the three-phase project, organizational policies and procedures were reviewed for compliance with the applicable regulations. This review took into account all of the security-related policies and procedures from PEIA and CHIP as well as overarching policies and procedures from the West Virginia Office of Technology. The output of the review included a Plan of Action and Milestones (POA&M) that assigned responsibility to the appropriate agency for the creation and modification of policies and procedures needed for compliance with the regulation. During phase two of the project, SRS conducted in-depth vulnerability scanning of the PEIA and CHIP networks. While onsite, SRS also completed a thorough onsite physical assessment of the agencies. Specific examples of work during this phase included an internal security vulnerability assessment on servers, workstations and network infrastructure, external security vulnerability assessment on web applications / sites accessible from the Internet, and a wireless networking assessment evaluating controls from NIST Special Publication 800-53 revision 4. During the third phase, the Risk Analysis, SRS worked with the WV agencies to identify potential threats against their critical assets and devise a plan to mitigate such threats. The latter includes creating cost estimates for the mitigating measures so that each agency would be well-informed of the cost associated with implementing the mitigation plan.			

Table 3: Past Performance 2: Navy Medicine Information Systems Support Activity (NAVMISSA)

Security Risk Solutions (SRS): Navy Medicine Information Systems Support Activity (NAVMISSA)			
Contracting Organization	Department of Defense/US Navy	**Performance Period:**	August 2008 – Dec 31, 2014
Description and relevance to solicitation requirements:			
SRS is tasked with providing Security Risk Management, Policy Support, Continuous Risk Management, Program Management and IT Contingency planning (ITCP) support to 29 Naval Medical Centers, Hospitals, and Ambulatory Clinics in the Navy Medicine (NAVMED) enterprise, 27 Major Information Systems, which collectively mass to approximately 55,000 users and 86,000 end nodes. This support assists the CIOs and Information Assurance Managers at each Medical Treatment Facility in maintaining a secure and compliant infrastructure by identifying and mitigating IT issues and addressing compliance considerations. This requires substantive Information Security expertise in such areas as IT Contingency Planning and Technical Risk Management in order to retain a robust and secure IM/IT capability/infrastructure. Specific examples of tasking includes development of guidance and draft policy language for patient access to the internet over wireless networks in Medical Treatment Facilities, development of a technical audit standard for all network protection appliances and enterprise servers (for use by CIOs at MTFs), development of a Reference Implementation Model for technical and Organization metrics and performance measurement by NAVMED Leadership, review of clinical systems as part of the compliance and governance process, and development of the Department of Defense /Intelligence Community (DOD/IC) security overlays recommended to NIST for inclusion in Special Publication (SP) 800-53 revision 4. SRS also supports NAVMED by providing Risk Management services including Vulnerability Assessment and Threat Identification. The Reference Implementation Model developed and deployed by SRS improved the efficiency and effectiveness of performing security reviews and analysis of IM/IT Systems while providing leadership with summary trending data. In addition SRS is tasked with Cyber Security Inspections (CSI) Stage II support. For this task, SRS provides support to the US Cyber Command (USCYBERCOM) Command Cyber Security Inspections (CSI) Stage II readiness team. SRS travels to sites selected for inspection by the FLTCYBERCOM (C10F) Office of Compliance and Assessment (OCA) to assess the security of Navy networks through a comprehensive, graded inspection involving all Cyber Security areas, specifically: Leadership Management, Physical Security, Administration, Training, Network Configuration, Network Operations, and Human Factors and Command Operational Behavior.			

Table 4: Past Performance 3: Security Vulnerability Testing: Army National ESS DIACAP Support

Security Risk Solutions (SRS): Army National Guard Electronic Security Systems			
Contracting Organization	Department of Defense	**Performance Period:**	August 2008 – Dec 31, 2014
Description and relevance to solicitation requirements:			
SRS was tasked with planning and executing all aspects of security Certification and Accreditation (C&A) planning and execution for the Army National Guard Electronic Security Systems which reside on various Guardnet locations throughout the US. Through the Space and Naval Warfare (SPAWAR) Systems Center Atlantic, SRS has been involved in architecting a multi-configuration Enterprise Security System for the National Guard Bureau and conducting security testing to obtain a system accreditation for ESS configurations. The system received an Authority to Operate (ATO) - the first of its kind for a type accredited ESS system- and is currently being deployed by the National Guard throughout the US. Key components included in the design and technical security review of various components, including hardware panels, database systems, access control systems, firewalls, and control center systems. These systems utilize Cisco firewall equipment, virtual machines, Microsoft .net, SWL, and a variety of other third party systems. SRS built on its strong track record in architecting secure configurations and performing DIACAP services in this environment, creating accreditation packages (including test results) that map to DoD baseline controls as well as NIST SP800-53 controls (as described by NIST SP 800-37). SRS authored the Security Architecture Description documentation, the DIACAP executive package, preliminary ST&E report, DIACAP sustainment plan, and Configuration Control Board process. SRS tested new components and updated the hardware/software baseline to include additional surveillance components such as intelligent video, sensors, new control center software, RF/wireless components etc. SRS sustained the accreditation by providing updates to the Plan of Action & Milestones (POA&M), liaising with the ESS Component Vendors to produce security updates and fix any vulnerabilities identified by SRS. SRS received vendor updates and performs Independent Verification and Validation (IV&V) before submitting to the CCB for approval.			

3 Mandatory Requirements

3.1 Mandatory Contract Services Requirements and Deliverables

Contract Services will meet or exceed the mandatory requirements listed below:

3.1.1 Relevant Staff Experience

Primary persons responsible for the engagement have a minimum of 5 years of experience in security design and testing of Microsoft .Net, Microsoft SQL Server, and Cisco Systems Networking. Copies of professional certifications which support this requirement are included at Appendix A, and Resumes are included at Appendix B.

SRS consultants are experienced, trained, and certified security professionals with a broad range of information security skills. Our staff of security and privacy experts holds degrees including Ph.D. and L.L.M., and/or internationally recognized security certifications backed with many years of credible and relevant experience. Professional certifications currently held by employees include **OSCP (Offensive Security Certified Professional), CISSP**, ISSEP, CISM, ITIL, CBCP, CBRM, Security+, CRISC and PMP. Copies of any staff certifications and degrees applicable to this project are attached at the Appendix, and are summarized in the Labor Matrix Table below.

SRS security experts have authored research papers, technical notes and book contributions which have been published and presented at international conferences. SRS are widely recognized as an authoritative source for policy and technical issues concerning several aspects of IT security and compliance. For example, staff from SRS and ACG contributed to the DoD Privacy Overlay for NIST SP 800 53r4 Appendix J, and participated as part of a DoD team which provided recommendations to NIST for improvement to NIST SP 800-53r4, which is a mandatory part of the NIST SP 800-37 process. All projects were completed successfully, on-time, on-budget, and without any negative action or complaint.

The staff proposed as part of the SRS team all have the necessary knowledge and experience required for successful completion of this project. Our staffing plan combines the proven leadership, program management skills, subject matter expertise, and industry and government relationships necessary. We are confident that our team will be able to effectively elicit the necessary information from representatives from participating WV Consolidated Public Retirement Board (CPRB) Offices, WV Office of Technology (OT) Offices, and organize the data in such a way that is usable and informative for the roadmap and subsequent recommendations. Our technical staff is well versed in network discovery, vulnerability assessment, penetration testing and physical security reviews. Our Security Experts are adept at efficiently facilitating Risk Assessments, can skillfully analyze Policies and Procedures and leverage their experience to provide a comprehensive regulatory compliance gap analysis and corrective action plan based on industry best-practices and Federal requirements.

Table 5: SRS and Key Personnel Project Experience

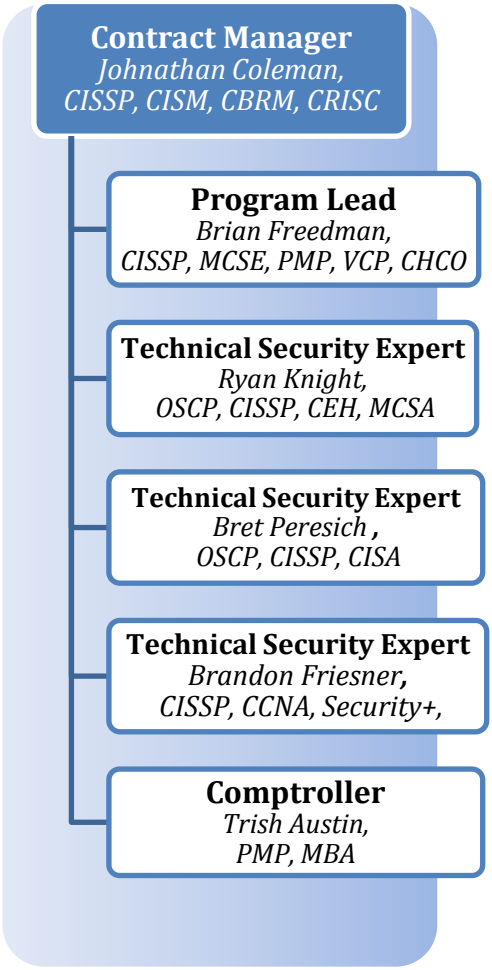
Client/Location	Project Focus	Reference Name/Contact Info	Relevance to Solicitation				
			Risk Assessment	Technical Vulnerability Assessment	External Penetration Testing	Physical Security Analysis	Policies and Procedures Review
Army National Guard Bureau	Security Risk Assessment, Applications Assessment	Tyrone (Vince) Patenaude tyrone.patenaude@navy.mil Tel: (843) 218-4197	✓	✓	✓	✓	✓
Comparative Billing Reports (CBR) Producer System for the Centers for Medicare & Medicaid Services (CMS) /Charleston SC & Washington DC	FISMA Audit and Security Risk Assessment (NIST SP 800-37/53)	Cornelia Dorfschmid cdorfschmid@strategicm.com Tel: (703) 683-9600, x.419	✓	✓	✓	✓	✓
Navy Medicine Information Systems Support Activity (NAVMISSA) /Multiple US hospitals throughout USA, Asia and Europe	Security Testing and Evaluation, Risk Assessment, Compliance, and IT Contingency Planning for 29 Major Hospitals and 27 Major Information Systems, with approximately 55,000 users and 86,000 end nodes.	Chris Cotton Chris.Cotton.ctr@med.navy.mil Tel: (804) 417-7699	✓	✓	✓	✓	✓
Georgetown University Medical Center (GUMC)/ Washington DC	Security Risk Assessment	Jeff Collmann, PhD collmanj@georgetown.edu Tel: (202)-870-2196	✓	✓	N/A	✓	✓
National Institutes of Health (NIH) / Bethesda, MD	Federal Safety Reporting Portal (SRP) Technical Risk Assessment and Certification & Accreditation	Latif Khalil LKhalil@JBSInternational.com Tel: (240) 645-4124	✓	✓	✓	✓	✓

As shown in Figure 1, our staffing plan consists of an experienced and proven Program Lead, a qualified Contract Manager, several Technical Subject Matter Experts, and the necessary program support staff.

Figure 1: Staffing Plan

KEY PERSONNEL PRIMARY FUNCTIONS

- **Contract Manager:** Responsible for overseeing all Vendor's responsibilities under this Contract. As a recognized industry expert, contract manager will also participate in assessment activities and provide Quality Assurance for technical testing, mitigation planning / roadmap development tasks, and executive briefings.
- **Program Lead:** Responsible for day-to-day execution of the project. Has deep experience managing large scale projects and conducting Security Vulnerability Assessments and Penetration Tests.
- **Technical Security Experts:** Provide technical vulnerability testing, penetration testing, analysis, including network discovery, vulnerability detection, false-positive determination and technical writing.
- **Comptroller:** Manages subcontractor budget allocation, financial burn rates, spend plans, subcontract management, subcontract invoice review and audit, quality control, monthly financial report development, program risk management.



Proposed staff are full time employees of SRS (prime contractor) or ACG (subcontractor). Although SRS has experienced very little employee turnover over the last decade, we recognize that it is always a possibility. In the event a proposed technical security expert leaves current employment or otherwise becomes unavailable over the course of the lifespan of the contract, they will be replaced with another technical expert of similar experience and credentials. In the unlikely event of any employee turnover, SRS will work closely with the client to ensure there is no disruption in service or overall impact to the schedule. Table 6 demonstrates the qualifications and certifications held by individuals proposed and available to support this project.

Table 6: Staff Qualification Matrix

Name	Proposed Role	Employer	Certification(s)	Degree/Professional Training	Years' Experience
Johnathan Coleman	Contract Manager/ Technical Security SME	SRS	**CISSP**, CISM, CBRM, CRISC	BEng, Aeromechanical Systems Engineering	20+ years
Brian Freedman	Program Lead/ Technical Security SME	SRS	**CISSP**, MCSE, PMP, VCP, CHCO	MS, Information Systems	20+ years
Ryan Knight	Technical Security SME	ACG	**OSCP, CISSP**, **CEH**, **MCSA**, Security+	BS *(in progress)*, Information Assurance and Security	15+ years
Bret Peresich	Technical Security SME	ACG	**OSCP, CISSP**, CISA	BS, Computer Information Systems and Security	15+ years
Brandon Friesner	Technical Security SME	SRS	**CISSP**, **CCNA** Security+,	MS, Systems Engineering	20+ years
Trish Austin	Financial Comptroller	SRS	PMP	MBA, Finance	15+ years
Personnel Below Available for Surge Support					
Jeanne Burton	Quality Assurance SME	SRS	PMP	Trained US Navy Cryptologist	30+ years
Michael Davino	Technical Security SME	SRS	**CISSP**	MS, Computer Science	30+ yearas
Amber Patel	Privacy/Security Policy Analyst	SRS		PgDL/LPC, Law LLM, Master of Laws	10+
Ronald Krutz	Technical Security SME	SRS	**CISSP, ISSEP**	PhD, Electrical and Computer Engineering	30+ years

Reference information is included on Attachment 2. All Information Security and Network Vulnerability Assessments were conducted in accordance with the National Institute of Standards and Technology Standards referenced in Section 3.3 of the RFQ.

3.1.2 Prioritize and rank the discovered vulnerabilities using the Common Vulnerability Scoring System (CVSS)

As a part of the U.S. governments SCAP (Security Content Automation Protocol), SRS understands the use of CVSS for standardizing and automating vulnerability management. Outputs will include an evaluation of the security policies and procedures, scans of the external entry points into the network, a review of all discoverable devices on the network, and review configurations for the server, firewall, and IDS configurations. SRS will work with the client to provide detailed recommendations for mitigating, remediating, and addressing all vulnerabilities identified.

The SRS team will validate output from the software tools used to generate the risk rating of existing vulnerabilities and exploits. SRS tools such as Retina and NESSUS use the MITRE

Common Vulnerabilities and Exposures (CVE®) and CVSS schema to baseline initial risk rankings. The SRS team validates each vulnerability and category of vulnerability to ensure that its risk ranking is relevant and not already mitigated down. For example, a "high" impact vulnerability on a system may in fact have been mitigated to a low impact based on other factors (e.g. a device in a segmented VLAN with network traffic restricted to "outbound only").

3.1.3 Evaluation of the security policy and procedures

The SRS Security Assessment methodology incorporates a comprehensive Gap Analysis of the policies and procedures in place. SRS has substantial knowledge of most of the applicable WV policies and procedures, and has recently conducted an in-depth review for WV CHIP, WV PEIA. This review also included a review of the applicable WVOT policies and procedures, as well as overarching State requirements. Our evaluation will include a gap analysis of the existing policies and procedures against those described by NIST SP 800-37 and 800-53. This review will determine:

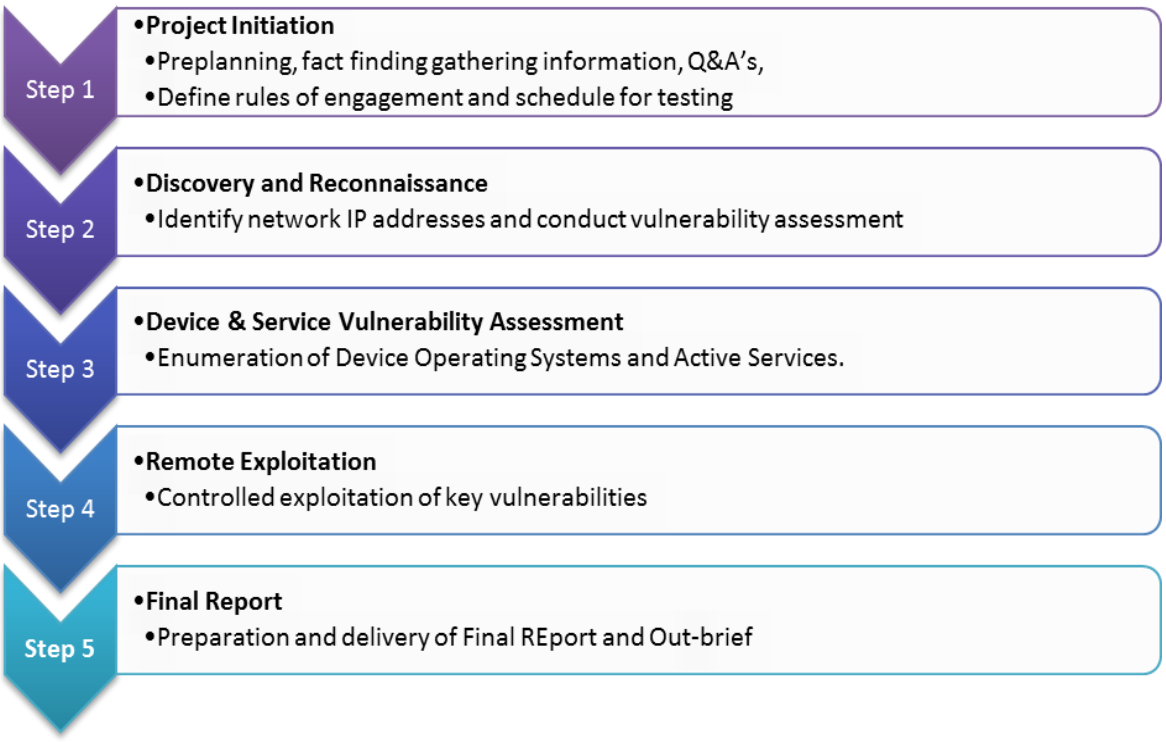
- Policies and Procedures that are missing
- Policies and Procedures that are incomplete
- Policies and Procedures that are not fully implemented

In addition, SRS will highlight areas of excellence and draw upon industry best practices, such as NIST guidelines, for recommendations to close gaps or enhance any practices which are considered minimally sufficient. The recommendations associated with any gaps and improvement on current practices will serve as the basis for the compliance "get well plan" portion of the written deliverables.

3.1.4 Scan of external entry points into the network

Our methodology for identifying access points is consistent with industry best practices, and finely tuned to result in an effective and efficient yet comprehensive process. It is based on techniques used to conduct external penetration tests, as well as internet facing application assessments. Together, these techniques cover the full spectrum of potential access points to the Covered Entities' networks. A recent example of our successful approach in penetration testing is in our work for a Federal Agency. Under this task, SRS provides the full range of technical, management and operations services associated with ensuring all aspect of FISMA reporting are being met, while also performing the lead role in all ST&E activities for the system, including Penetration testing. Our tasking also includes a review of technical specifications and artifacts of system evidence, the development of all Certification and Accreditation artifacts including System Security Plan (SSP), Information Security Risk Assessment (ISRA) and Contingency Plan (CP) as well as creation and mitigation of multiple Corrective Action Plans (CAPs) and the initial draft of the SSP Workbook. Through these activities, SRS helped the operational, development, and design teams to ensure regulatory requirements are adhered to and that the security requirements are appropriately documented and implemented. As a detailed example of our hands-on experience, the following bullet points are included to demonstrate (at a high level) our overall understanding and implementation of our 5-step methodology as used for the penetration testing portion of the ST&E activity. The penetration testing portion of the ST&E task consisted of 5 primary steps as shown in Figure 2: Penetration Testing Methodology Overview:

Figure 2: Penetration Testing Methodology Overview



3.1.4.1 Example of Penetration Testing Methodology Utilized by SRS:

- The SRS team scanned the IP address space registered to via external access in order to assess the Internet facing network infrastructure for vulnerabilities. The external investigation began with an initial information gathering/discovery step to enumerate hosts belonging to the client assigned IP address space. This discovery phase was completed in lass then two days. Following the discovery, additional testing was targeted to specific IP addresses in order to fully evaluate the potential access points that were discovered. This goes beyond the basic "ports, protocols, and services" testing: in this instance, testing objectives were to gain access to and obtain data from external devices, devices located on a DMZ or 'extranet', and devices located internally to the client organization. Security areas investigated included: network security, host level security, service level security, and application level security. External facing devices in scope for testing included, but were not limited to: routers, firewalls, web-servers, Email servers, file servers, database servers, and other accessible hosts that could be identified. A preplanning meeting was scheduled to communicate testing rules of behavior, and for identification of testing address hosts or networks that may be out-of-scope for testing. Specific exclusions to testing were documented (e.g. Denial of Service attacks on production systems).
- SRS implemented the following measures to minimize risk during the engagement:
    - During the project initiation meeting, testing windows were defined. In this instance, testing was restricted to off-peak hours.

- SRS and the customer defined "Rules of Engagement" before project initiation, and discussed risk tolerance and any special circumstances.
- SRS established an emergency contact plan, including event triggers that would require notification or escalation.

3.1.5 Review of all of the devices on the network with static IP addresses:

The techniques used meet Federal Standards for Certification and Accreditation (e.g. NIST SP800-53 revision 4) and include a full analysis of the often massive amounts of resulting data. These assessments typically include internal assessment and external assessments.

Those internal assessments involve a full scan of all available hosts, with elevated credentials, in order to fully and rigorously identify any known vulnerabilities on the systems. Typical vulnerabilities span the gambit from missing software patches and out of date virus definitions, to unlicensed applications and weak passwords. SRS staff also conduct activities that cannot be readily addressed by scanning tools alone, such as auditing system administrator account activities, validating application of least privilege principles, testing router and firewall configurations, reviewing network topology for defense in depth and architecture best practices, verifying employee training records against staff rosters, and testing (through spot-checks) employee understanding of organizational policies and procedures. All aspects of organizational policies and procedures are in scope for the assessment, and compliance is measured against NIST special publications, ISO standards, CVE / CVSS vulnerability database information, and regulatory language in appropriate Federal Register preamble and document entries.

We refer to the technical phase of the Assessment as the Security Test and Evaluation (ST&E) phase, and include penetration testing (external) and vulnerability testing (internal). Our team has extensive experience in providing ST&E support for its customers, having completed over 50 ST&Es on Federal programs and networks over the previous decade. The ST&Es have been conducted using Government approved standardized operating procedures (SOPs) and scoring methodology in accordance with Federal (NIST), and Department of Defense standards. Our team's ST&E efforts focused on predetermined targets of evaluation as directed by the customer, or as identified during the discovery phase. The ST&E assessment team holds several key certifications and unique and required qualifications such as the **OSCP (Offensive Security Certified Professional)**, Navy's Fully Qualified Navy Validator (FQNV) designation, as well as **Certified Information Systems Security Professional (CISSP)** and Certified Information Systems Auditor (CISA); these qualifications and certifications assist in demonstrating the necessary skills to complete thorough and successful ST&E events.

SRS has proven experience and credibility in performing technical assessments on Federal information systems, networks and applications. We have conducted numerous on-site and remote

> ***"Security Risk Solutions went above and beyond what we had expected from a computer security company. They were contracted to conduct a security vulnerability assessment/penetration test and were quite simply, impressed."***
> David C. Lewis, CISSP, Information Security Officer, IESO

vulnerability assessments on clinical systems and general support systems, and are experienced in performing disciplined and rigorous penetration tests. SRS has received written endorsements and customer appreciation/merit awards (e.g. Navy Bravo Zulu commendations) for our technical testing.

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

SRS is experienced and capable of providing the necessary reviews for various server, firewall and IDS configurations, as well as for other components typically considered part of a network security suite. Systems include inner and outer security screening routers, bastion hosts, DNS, DHCP, proxy servers, VPN devices, as well as automated scanning hosts, intrusion detection systems and web traffic monitors. Our services will include a network topology architecture review (to ensure defense in depth/network interfaces are documented and follow best practices), as well analysis to ensure security controls are implemented, consistent with security standards, configuration verification and validation. These tasks include manual review of configurations, as well as some automated testing using a variety of tools and open source applications.

Included in the assessment is a thorough host/server/network analysis. For servers in-scope for the assessment, SRS will verify that they are appropriately hardened, with all unnecessary services, ports and protocols disabled, as well as being appropriately configured to limit access to server resources to only authorized users. SRS tools utilize scans and checks for Unix, Linux, Windows and third party proprietary systems. SRS will also conduct a comprehensive search for unlicensed software, and for home-grown data repositories which may contain unsecured confidential or sensitive information.

SRS has Cisco certified individuals with specific experience on ASA 5505 and similar range of appliances. For example, SRS developed the Access Control Lists baseline configuration for ASA 5505 deployments routinely reviews and tests the effectiveness of the ACL baseline.

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

SRS will work with the prime contractor to ensure they have a plan of action and milestones (POA&M) describing in sufficient detail, the steps required to implement identified vulnerabilities. Since the assessment has not yet been conducted, and the scope of the potential vulnerabilities is not yet known, the nature and scope of post-assessment remediation services is difficult to quantify. SRS remains committed to the success of the WV Consolidated Public Retirement Board's project, and will provide reasonable and appropriate post-remediation services, based on the nature of the vulnerabilities identified.

3.1.8 Written Reports

For each assessment, SRS will produce a comprehensive written report, to include the following mandatory sections:

- Executive Summary
- Summary of Target Environment
- Scope (including systems assessed and method used)

- Findings (in social engineering, data loss prevention, firewall architecture and policy, and endpoint assessment)
- Recommendations (including "quick wins" and strategic recommendations)
- Baseline and cross-reference all observed deficiencies and associated recommendations to National Institute of Standards and Technology Special Publication 800-53(revision 4) and/or SANS Consensus Audit Guidelines
- Appendices (including evidence and screenshots, and raw results).

As previously described, SRS commits to ranking all vulnerabilities and risks. Risk rankings will be provisionally determined by the scanning tools (if they are the source of the finding), and validated according to outcome, impact, vulnerability severity, likelihood, and ease of exploitation.

All written reports go through an internal Quality Assurance review before delivery, and draft findings/recommendations are discussed with the customer (for accuracy/completeness) before being finalized in the report.

3.1.9 Firewall Architecture and Policy Review

3.1.9.1 Security Content Automation Protocol (SCAP) Approved Scanning Tool

As described in paragraphs 3.1.2 – 3.1.8 above, SRS will perform external automated vulnerability scanning using a variety of tools and manual techniques, including vulnerability scanning solution approved by the Security Content Automation Protocol (SCAP) to identify Internet-exposed weaknesses at the network and host level. SRS uses and is highly experienced with a variety of SCAP validated tools, including their configuration, use and understanding of their limitations. Per the RFQ validated products list and products listed on the SCAP Validated Products page (http://nvd.nist.gov/scapproducts.cfm) – SRS will download SCAP expressed checklists, import the SCAP expressed checklist into the SCAP validated tool, and scan computer systems assessing the configuration compliance with the checklist.

3.1.9.2 Identify deficiencies in firewall policy, architecture, and administration.

As described in the preceding paragraphs (3.1.2 – 3.1.9), SRS will use a variety of methods to identify potential vulnerabilities in the firewall policy, architecture and administration. Our staff includes individuals with Cisco and industry security certifications who are experienced and knowledgeable in ASA 5505 and similar appliances, as well as being experienced in the audit/review/testing of them. Methods include expert interview, paper analysis (e.g firewall rule review) configuration review, and direct observation.

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

As described more fully in paragraph 3.1.4, our methodology for identifying access points is consistent with industry best practices, and finely tuned to result in an effective and efficient yet comprehensive process. Steps used to quantify the attack surface include:

- Initial information gathering/discovery step to enumerate hosts belonging to the client assigned IP address space. This is done using a variety of tools, manual searches, and other discovery techniques.
- Verify hosts to be targeted (discussions with client/verification of ownership)
- Document internet facing nodes, interfaces, services, ports and protocols, and describe recommendations for reducing exposure. Examples may be geared towards architecture design (e.g. systems in DMZ, VPN configuration, use of VLANs etc) and/or focused on specific systems (e.g. unneeded ports/protocols).

The technical approach includes a full security gap analysis (all policies, procedures) and a technical assessment. The technical assessment incorporates an internal network vulnerability assessment, including network discovery, and credentialed/elevated vulnerability assessment to document the true status of the network infrastructure. It also includes a manual review of compliance/implementation status of the policies and procedures, including password policies, requirements for unique user IDs, and a manual review of all firewall rules, access control lists, VLAN configuration, and remote access solutions. In addition, an external technical assessment will be conducted, which uses penetration techniques to identify and test all external interfaces and document the ports, protocols and services running. SRS will also attempt to validate any of the identified vulnerabilities, and of course eliminate any false positives. Our team will prioritize any technical vulnerabilities found according to the severity, and will document findings in the "compliance roadmap" report and presentation.

3.1.10 Endpoint Assessment

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

SRS will conduct automated scans, as required by the RFQ. In addition to any requisite scans conducted using SCAP validate tools, SRS will utilize manual methods to check any identified vulnerabilities for false positives. With express permission from the client, SRS will attempt to exploit vulnerabilities identified in the sampling of endpoints in order to determine if they (a) can be used to potentially disclose confidential information, and (b) if they can be used by a potential intruder as an entry point into the network where other systems and information by be subsequently compromised.

SRS will provide all raw results, as well as consolidated results and executive summaries of scan results. Results will be ranked and mapped to NIST SP 800-53 and will be supplemented with detailed steps for mitigation.

All security findings will be properly documented so that they can be verified, undisputed, and replicated if necessary (for testing and validation purposes). SRS will make sure that no detail is omitted when capturing details of any security findings. Examples of supporting evidence include screenshots, archives of audit data, credentials in use at time of access etc. A format consistent with recommendations for capturing data in the Incident Response Plan is used, so that if in fact the breach is real, the next steps for mitigation and breach notification determination can be implemented.

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

SRS has experience working with a number of security suites and appliances, and understands how to configure and validate configuration of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) so that they can be effective, without causing negative impacts to network or operational behavior. For example, SRS staff proposed for this engagement have been responsible for oversight and execution of the Navy Medicine Enterprise Perimeter Protection Group (PPG), Host Based Security System (HBSS), Enterprise Incident Response, and Public Key Infrastructure (PKI) Phase II projects. In this capacity, SRS staff fine-tuned a variety of processes and tools including NitroView System Information and Event Management (SIEM), Riverbed Steelhead WAN Network Optimization, and Network Protection Suites, and Network Operations and Support Center assets.

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

A critical part of any successful assessment project is development of the roadmap, or Plan of Action and Milestones (PO&M) for closing gaps and mitigating vulnerabilities. SRS addresses this by preparing high-level mitigation strategies, mapped directly back to risks and potential impacts documented through the analysis process. The high-level mitigation strategies are developed with the client, but leverage the deep experience and industry best practices that the SRS assessment team has developed with over a decade of experience in conducting assessments. The high-level mitigation strategies are formally presented to the client and discussed in terms of feasibility and customer buy-in, understanding resource constraints and the need to prioritize remediation activities.

In support of this prioritization conundrum, the SRS team presents mitigation strategies in the form of a “get well” plan, or compliance/risk corrective action roadmap. Resource estimates for each mitigation strategy will be provided in terms of cost (Rough order of Magnitude), timeline, and any additional resources needed to succeed, such as personnel).

3.1.11 Data Loss Prevention Gap Analysis

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

The network discovery process utilized as part of the vulnerability assessment will be used to identify network interfaces, egress points/demarcation points for information flow. These interfaces will be reviewed for potential vulnerabilities which may lead to inadvertent disclosure of confidential data. SRS will use manual means and technical tools to evaluate the

interfaces, which may include packet analysis/network traffic sampling. For systems outside of the network, but connected to it, SRS will leverage the "external" assessment techniques to validate ports, protocols and services open to interface with third party systems, inbound and outbound. SRS will use network sniffers to capture traffic traversing those interfaces and review for any signs of clear-text confidential data. SRS will also document all available information about the connecting systems, and provide recommendations for improving the security posture if appropriate (i.e. restricting use of unsecured protocols). In addition to the network tools, SRS will use interview techniques and manual technical tests to identify potential weakness. SRS has used these techniques very successfully in the past to identify vulnerabilities not readily detectable by many scanning tools (e.g. 3rd party vendor "storing" confidential information on a shared server).

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

Currently deployed technologies for responding to potential data loss for lost or stolen devices will be evaluated, tested and optimized. Additional solutions / methods will proposed as appropriate, and may include fine tuning of currently available technology to more fully enable the features. Examples include utilization of encryption on mobile devices, remote wipe capabilities, and remote tracking capabilities.

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

Similar to the roadmap discussed in section 3.1.10.3, the roadmap will include a prioritized list of recommendations for Data Loss Prevention mitigation, aligned with best practices and achievable within 18 months. Mitigation strategies will be presented in the form of a "get well" plan, or compliance/risk corrective action roadmap. Resource estimates for each mitigation strategy will be provided in terms of cost (Rough order of Magnitude), timeline, and any additional resources needed to succeed, such as personnel).

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

SRS will ensure that the completed DRAFT roadmap and reports are delivered to the customer for review, with adequate review time and consultation/discussion included. All comments will be addressed and discussed with the customer, and draft reports will be updated to reflect the outcomes of the discussions. Only then will the roadmap, presentations, and assessment reports be considered final and submitted to the customer for acceptance.

Along with delivery of the report will be a final-report out-brief and Question/Answer discussion. This gives executives, sponsors and other stakeholders opportunity to ask questions, dig deeper into findings or recommendations, and garner clarity and context which may not have been readily apparent.

SRS will also participate in vendor meetings at the request of the client, in order to provide support or assistance in fielding questions the vendor may have in response to the test results.

3.1.13 Evidence of the performance of a vulnerability assessment and/or penetration test on a government entity or corporation that has the minimum of 5,000 employees:

Table 7 highlights some of our past performance for organizations with over 5000 employees:

Table 7: Evidence of Assessments

Entity/Corporation Name	Approximate Employee Count	Project Name/Focus
State of West Virginia	30,000	Technical Vulnerability Assessment, Penetration Testing, Risk Assessment
US Navy	45,000	Vulnerability Assessments, Continuous Risk Management,
Army National Guard Bureau	358,200	Technical Vulnerability Assessments

Appendix A: Resumes for Personnel Proposed

Johnathan Coleman, *FQNV# I0627, CISSP, CISM, CBRM, CRISC*

INSTITUTION AND LOCATION	DEGREE (IF APPLICABLE)	YEAR(S)	FIELD OF STUDY
Royal Military College of Science, Shrivenham, England	BEng (Bachelor of Engineering)	1992	Aeromechanical Systems
6 Military Intelligence Company, England	N/A	1994	Information Security
Royal School of Signals, Blandford, England	N/A	1996	Cryptology and INFOSEC

2005 - Present: Mr. Coleman is the Principal Consultant at Security Risk Solutions, Inc., a small, woman owned vendor neutral consulting business specializing in Information Security Risk Management. Since 2009, he has served as a Subject Matter Expert (SME) at Space and Naval Warfare (SPAWAR) Systems Center Atlantic supporting NAVMISSA's Navy Medicine (NAVMED) Enterprise CyberSecurity (ECS) Program. During this time, he has provided technical and policy expertise in the area of Risk Management, HIPAA Security, and participated as a senior member of the Cyber Security Audit team charged with preparing Navy Hospitals for compliance audits. In this capacity, he led and performed numerous technical risk assessments designed to address specific requirements needing additional validation on complex technical issues. Examples include conducting a technical assessment to recommend a configuration for the DoD/VA PKI Root Certificate cross-trust deployment (for Federal Health Care Center [FHCC] / Naval Hospital Great Lakes and subsequently the rest of the enterprise). As another example, Mr. Coleman led and conducted the Joint Task Force-National Capital Region Medical (JTF CAPMED) assessment to identify the risk associated with implementing changes in the Enterprise Services Active Directory (AD) Domain Controllers, Firewalls, and VPN devices necessary for establishing an AD trust relationship between the JTF-CAPMED and Navy forests. Other work for the Navy Medicine Enterprise enterprise (approx. 2100 bed capacity) includes reviewing and updating Incident Response Plan (IRP) methodologies for the CERT/IRP teams in order to address new requirements (e.g. HIPAA breach notification reporting introduced as part of the HIPAA Omnibus Rule).

Mr. Coleman was also responsible for designing, prototyping and implementing the Risk Management Framework (RMF) for NAVMED, whereby results from various functional teams are captured in an executive-level reporting dashboard with drill-down capabilities so that leadership can see IA risks across the enterprise as well as the supporting detail for each hospital or branch clinic. Mr. Coleman served as part of the USCYBERCOM directed Command Cyber Security Inspections (CSI) Stage II readiness team. The team traveled to sites selected for inspection by the Department of Defense to assess the health and security of Navy networks through a comprehensive, graded inspection involving all Cyber Security areas, specifically: Leadership Management, Physical Security, Administration, Training, Network Configuration, Network Operations, and Operational Behavior.
Mr. Coleman has supported the U.S. Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC) by leading the standards and interoperability projects for Data Segmentation for Privacy and the Prescription Drug Monitoring Program. He worked closely with the Chief Privacy Officer at ONC to develop materials for presentation at HIMSS2014 on HIPAA Security Risk Assessments, and to conduct development, testing and evaluation for security and privacy standards for adoption by the Centers for Medicare and Medicaid Services (CMS) Meaningful Use Certification Program for the certification of Electronic Health Records (EHR) systems.

Previous work with ONC includes participation on the American National Standards Institute (ANSI) team as a contractor to the Health Information Technology Standards Panel (HITSP) to harmonize standards for seamless and secure electronic exchange of patient data. He co-chaired the HITSP Security, Privacy and Infrastructure ARRA tiger team which was chartered by HHS to develop Interoperability Specifications to meet the requirements of the AHIC Use Cases and new provisions under HITECH. In this capacity Mr. Coleman provided testimony to the National Committee on Vital and Health Statistics (NCVHS) (the advisory committee to HHS), to the National Governors Association (NGA) State Alliance for eHealth, and to the Federal Health Architecture (FHA) Security Strategy Committee, and has participated as an invited speaker at a seminar hosted by NIST/CMS on HIPAA Security Rule Implementation and Assurance.

In addition to his work at HHS, Mr. Coleman assists organizations with the development and implementation of information security programs including information security needs analysis, regulatory compliance, organizational resiliency planning, institutionalization of Risk Assessment and Business Impact Analysis (BIA)

methodologies, and facilitation of regulatory compliance reviews. Mr. Coleman has demonstrated experience with government agencies and commercial organizations in developing and analyzing complex computing systems in terms of security requirements, and mapping those requirements to the organizations' mission. He has participated as a lead auditor in numerous Security reviews, providing compliance gap analyses and recommendations which have been used in the development of remediation plans. Other tasking currently includes providing SME support for a joint Food and Drug Administration (FDA) and National Institutes of Health (NIH) sponsored Adverse Event Reporting (AER) project. In conjunction with Georgetown University Medical Center, he supported the Intelligence Community on a Biosurveillance and early warning system which operates as a primer for U.S. countermeasure response plans in the context of a potentially catastrophic bio-event.

He is a Navy Certification Authority (CA) Fully Qualified Navy Validator (FQNV), a Certified Information Systems Security Professional (CISSP), accredited by the International Information Systems Security Certification Consortium and is a Certified Information Security Manager (CISM) and Certified in Risk and Information Systems Control (CRISC) as accredited by the Information Systems Audit and Control Association (ISACA). As a Visiting Scientist at the Software Engineering Institute/ CERT® Coordination Center (SEI/CERT) at Carnegie Mellon University, he participated in research, training and delivery of the Operationally Critical, Threat, Asset and Vulnerability Evaluation (OCTAVE®) and Mission Assurance Analysis Protocol (MAAP).

Published work can be found at http://www.securityrisksolutions.com/publications.html and includes:

- **Protecting High Stakes PHI;** Journal of AHIMA; *April 2014, ©2014 American Health Information Management Association*
- **Meaningful Use Risk Assessments: Requirements, Methodology, Challenges and Lessons,** Joint presentation / education session with the Chief Privacy Officer, Office of the National Coordinator for Health IT, Department of Health and Human Services. *J.Pritts, JD & J.Coleman: HIMSS 2014 Conference and Exhibition, Orange County Convention Center, Feb 2014*
- **Extra-Sensitive PHI: Appropriate Sharing using Data Segmentation for Privacy** *HIMSS 2013 Conference and Exhibition, March 5th 2013, Ernest N. Morial Convention Center, New Orleans, LA*.
- **Segmenting Data Privacy;** Journal of AHIMA *February 2013 ©2013 American Health Information Management* Association
- **Privacy Protection for Substance Abuse Treatment Information** Presentation on behalf of the Data Segmentation for Privacy Initiative, Office of the Chief Privacy Officer, Office of the National Coordinator for Health IT, Department of Health and Human Services, *HIMSS 2012, February 23, 2012, Sands Convention Center, Las Vegas, NV.*
- **Privacy Consent and Access Control: Cross Enterprise Security and Privacy Authorization (XSPA)** Presentation and Advanced Technology Demonstration on behalf of the Organization for the Advancement of Structured Information Standards (OASIS), *HIMSS 2009, April 4-8 2009, McCormick Place, Chicago IL.*
- **Presentation to Federal Health Architecture (FHA) Security Strategy Committee:** Briefing on relationship between FISMA, HIPAA, NHIN, CCHIT, and HITSP. *November 7, 2008; Department of Health and Human Services, Washington DC.*
- **NIST/CMS Workshop: HIPAA Security Rule Implementation and Assurance**; Presentation on HITSP Security and Privacy Standards *January 16, 2008; NIST Main Campus,100 Bureau Dr, Gaithersburg,MD*
- Acknowledged Contributor: **Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process** *Richard A. Caralli et al; May 2007 Technical Note CMU/SEI-2007-TR-012 ESC-TR-2007-012;* © Copyright 2007 Carnegie Mellon University
- **Testimony to the National Governors Association (NGA) State Alliance for e-Health, Health Information Protection Taskforce** on behalf of the Healthcare Information Technology Standards Panel (HITSP). *April 25, 2007; Hyatt Regency, Crystal City*
- **Presentation on behalf of the Healthcare Information Technology Standards Panel (HITSP)** *on Requirements, Design and Standards Selection for the Security and Privacy Technical Committee Town Hall, April 19, 2007*
- **Presentation on behalf of the Office of the National Coordinator (ONC) for Health Information Technology** *1st Nationwide Health Information Network Forum: Functional Requirements for Security; Authorization,*

Authentication, Confidentiality, and Credentialing June 28-29, 2006; Natcher Center, National Institutes for Health

- **Position Paper on the Critical Infrastructure Protection Center DITSCAP Automated Tool Initiative;** J.Coleman, CISSP, CISM *Space and Naval Warfare Systems Center, Intelligence and Information Warfare Department, Critical Infrastructure Protection Center*, March 2005
- Acknowledged Contributor: **Applying OCTAVE: Practitioners Report;** Carol Woody, PhD; Technical Note CMU/SEI-2006-TN-010, May 2006; © Copyright 2006 Carnegie Mellon University
- Acknowledged Contributor: **Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments;** Christopher J. Alberts, Audrey J. Dorofee; Technical Note CMU/SEI-2005-TN-032 September 2005; © Copyright 2005 by Carnegie Mellon University
- **Assessing Information Security Risk in Healthcare Organizations of Different Scale**; J.Coleman; *International Congress Series Special issue: CARS 2004 - Computer Assisted Radiology and Surgery. Proceedings of the 18th International Congress and Exhibition*, Reference: ICS3932 Vol 1268C pp 125-130, © Elsevier, 2004 *Presented at the Computer Assisted Radiology and Surgery Congress*, *Chicago*, *2004*
- **HIPAA Program Reference Handbook**; *edited by Ross Leo*; Chapter 6; ISBN: 0849322111 CRC Press, © Auerbach Publications, 2004
- **Medical Information Assurance Readiness Teams: An Interdisciplinary Approach to Information Assurance;** J.Coleman, CISSP, CISM; *Presented at the 2003 American Telemedicine Association Annual Meeting*, Orlando, Florida, April 2003
- **Organizing Safety: The Conditions for Successful Information Assurance Programs;** Jeff Collmann, Ph.D, J.Coleman CISSP, CISM, Kristen Sostrom, Willie Wright, M.B.A.; *Journal of Telemedicine and eHealth,* Sep 2004, Vol. 10, No. 3: 311-320
- **A Risk Assessment Approach to HIPAA Security;** J.Coleman; *Presented at the Annual Meeting of the South Dakota Chapter of the Healthcare Financial Management Association, April 2004, Sioux Falls, SD*
- **Execution of a Self-Directed Risk Assessment Methodology to address HIPAA Data Security Requirements;** J.Coleman, CISSP, CISM, *PACS and Integrated Medical Information Systems: Design and Evaluation; Progress in Biomedical Optics and Imaging;* SPIE (International Society for Optical Engineering), Vol., No. 24. ISSN 1605-7422, Feb 2003, *Presented at the PACS and Integrated Medical Information Systems Conference, San Diego, CA, Feb 2003*

Milton Brian Freedman *MS, CISSP, PMP, CHCO*

INSTITUTION AND LOCATION	DEGREE (IF APPLICABLE)	YEAR(S)	FIELD OF STUDY
University of Miami, Coral Gables, FL	BS (Bachelor of Science)	1994	Speech Communications / History
Strayer University, Washington, D.C.	MS (Masters of Science)	2010	Information Systems

CITIZENSHIP AND CLEARANCE: US Citizen, DoD Top Secret

2014 - Present: Mr. Freedman is a Senior Information Assurance Analyst at Security Risk Solutions, Inc. In this capacity, Mr. Freedman leverages deep project management and technical experience in order to lead key elements to several Health-Information Technology (IT), Privacy and Security initiatives. One specific example includes Mr. Freedman's role as Deputy Program Manager for a large State of West Virginia HIPAA Security Risk Assessment effort. This effort involves a deep HIPAA Security Rule assessment on behalf of multiple State agencies in order to ensure compliance and program maturity. He helped to design and develop solutions that allowed the State of West Virginia to manage diverse risks through a consistent, coordinated, and sustainable strategy.

Mr. Freedman has also provided direct support to the Office of the National Coordinator for Health Information Technology (ONC) on an in-depth security risk assessment of the DIRECT Certificate Discovery Tool (DCDT). This tool was created to support automated testing of systems planning to enact the Certificate Discovery and Provider Implementation Guide, which was approved as a normative specification by the DIRECT community. It is based on the written test package and requirement traceability matrix created by the Modular Specifications project under the direction of the ONC and National Institute of Standards and Technology (NIST). In support, Mr. Freedman evaluated the implementation and effectiveness of the security controls associated with an information system according to NIST 800-53, revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. Additionally, Mr. Freedman's assessment of the DCDT application included an extensive system and web application penetration testing necessary to support comprehensive scan results and technical analysis.

Mr. Freedman also serves as an acting member on the ONC Federal Advisory Standards Committee Transport and Security Standards Workgroup. The workgroup is charged with making recommendations to the National Coordinator for Health IT on standards, implementation specifications, and certification criteria for the electronic exchange and use of health information.

Mr. Freedman is an Adjunct Instructor for the Department of Network Systems Management at a local Technical College where he teaches classes in Information Systems, Networking, Information Assurance and HIPAA and PCI compliance.

With over 20+ years of experience in Information Technology, Mr. Freedman has spent the past 15 years with a deep involvement with Information Assurance which has included security design and testing programs around application development and IT infrastructure. Application development security design and testing projects have been based on Microsoft .Net/C#, Java, and Python utilizing various database management systems such as Microsoft SQL Server, Oracle, and MySQL. Infrastructure testing has included technologies from Microsoft, Cisco, HP, NetAPP, EMC, VMWare, and several Linux distributions.

Mr. Freedman is a Certified Information Systems Security Professional (CISSP) accredited by the International Information Systems Security Certification Consortium, and is Project Manager Professional (PMP) as accredited by the Project Management Institute (PMI). Mr. Freedman has also earned the Certified HIPAA Compliance Officer Certification (CHCO) accredited by the American Institute of Healthcare Compliance (AIHC). He also holds several other technical certifications from Microsoft, Cisco, and VMware.

2012 – 2014: As Chief Information Officer for Palmetto Primary Care Physicians, one of South Carolina's largest independent primary care practices, Mr. Freedman was responsible for coordination and oversight of all operational and technology functions across 33 locations. He managed a team of system administrators and application specialists which supported the IT needs and electronic medical record / practice management system for the company. He also served as the organizations HIPAA Compliance Officer, drafting and/or rewriting all related policies and procedures for final rule, and designing and delivering corresponding HIPAA training program to more than 650 employees. Mr. Freedman also created and implemented an annual risk management / analysis program to focus on both HIPAA and Meaningful Use compliance. The risk management program he developed has provided Palmetto with a continuous risk management program. As a part of the risk management program, Mr. Freedman created a vulnerability security

design and testing program on all critical applications including the Electronic Health Record / Practice Management system, and network infrastructure which was based on Microsoft .NET, Microsoft SQL Server, and Cisco Networking technologies.

2009-2012: Mr. Freedman was a Program Manager (US Navy Civilian) for SPAWAR Systems Center Atlantic, managing projects with a total annual budget of over $30 million for the SPAWAR Department of Veterans Affairs program. He supervised project deadlines, task, and progress for projects involving over seventy contractors and employees. He produced the Agile Integrated Development Environment (AIDE), which is a mix of Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) for Veteran Affairs software development including IBM Jazz Rational Tools, Microsoft SharePoint, and virtualized servers in a cloud computing environment. Mr. Freedman's work for AIDE subscribed to an established software development lifecycle using the Agile SCRUM methodology.

2007-2009: Mr. Freedman was a Project Team Lead / Senior Systems Engineer for WareOnEarth Communications. In this capacity, he managed a team for the Enterprise Service Operations Center (ESOC) supporting over seventy sites worldwide and over 55,000 users for U.S. Navy Medicine (NAVMED). He supervised teams supporting Microsoft Office SharePoint Server (including application development with Microsoft .NET / C#), system and network monitoring, Microsoft SQL Server, database administration, engineering, system backups, hardware, and virtualization using VMware for the enterprise. Part of his responsibility was to develop a security design and testing program on Navy Medicine's Global Enterprise Cisco Network Infrastructure and Microsoft SharePoint which included custom applications developed in Microsoft .NET/C#, and a Microsoft SQL Server.

2007-2009: Mr. Freedman served as the Director of Infrastructure Services and Security for Benefitfocus, a leading provider of benefits technology. He managed the Infrastructure Services and Information Assurance Group, including help desk, system administration, networking, facilities, security and compliance. One of his projects included designing a build-out of the entire infrastructure of a new corporate campus including, but not limited to data center, security and fire systems, HVAC, power reliability (UPS and generator systems), and network cable plant. Mr. Freedman further managed all network/systems operations including setup and maintenance of firewalls, routers, switches, telecommunications, building control/automation, and servers in two production data centers and local offices. Mr. Freedman also served as the organization HIPAA Privacy and Security Compliance Officer developing all related policies and procedures. He also performed periodic risk analysis and network penetration testing to ensure network and applications security and integrity.

2001-2002: Mr. Freedman was a Senior Systems Engineer, for eGroup. In this capacity, he worked with statewide clients to design and support networks using Microsoft Server products, Cisco Hardware and backup/recovery solutions.

2000-2001: Mr. Freedman was the President and Business Owner of Flash Consulting, an IT services firm. In this capacity, he provided comprehensive computer, networking, security, database, and other IT support to local area businesses, such as Windows 2000/NT server installation, installation of Microsoft BackOffice products (Exchange, SQL Server, Internet Information Server, Proxy Server), penetration testing, policy creation, risk analysis, disaster recovery planning, backup and recovery solutions, software selection, and creation of database applications using both Microsoft SQL Server and Microsoft Access. Flash Consulting was successfully acquired by eGroup in 2001.

1998-2000: Senior Network Engineer for Universal Data Solutions where he worked with customers to design, implement and deploy server and application solutions.

1994-1998: Mr. Freedman worked in New York City for several companies including Lexis Counsel Connect, Internet Channel, and Paperless Office Enterprises.

Published work:

- **LogMeIn Rescue Product Review: To the Remote Support Rescue,** *Redmond Magazine, July 2010 ©2010 1105 Media Inc.*
- **Take the Pain Out of Backups,** *Redmond Magazine, March 2010 ©2010 1105 Media Inc.*
- **Repairs Made Easy,** *Redmond Magazine, August 2009 ©2009 1105 Media Inc.*
- **The IT Regulator and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments,** *Technical Editor, ©2008 Syngress*
- **PCI Compliance: Implementing Effective PCI Data Security Standards**, *Co-Author, ©2007 Syngress.*

Brandon Friesner, *FQNV# I0933, MS, CISSP, CCNA*

INSTITUTION AND LOCATION	DEGREE (IF APPLICABLE)	YEAR(S)	FIELD OF STUDY
Park University, Parkville, MO	BS (Bachelor of Science)	2008	Computer Information Systems
Southern Methodist University, Dallas, TX	MS (Master of Science)	2011	Systems Engineering

2012 – Present: Mr. Friesner currently serves as a Senior Information Assurance Professional for Security Risk Solutions, Inc., a small, woman owned vendor neutral consulting business specializing in Information Security Risk Management. In support of the Navy Medicine (NAVMED) Enterprise Cyber Security (ECS) Program, Mr. Friesner ensures the continuity of NAVMED Enterprise mission essential functions (MEFs) against a wide range of potential natural, environmental, and man-made threats by assisting Enclaves and Programs of Record (PORs) in the development and exercising of IT Contingency Plans (ITCPs) to comply with Federal /departmental policies and guidelines (e.g., FISMA, DoDI 8500.2, NIST, HIPAA/HITECH). Mr. Friesner focuses on the development and institution of an NAVMED Enterprise Risk Management Framework, technical risk assessment, and the security evaluation and strategy development to ensure networks, information systems, and data are adequately protected in accordance with DoD 8500.2, NIST 800-53, HIPAA/HITECH, and other applicable regulations and best practices. Mr. Friesner serves as the Information Systems Security Officer (ISSO), responsible for the management and execution of DIACAP and Configuration Management (CM) activities for the Army National Guard Electronic Security Systems (ESS) Version 2.0. Mr. Friesner performed requirements analysis, security testing and evaluation, remediation and mitigation, artifact development, and interfaced with the Certification Authority and the Designated Approving Authority to ensure concurrence. For the National Organization of Rare Disorders (NORD), Mr. Friesner worked as a contractor supporting the Software Development Team responsible for the design, development, testing, deployment, and maintenance of the NORD Medical Assistance Program (MAP). He has developed the Security Requirements Traceability Matrix which outlined baseline security controls commensurate with requirements specified in the HIPAA Security Rule and suggested security controls defined in NIST SP 800-53. He also developed and institutionalized the NORD MAP System Security Plan. Mr. Friesner has provided Information Security services to the Charleston County Aviation Authority (CCAA) to include authoring the CCAA Information Security Framework, which provides an overview and comparative analysis of three frameworks tailored to meet the needs of CCAA. The framework developed by Mr. Friesner identified a security control baseline for augmenting the PCI DSS V2.0 requirements with selected and targeted compensating controls from NIST SP 800-53 and OCTAVE Catalog of Practices V2.0. Also for the CCAA, Mr. Friesner developed organizational Information Security Policies and Procedures, as well as security specific plans, such as the Risk Assessment Methodology, Security Incident Response Plan, the Security Awareness and Training Plan.

2009 – 2012: During this period, Mr. Friesner served as an Information Technology Specialist (Information Security) for the Space and Naval Warfare (SPAWAR) Systems Center Atlantic. As a Navy Civilian, Mr. Friesner contributed to the research and development, design, implementation, administration, and support of the Navy Medicine Enterprise Architecture for the Navy Medical Information Systems Support Activity (NAVMISSA). From 2009-2010, he was designated as the Lead Project Engineer/Technical Risk Manager for the Navy Medicine Enterprise Perimeter Protection Group (PPG), Host Based Security System (HBSS), Enterprise Incident Response, and Public Key Infrastructure (PKI) Phase II projects. He developed and maintained common risk impact criteria for centrally managed assets, to include the Navy Medicine Enterprise Services, NitroView System Information and Event Management (SIEM), Riverbed Steelhead WAN Network Optimization, and Network Protection Suite Programs of Record, as well as all the Network Operations and Support Center assets. Mr. Friesner developed and executed an appropriate information security risk assessment methodology of the centrally managed assets and processes, to include creation and tracking of relevant risk management metrics. Mr. Friesner also developed and maintained CMMI Level 2 traceability and developed a roadmap for the implementation and traceability of ITIL Security Management process activities for the Navy Medicine Cyber Evaluation and Response Team (CERT) functions. From 2010-2012, Mr. Friesner served as Information Assurance Manager (IAM) for the Navy Medicine Enterprise Services Operations Center. His duties also included, in addition to serving as the IAM, the management and execution of the Navy Medicine Enterprise Information Assurance CERT Technical Teams, including: Enterprise Technical Risk Management, Information Assurance Directives Validation and Verification, Enterprise Technical Systems Support and Enterprise Incident Response and Analysis. In this position, Mr. Friesner conducted risk assessments, directives compliance and reporting, risk modeling, simulation, mitigation, intrusion prevention/detection analysis, and incident response for all centrally managed assets within the scope of the CERT. Mr. Friesner was responsible for establishing, implementing and maintaining the DoD information system IA program, and for documenting DoD Certification and Accreditation process for Navy Medicine networks and information systems located at SPAWAR Atlantic and Enterprise deployed Programs of Record. His efforts resulted in Navy Medicine Enterprise Services Operations Center's receipt of a three year Authority to Operate (ATO) from the Navy Certification Authority, a first for the organization. As the IAM, Mr. Friesner instituted the continuous monitoring of systems and the information environment for security-relevant events and configuration changes that negatively impact IA posture and periodically assessed the quality of IA control implementation against performance indicators such as security incidents, feedback from external inspection agencies, and operational evaluations. Based on these assessments, Mr. Friesner recommend changes or improvements to the implementation of assigned IA controls, the assignment of additional IA controls, or changes or improvements

to the design of the IS itself.

2005 – 2009: Mr. Friesner served as Systems Security Engineer for Science Applications International Corporation (SAIC), contributing to the research and development, design, implementation and sustainment of the Navy Medicine Enterprise Architecture for the Navy Medicine Information Management Command (NMIMC), in support of contract projects based out of the Space and Naval Warfare (SPAWAR) Systems Center Atlantic. From 2005-2006, Mr. Friesner served as a Lead Deployment Engineer for the Navy Medicine Enterprise Services and Active Directory team, responsible for the implementation and migration of an Enterprise Active Directory solution across Navy Medicine. Mr. Friesner administered network security and access devices, DNS, access control lists (ACL's), TCP/IP, systems management and monitoring technologies, and MS Exchange. He also provided training to on-site operators and performed System Operational Verification and Testing (SOVT) on deployed network security systems. From 2006-2007, Mr. Friesner supported the Navy Medicine Enterprise Engineering and Technical Services Team. His was responsible for the assessment and analysis of emerging technologies, translation of business requirements into IM/IT requirements, and assessment of proposed portfolio items against Enterprise Architecture views. Mr. Friesner also provided project management support, technical evaluation and recommendation, and information assurance consulting services to Navy Medicine. From 2007-2009, Mr. Friesner served as the Lead Project Engineer for the Navy Medicine Enterprise Host Based Security System (HBSS) project, duties included: project initiation, planning, technical design, configuration, and deployment preparation tasks. He conducted in-depth research, evaluation, and testing in the development of the Navy Medicine Enterprise HBSS architecture. Mr. Friesner provided subject matter expertise and advanced solutions relating to all technical aspects of the Navy Medicine Enterprise HBSS deployment to include: deployment coordination and preparation, hardware selection and procurement, technical training and documentation, and management of personnel.

2003 – 2005: During this period, Mr. Friesner worked for WareOnEarth Communication, Inc. as a Network Engineer. While with this Firm, he provided subject matter expertise to the Space and Naval Warfare (SPAWAR) Systems Center Atlantic, specifically the Military Health Systems program. Mr. Friesner was responsible for the development and implementation of network security policies for small, mid-sized, and large Medical IT environments, to include the design, installation, implementation and maintenance of complex security network configurations. Mr. Friesner led the implementation of secure Internet connectivity solutions including firewalls, router ACL's, demilitarized zones (DMZ), VPN's, IDS's, and DNS. Mr. Friesner also contributed to the operation, design, and implementation of 802.11 technologies and standards for the Tri-Service Infrastructure Management Office (TIMPO). He deployed 802.11 wireless solutions providing encryption, authentication, data integrity checking, key exchange, and date compression to ensure integrity of enterprise applications and network resources.

1999 – 2003: Mr. Friesner served in the U.S. Marine Corps for four years with duty assignments with the II Marine Expeditionary Force (MEF). His primary responsibilities included the design, implementation, administration, and sustainment of network systems in support of operations worldwide, including both tactical and garrison. While serving with II MEF, Mr. Friesner provided network and systems support while deployed with the 22nd Marine Expeditionary Unit (MEU) Joint Task Force (JTF) in 2002 during Operation Enduring Freedom and with the II Marine Expeditionary Brigade, 8th Communications Battalion in 2003 during Operation Iraqi Freedom. Mr. Friesner's individual awards include the Global War on Terrorism Service Medal, National Defense Service Medal, Navy and Marine Corps Achievement Medal, Certificate of Appreciation, and two Sea Service Deployment Ribbons.

Ryan Knight, CISSP, C|EH, OSCP

Information Assurance Specialist

SPECIALIZED QUALIFICATION:
Information Technology and Information Security experience on various Dept. of Energy and Dept. of Defense projects including US Army, Navy, Air Force, and Marines. Focus on Information Assurance (IA) compliance testing and support.

CERTIFICATIONS:

CompTIA Certifications: A+, Security+, Network+
Microsoft Certifications: MCP, MCSA: Security Specialization
ISC2: Certified Information Systems Security Professional (CISSP)
C|EH: Certified Ethical Hacker
CNDA: Certified Network Defense Architect
OSCP: Offensive Security Certified Professional

CLEARANCE: Top Secret

SPECIFIC TASK EXPERIENCE:

Athena Consulting Group, North Charleston, SC 1/2007-Present

Navy Medicine- Computer Security Specialist

Key team member on the Controls Verification and Validation (CV&V) team for the Navy Medicine Information Systems Support Activity (NAVMISSA) and previously on the Mitigation and Remediation Support (MARS) team. Duties on these tasks include:

- Travel to Navy Hospital locations worldwide for scheduled visits to test site system security on all technologies and verifying that sites are complying with security standards set by DISA (Defense Information Systems Agency).
- Perform Information Assurance (IA) analysis, Certification and Accreditation (C&A), and Security Testing and Evaluation (ST&E) of DoD information systems in accordance with DISA guidelines.
- Develop detailed reports to ensure sites receive an informative document detailing how secure their environment is.
- Member of IV&V (Independent Verification & Validation) team.
- Perform wireless scanning (using Flying Squirrel and the Aircrack suite) to include penetration testing and rogue access point detection.
- Create POA&M (Plan of Action and Milestones) to allow sites to track progress for securing their environment.
- Perform Gold Disk Platinum and SCAP checks using the output to help develop mitigation strategies.
- Test 8500.2 IA controls to ensure site compliance
- Member of the IATT (Information Assurance Tiger Team) security response team.
- Utilize Hercules, LANdesk, SMS, SUS, and Group Policy to mitigate vulnerabilities for Navy

Hospital organizations.
- Scan and secure HP-UX devices for Navy Hospital organizations.
- Utilize the vulnerability scanning software Retina and REM.
- Generate vulnerability reports, showing an organizations security posture.
- Develop and execute plans for mitigating vulnerability reports.
- Travel to Navy Hospital locations for scheduled visits to prepare a site's network in preparation for their ATO (approval to operate).

Perform Penetration Testing and Social Engineering. These Penetration tests have been successfully performed for financial and medical institutions. Utilizing Kali/BackTrack, various WebApp testers, and Metasploit along with custom scripts and exploits I have successfully performed penetration for all contracts thus far. Utilizing the AirCrack suite, performed Wireless penetration successfully to include WPA2. Additionally, Social Engineering audio has been successfully recorded while retrieving PII/PHI data and account usernames and passwords. Upon completion of penetration testing efforts, the sites were provided a detailed vulnerability scan and risk assessment document that includes fixes, most urgent issues, and wireless mapping.

General Dynamics 07/2005-01/2007 *Sr. System Administrator*

While employed with General Dynamics, I supported the MC4 project (Army Healthcare) by managing the 3rd Infantry Division while located CONUS, and supporting the 10th and 47th CSH (Combat Support Hospitals) while deployed to Baghdad and Mosul, Iraq OCONUS. Duties on this task include:

- Assume role as Ft. Stewart site lead, supporting the 3rd Infantry Division.
- Administrator for the MC4 (Medical Communications for Combat Casualty Care) program.
- Ensure network connectivity to the 47th CSH (Combat Support Hospital) while deployed to Mosul, Iraq.
- Manage Cisco 3745 Router/VOIP phone system.
- Administer Windows 2000 member server providing DHCP, SMTP, and Oracle 8I services.
- Administer Windows NT Domain, user accounts, and a proprietary MUMPS Database.
- Administer CHCSII-T, and CHCS medical applications, accounts, and database integrity.
- Constantly evaluate and upgrade the networks computer security utilizing GFI LANguard, MBSA, Norton System Center, Windows Updates, Whats Up Gold, and Solarwinds Network Management suite.
- Provide MC4 Program support for northern Iraq while deployed (which involves supporting 10+ small networks via telephone, or actual site visits).
- Provide MC4 Program support for the eastern United States when not deployed.
- Function as a help desk for any computer related issues throughout the 47th CSH in Mosul, Iraq.
- Assisting in troubleshooting/setting up VSAT internet connections.
- Maintain MEDWEB servers to ensure 24hr uptimes, and safe shutdowns.

DS3 Computing Solutions 5/04-7/05 *Functional Systems Administrator*

Led IT related activities for the 23rd Fighter Group and 5 attached squadrons. Duties on this task include:

- Provided Internet connectivity/E-mail service to the Air Force as a civilian contractor.
- Ensured network connectivity to multiple locations.

- Administered Net IQ.
- Create RIS/Ghost images.
- Investigate and report misuse and abuse of government electronic equipment.
- Design/plan/implement network infrastructure including hardware components and software configurations.
- Utilize MBSA to detect software vulnerabilities.
- Trained associate Field Service Agents for ten hours each month.
- Backed up system state and data for file/print servers.
- Create/Delete/Modify/Troubleshot user accounts in both Win2000 Active Directory, and Net IQ.
- Administered file and print servers.
- Administered Norton System Center.
- Assisted in web site creation.
- Managed systems via SMS 2003.
- Lead special projects as designated by commanding personnel.
- Functions as Help Desk Manager over an entire Fighter Group consisting of 5 squadrons.
- Maintained $300K budget, along with training budgets.
- Create and evaluate RFQs (Request For Quote).
- Make any technology purchases for entire Fighter Group.
- Point of distribution for all technological equipment for Fighter Group.
- Point of authority for any computer/printer upgrades, or any IT product.
- Inventoried/Maintained Software Licenses, Hardware, Printer supplies.
- Designed and implemented computer replacement plan.
- Set up projection devices utilizing mirror for optimal display.
- Minor projection equipment repair.
- Purchased and configured Cisco Catalyst 3750 series switches.
- Maintained/Installed/Troubleshot Pairgain devices.
- Managed servers using Terminal Services (RDP).
- Supervised Fighter Group Technical Services staff, including assigning workloads and approving leave.

ITT Industries, Systems Division 11/03-05/04 *Systems Administrator*

Deployed to Iraq and Afghanistan with the US Army 63rd and 67th Signal Battalions. Duties on this task include:

- Provided Internet connectivity/E-mail service to the Army as a civilian contractor.
- Ensured network connectivity to multiple locations.
- Created both SIPR/NIPR Active Directory Forests.
- Administered Active Directory.
- Helped to commercialize equipment from the 63rd/67th Sig Bn.
- Create/Delete/Modify/Troubleshot user accounts in both Win2000 Active Directory, and Exchange 2000.
- Administered DNS, DHCP, WINS, Exchange 2000, SNAP! Server, Dell POWERVAULT.
- Administered Norton System Center.
- Assisted in SMS management.
- Utilized VMWare to test changes on private network.

- Instructed Help Desk on how to Baseline machines before being added to the NIPR Domain.
- Made changes to the ARP table to allow user s access to the internet.
- Blocked IP addresses from Cisco PIX Firewall.
- Maintained/Installed/Troubleshot Campus STAR Pargain devices.
- Managed servers using Terminal Services (RDP).

Advanced Technology Services 8/02-10/03 *LAN Administrator/Field Service Representative*

Supported the Dept of Energy at Savannah River Site. Duties on this task include:

- Create/Delete/Modify user accounts in both Win2000 Active Directory, and Exchange 2000.
- Administer File Server, and Quota accounts.
- Create Group Policy Objects.
- Administer Active Directory.
- Provide desk side computer hardware/software/networking and printer support for a site consisting of over 12,000 users.
- Install/configure/troubleshoot DOS, WINNT, Windows 95, Windows 98, Windows 2000, Lotus Notes, Microsoft Office 97, Microsoft Office XP.
- Cross-trained for the Dispatch/Logistic/Administrative Specialist position, becoming the primary back up.
- Utilized VMWare to test changes on private network.
- Provided numerous tech tips to the Help Desk that eliminated hundreds of escalations resulting in higher resolution rates for the agents.
- Assisted in the Windows NT, 95, and 98 migrations to Windows 2000.
- Provide support to on-site Help Desk Technicians.
- Perform Lead Technician responsibilities for desk side technicians.
- Supported the transition from Novell Netware 5 to an Active Directory environment.

McCall Thomas Computers 02/00-08/02 *Lead Configuration Technician*

- Developed and implemented more efficient procedures for the configuration, and installation departments.
- Trained all new and existing employees on new technologies, and newly developed procedures.
- Created and managed a department that saved the company tens of thousands of dollars.
- Configure IBM PCs and laptops, as well as Compaq RAID arrays, and servers according to customer specifications.
- Cross-trained for each position, becoming the primary back-up.
- Install Operating System and any applicable software.
- Troubleshoot/repair any and all PC hardware/software issues.
- Troubleshoot/resolve Novell Netware 5 issues.
- Assisted in the Windows NT, 95, and 98 migration to Windows 2000, both client and server side.
- Reduced the Configuration Department error counts to the lowest levels since the company's inception.

Bret Peresich, CISSP, OSCP, CISA, FQNV

Project Manager/Project Lead

SPECIALIZED QUALIFICATION:

Information Assurance specialist with more than 15 years of experience, including hands-on technical work and project management, as well as working directly with customers in a consulting capacity. Coordinated and directed teams involved in Security Test and Evaluation (ST&E) for System Security Authorization Agreement (SSAA) development, risk assessments, server and workstation migration for Navy and Marine Corps Intranet (NMCI), and server deployments, with an emphasis on learning solutions and end-user support. Excellent technical, communication, presentation, and customer service skills. Resourceful problem solver with proven ability to bring quick resolution to challenging situations. Management background includes leading teams, developing and managing budgets, devising timelines, monitoring project standards for all deliverables, creating strategies, overseeing the technical design and development of all learning solutions, new business development, documentation, development of training curriculum, conducting training, and maintaining quality assurance.

CERTIFICATIONS:

CISA: Certified Information Systems Auditor - ISACA
ISC2: Certified Information Systems Security Professional (CISSP)
OSCP: Offensive Security Certified Professional

HARDWARE: IBM and compatible DOS and UNIX Personal Computers (PCs), related interfaces, and peripherals.

SOFTWARE: Microsoft Office Suite: Excel, Word, Access, Outlook, Project, PowerPoint Publisher, and Visio. General Applications: Adobe Acrobat Professional, Camtasia Studio, Google Earth, SmartDraw 2007.

SERVER APPLICATIONS: Microsoft SQL Server 2000, 2005 and 2008.

NETWORKING: Cisco Routers and Switches, Cisco PIX, Symantec Firewall (firewall rulesets).

NETWORK/VULNERABILITY ANALYSIS TOOLS: Etherpeek, Ethereal (Wireshark), Nessus, Internet Security Scanner (ISS), eEye Digital Retina and REM, Rapid7 Metasploit and NexPose, McAfee Hercules, NMap, NetCat, Kismet Wireless Access Point Detection, Netstumbler, Flying Squirrel and MeerCAT.

PROGRAMMING LANGUAGES: Assembly, C/C++, Java, Visual Basic, Perl, HTML

SPECIFIC TASK EXPERIENCE:

Athena Consulting Group, North Charleston, SC 2006-Present *Program Manager / Project Lead*

Provide senior level advice and guidance on technical problems, solutions and challenges as they relate to the Navy Medicine Information Assurance environment. Conduct risk assessments and deliver findings and reports to senior level management. Prepare and submit whitepapers, position papers and briefs explaining technical issues to senior leadership.

- Project Lead for the Navy Medicine Enterprise Information Assurance Controls Verification and Validation (CV&V) Team
- Developed the CV&V Team Standard Operating Procedures
- Conducted Site and Program of Record (POR) Systems Security Test and Evaluation (ST&E) for Certification and Accreditation (C&A)
- Conducted Independent Verification and Validation (IV&V) assessments for sites and POR systems as part of the DIACAP Approval To Operate (ATO) life cycle
- Developed custom vulnerability reporting tools for CV&V
- Project Lead for the Secure Compliance Tool Suite Deployment Team
- Technical Lead for SPAWAR Charleston NMCI Migration Team
- Developed the Navy Medicine Concept of Operations (CONOPS) and Standard Operating Procedures (SOP) for SCCVI-SCRI implementation
- Developed the cost estimate to deploy the Secure Compliance Tools Suite throughout Navy Medicine sites
- Developed the Secure Configuration Compliance Validation Initiative-Secure Configuration Remediation Initiative (SCCVI-SCRI) deployment strategy for Navy Medicine

Vulnerability/Penetration Testing

Conducted vulnerability scanning utilizing NMAP, BeyondTrust Retina Network Vulnerability Scanner, and Nessus as well as Penetration Testing with Rapid7 Metasploit.

- Performed vulnerability scanning and penetration testing for A/P Recovery, Inc. Provided detailed Assessment Report detailing penetration attempts and successful exploits as well as recommendations to remediate known vulnerabilities.
- Performed vulnerability and penetration testing for West Virginia Public Employees Insurance Agency (PEIA) and Children's Health Insurance Program (CHIP)
- Performed wireless scanning and WiFi penetration testing of WV-PEIA wireless network. Successfully cracked their WPA2 WiFi password.

RL Phillips 2002-2006 *Information Assurance Specialist*

- Conducted Security Test and Evaluation (ST&E) of Navy Medical Information Management Center systems for DITSCAP Accreditation
- Conducted Preliminary Vulnerability Test and Assessment of Navy Medical Information

- Management Center (NMIMC) Network Operating Center using Retina Network Security Scanner and DISA Gold Disk
- Provided Out-Brief and PowerPoint Presentations to NMIMC Upper Management.
- Developed detailed vulnerability analysis report and mitigation plan for NMIMC site personnel
- Analyzed various firewall rulesets for UTNProtect Policy compliance
- Analyzed router configuration files for current NCDOC Blocked IP List compliance and implementation of NSA Security Guidelines and Industry Best Practices for router security
- Scanned various servers and workstations for vulnerabilities and IAVM compliance
- Analyzed Securify SecurVantage reports for network behaviors and compared traffic against known server lists to identify unknown servers and unexpected network traffic

SPAWAR Systems Center Charleston, North Charleston, SC 2000-2002 *Network Technician DT-0856-2*

- Chaired the Security Working Groups for NMCI Legacy Application migration efforts
- Developed processes and procedures for Legacy Applications Quarantine Reduction Team
- Developed processes and procedures for Information Management Team
- Technical Lead for Legacy Applications Quarantine Reduction
- Conducted Legacy Systems Security Improvement Pilot at NAVAIR Orlando
- Installed Securify SecurVantage for network traffic monitoring and analysis
- Conducted training for Quick Look Assessment Teams covering Nessus Vulnerability Scanner, Kismet Wireless Access Point Detection Software, Securify SecurVantage, WildPackets EtherPeek, and analyzing firewall rulesets and router configurations
- Quick Look Assessment Lead Technical Advisor
- Developed processes and procedures for the Information Assurance Tiger Team (IATT) Quick Look Assessment Teams
- Conducted port and protocol analysis of network communication of legacy applications within the Department of the Navy
- Worked with sites to develop accurate server lists based on network mapping
- Developed network topology diagrams for various Navy sites after mapping the network using scanning tools
- Advised the Legacy Application Information Assurance group for Navy Marine Corps Intranet (NMCI) in best strategies for mitigating known and possible risks for the migration of Department of the Navy legacy applications into NMCI
- Advised in writing the draft version of the Legacy Systems Transition Guide and the System Transition Engineering Review Questionnaire for the NMCI Legacy Systems Security Improvement pilot

Best Buy 1998 to 2000 *Services Supervisor*

Program/Project Management

- Attention to detail
- Work well independently and on a team
- Excellent customer service skills
- Excellent oral and writing skills

- Excellent at problem solving and decision making
- Possess and display excellent technical competence
- Work well under stress
- Able to meet deadlines
- Flexible to changes in tasking
- Able to adapt quickly

US Navy (Veteran) 1988 to 1998 *Fire Controlman – Petty Officer First Class*

- Great Lakes Naval Training Center – FC 'A' School 1988-1989
- DamNeck, VA – Mk92 Mod2 Fire Control System 'C' School 1989-1990
- DamNeck, VA – Harpoon Weapon System AN/SWG-PA Maintenance (Surface Application 1994
- USS Nicholas (FFG-47) 1990-1995
- Maintained and troubleshot MK92 Mod 2 Fire Control Weapons System
- Maintained and troubleshot AN/SWG Harpoon Weapon System Console
- Watchstander on MK92 FCS and Harpoon Console in Combat Information Center (CIC)
- Member of the Damage Control Training Team
- Member of the Combat Systems Training Team
- Bureau of Naval Personnel (BUPERS) 1995-1998
- FC Schools Detailer: Responsible for quota control of 35 NEC producing schools. Collateral duties included LAN administrator for Pers 406 and 402; Branch MWR and Government Savings Bond representative. Developed Branch checkbook application to automate personnel and budget accounting for $25M+ budget.

EDUCATION: Bachelor of Science, Computer Information Systems

Strayer University, Charleston, SC GPA: 4.0 Emphasis on Computer Security.

ADDITIONAL TRAINING:

Certified Information Systems Auditor (CISA), ISACA, 2010

Offensive Security Certified Professional (OSCP), Offensive-Security, 2007

Certified Information Systems Security Professional (CISSP), ISC(2), 2005

Security SecurVantage Certification, Security, 2003

CompTIA A+ Certification, CompTIA, 2000
Offensive Security 101, Offensive-Security, Online, 2007
Retina Security Scanner/REM Training, DISA, Online, 2005
Hercules SCRI Training, Citadel, 2005
SANS Track 2 - Firewalls, VPNs, and Perimeter Security, SANS, 2003

Ms. Trish Austin, MBA, PMP
Comptroller, Security Risk Solutions, Inc.

Education

INSTITUTION AND LOCATION	DEGREE	YEARS	FIELD OF STUDY
State University of New York at Geneseo	BS (Bachelor of Science)	1993	Accounting
Oklahoma City University	MBA (Master of Business Administration)	2000	Business Administration with a Concentration in Finance

Qualifications Summary

Ms. Austin has proven experience in financial management, budgeting, and forecasting revenue and expenses for large government programs. She has demonstrated highly effective analytical and planning skills and project management abilities in a fast-paced team oriented environment. She is customer service-oriented with excellent communication skills. In addition to her MBA, Ms. Austin holds a Project Management Professional (PMP) certification.

Experience Summary

Security Risk Solutions, Inc.
Comptroller *(Feb 2012 – present)*
Ms. Austin currently serves as the Comptroller at SRS. Ms. Austin's responsibilities include development and implementation of all aspects of financial management at SRS, as well as providing various support activity to the Leadership team. Her activities include, but are not limited to, payroll, budgeting and forecasting, internal financial audit functions, employee expense report review and approval, invoice preparation, cost proposal research and compilation, contracts administration, and financial policy and procedure development. Additionally, she gives recommendations on selections of accounting and timekeeping systems to ensure compliance with Defense Contract Audit Agency (DCAA) rules and regulations.

South Carolina Research Authority (SCRA)
Project Manager and Financial Analyst *(2001-2012)*
Ms. Austin was a Project Manager and Financial Analyst, working on several different programs during her tenure at SCRA and its affiliate, Advanced Technology Institute (ATI). Her responsibilities included managing, forecasting, and analyzing revenue and expense budgets for the 22 million dollar Healthcare Information Technology Standards Panel (HITSP) program and the 18 million dollar Vanadium Safety Readiness (VSR) and Vanadium Technology Partnership (VTP) programs. She worked closely with program managers to provide timely analysis, Earned Value Management (EVM) reports, as well as monthly and quarterly reports as stipulated in program contracts, while assisting multiple subcontractors with managing their internal finances to streamline their own practices. She contributed input to the development of annual corporate labor and subcontracted budgets for various divisions within SCRA/ATI, generated reports for senior management, and proactively sought out various process improvement methods, thereby providing for more efficient processes within the company.

Logix Communications
Business Analysis Manager and Financial Analyst *(1998 – 2001)*
Ms. Austin was a Business Analysis Manager and Financial Analyst while working at Logix Communications, a privately-owned telecommunications company based in Oklahoma City. Her responsibilities included development and maintenance of business models to provide revenue and cost analysis for new and existing telecommunications products. She developed Access databases and managed a collection of metrics data to fulfill internal reporting requirements and presented findings to senior management. She also worked on a team assembled to determine the cost/profitability of new products and made decisions regarding whether to market certain products to customers. She provided monthly actual versus budget analysis, break-even analysis and financial analysis, as well as ad hoc reporting.

MCI-Worldcom Telecommunications

Ms. Trish Austin, MBA, PMP
Comptroller, Security Risk Solutions, Inc.

Revenue Reporting Analyst *(1995 – 1998)*

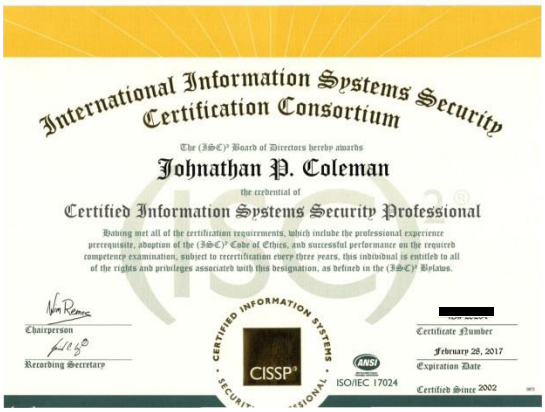
During this period, Ms. Austin worked for MCI WorldCom Telecommunications as a Revenue Reporting Analyst. In this role, Ms. Austin provided financial reporting and cost/budget analysis to senior management in a variety of internal departments. She developed a PowerPoint training manual for MCI's performance and revenue tracking systems and trained new users. She acted as the primary point of contact to MCI's large account sales teams regarding all revenue tracking issues and provided support for the company's commissions and revenue analysis systems.

Certifications and Affiliations

- Certified Project Management Professional (PMP)
- Current member of the Project Management Institute, Charleston SC Chapter

Appendix B: Copies of Staff Certifications and Degrees

NOTE: Due to the extensive number of certifications and degrees held by our team, only a sample have been included here. A fully comprehensive set of valid certificates for each team member will be provided upon request.


International Information Systems Security Certification Consortium

The (ISC)² Board of Directors hereby awards

Johnathan P. Coleman

the credential of

Certified Information Systems Security Professional

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

Chairperson

Recording Secretary

Certificate Number

February 28, 2017
Expiration Date

Certified Since 2002

CISSP

ISO/IEC 17024


CISM Certified Information Security Manager

ISACA

CERTIFIED INFORMATION SECURITY MANAGER

ISACA hereby certifies that

Johnathan Peter Coleman

has successfully met all requirements and is qualified as a Certified Information Security Manager.
In witness whereof, we have subscribed our signatures to this certificate.

Requirements include prerequisite professional experience; adherence to the ISACA Code of Professional Ethics and the CISM continuing professional education policy; and passage of the CISM exam.

19 February 2003
Date of Certification

31 January 2016
Expiration Date

Certificate Number

ANSI

ISACA


Cranfield

Cranfield Institute of Technology

JOHNATHAN PETER COLEMAN

Has this day been admitted to the Degree of **Bachelor of Engineering** having studied in the Faculty of Military Science, Technology and Management.

DEGREE

IN

AEROMECHANICAL SYSTEMS ENGINEERING

Professor

Registrar

17 July 1992


CNSS

SENTEK GLOBAL

Certificate of Completion

Awarded to

Johnathan Coleman

For the successful completion of

DIACAP Advanced Validator Course

Cert No.

02 March 2012
Date of Completion

Instructor Signature


Project Management Institute

THIS IS TO CERTIFY THAT

Trish Austin

HAS BEEN FORMALLY EVALUATED FOR DEMONSTRATED EXPERIENCE, KNOWLEDGE AND PERFORMANCE IN ACHIEVING AN ORGANIZATIONAL OBJECTIVE THROUGH DEFINING AND OVERSEEING PROJECTS AND RESOURCES AND IS HEREBY BESTOWED THE GLOBAL CREDENTIAL

Project Management Professional

IN TESTIMONY WHEREOF, WE HAVE SUBSCRIBED OUR SIGNATURES UNDER THE SEAL OF THE INSTITUTE

Peter Monkhouse - Chair, Board of Directors

Mark A. Langley - President and Chief Executive Officer

PROJECT MANAGEMENT INSTITUTE CORPORATE SEAL 1969

PMP® Number 1560739

PMP® Original Grant Date 13 December 2012

PMP® Expiration Date 13 December 2015

PMI Project Management Institute

Cisco Career Certifications

Brian M Freedman

Has successfully completed the Cisco Career Certifications test requirements and is recognized as a

Cisco Certified Network Associate — CCNA

Valid Through: October 22, 2004

Cisco ID# [redacted]

John Chambers
President and CEO
Cisco Systems, Inc.

Cisco Systems

Microsoft Certified Systems Engineer

BRIAN M FREEDMAN

Has successfully completed the requirements to be recognized as a Microsoft Certified Systems Engineer: Windows Server 2003.

Date of achievement: [redacted]/2008

Certification number: [redacted]

Satya Nadella
Chief Executive Officer

Microsoft CERTIFIED Systems Engineer

Microsoft Certified Systems Administrator

BRIAN M FREEDMAN

Has successfully completed the requirements to be recognized as a Microsoft Certified Systems Administrator: Windows Server 2003.

Date of achievement: 11/19/2007

Certification number: [redacted]

Satya Nadella
Chief Executive Officer

Microsoft CERTIFIED Systems Administrator

Microsoft Certified Systems Engineer

BRIAN M FREEDMAN

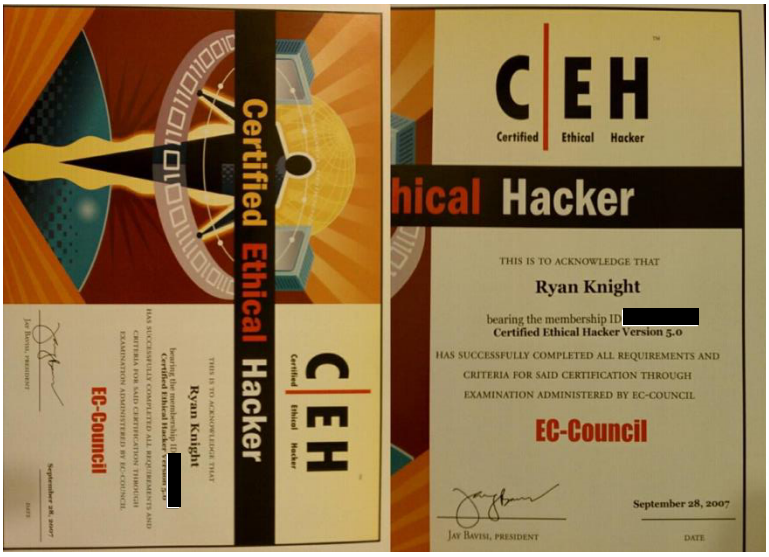
Has successfully completed the requirements to be recognized as a Microsoft Certified Systems Engineer: Windows NT 4.0.

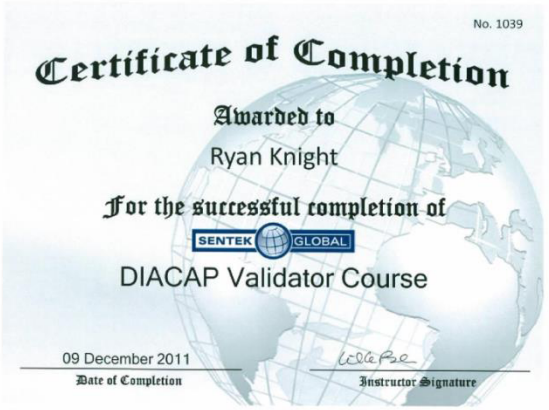
Date of achievement: 02/02/1998

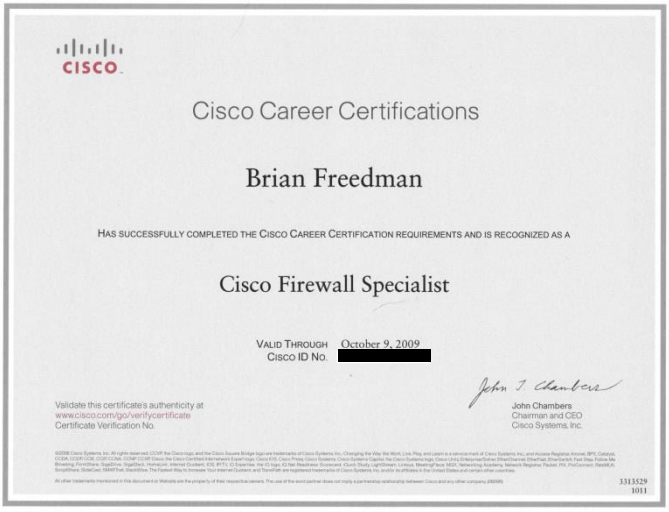
Certification number: [redacted]

Satya Nadella
Chief Executive Officer

Microsoft CERTIFIED Systems Engineer


Certified Ethical Hacker
C|EH
Certified Ethical Hacker
EC-Council
C|EH
Certified Ethical Hacker
hical Hacker
THIS IS TO ACKNOWLEDGE THAT
Ryan Knight
bearing the membership ID [redacted]
Certified Ethical Hacker Version 5.0
HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND
CRITERIA FOR SAID CERTIFICATION THROUGH
EXAMINATION ADMINISTERED BY EC-COUNCIL
EC-Council
September 28, 2007
Jay Bavisi, President
DATE

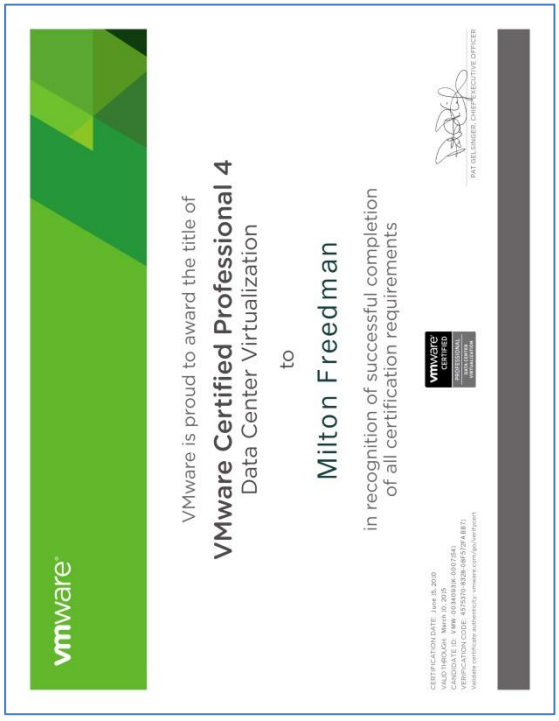

No. 1039
Certificate of Completion
Awarded to
Ryan Knight
For the successful completion of
SENTEK GLOBAL
DIACAP Validator Course
09 December 2011
Date of Completion
Instructor Signature


CISCO
Cisco Career Certifications
Brian Freedman
HAS SUCCESSFULLY COMPLETED THE CISCO CAREER CERTIFICATION REQUIREMENTS AND IS RECOGNIZED AS A
Cisco Firewall Specialist
VALID THROUGH October 9, 2009
CISCO ID No. [redacted]
John Chambers
Chairman and CEO
Cisco Systems, Inc.
Validate this certificate's authenticity at
www.cisco.com/go/verifycertificate
Certificate Verification No.
3313529
1011

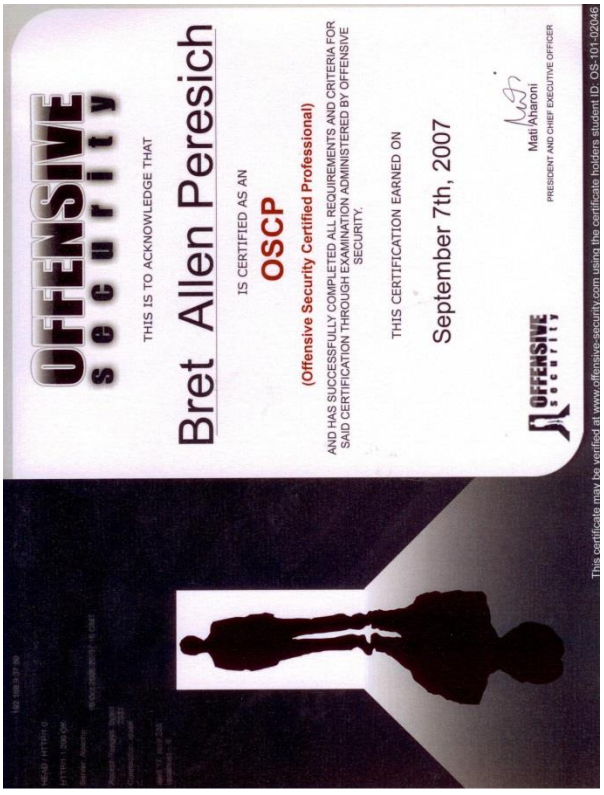

C|NDA
Certified Network Defense Architect
Certified Network Defense Architect
THIS IS TO ACKNOWLEDGE THAT
Ryan Knight
bearing the membership ID [redacted]
CNDA Version 3
HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND
CRITERIA FOR SAID CERTIFICATION THROUGH
EXAMINATION ADMINISTERED BY EC-COUNCIL
EC-Council
September 28, 2007
Jay Bavisi, President
DATE


OFFICIAL SEAL OF MICROSOFT CERTIFICATION
Microsoft Certified
Professional


BRIAN M FREEDMAN
Has successfully completed the requirements to be recognized as a Microsoft Certified Professional.
Date of achievement: 07/14/1997
Certification number: [redacted]
Satya Nadella
Chief Executive Officer
Microsoft
CERTIFIED
Professional


vmware
VMware is proud to award the title of
VMware Certified Professional 4
Data Center Virtualization
to
Milton Freedman
in recognition of successful completion
of all certification requirements


International Information Systems Security
Certification Consortium
Certified Information Systems Security Professional
CISSP
CERTIFIED · INFORMATION SYSTEMS · SECURITY PROFESSIONAL
ISO/IEC 17024
(ISC)


OFFENSIVE security
THIS IS TO ACKNOWLEDGE THAT
Bret Allen Peresich
IS CERTIFIED AS AN
OSCP
(Offensive Security Certified Professional)
AND HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND CRITERIA FOR SAID CERTIFICATION THROUGH EXAMINATION ADMINISTERED BY OFFENSIVE SECURITY.
THIS CERTIFICATION EARNED ON
September 7th, 2007
Mati Aharoni
PRESIDENT AND CHIEF EXECUTIVE OFFICER
This certificate may be verified at www.offensive-security.com using the certificate holders student ID: OS-101-02046

OFFENSIVE security
THIS IS TO ACKNOWLEDGE THAT
Ryan Knight
IS CERTIFIED AS AN
OSCP
(Offensive Security Certified Professional)
AND HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND CRITERIA FOR SAID CERTIFICATION THROUGH EXAMINATION ADMINISTERED BY OFFENSIVE SECURITY.
THIS CERTIFICATION EARNED ON
July 26, 2007
Mati Aharoni
PRESIDENT AND CHIEF EXECUTIVE OFFICER
This certificate may be verified at www.offensive-security.com using the certificate holder's student ID: OS-101-02035

REQUEST FOR QUOTATION

Information Security and Network Vulnerability Assessment

Attachment 1 - Vendor References

Reference No. 1	
Name:	Thomas D. Miller, MA, LPC, ALPS, ADC
Position:	Privacy Officer, West Virginia Department of Administration, Public Employees Insurance Agency/WV CHIP
Address:	601 57th Street, SE, Suite 2, Room 1008 Charleston, West Virginia 25304-2345
Telephone Number:	304-558-7850, Extension 52663 email to: thomas.d.miller@wv.gov
Project Name:	Security Risk and Vulnerability Assessment
Project Description:	Security Risk Assessment services will include all aspects of information security including, but not necessarily limited to: physical security, IT related systems, policies and procedures, staff training, and third party interaction(s).

Reference No. 2	
Name:	Chris Cotton
Position:	Navy Bureau of Medicine, Cyber Security Inspection (CSI) Program Lead (CTR)
Address:	5113 Leesburg Pike Falls Church, VA 22041
Telephone Number:	(804) 417-7699 Email to: Chris.cotton.ctr@med.navy.mil
Project Name:	Cyber Security Inspections (CSI) Stage II support
Project Description:	Provide support to the US Cyber Command (USCYBERCOM) Command Cyber Security Inspections (CSI) Stage II readiness team. Travel to sites selected for inspection by the FLTCYBERCOM (C10F) Office of Compliance and Assessment (OCA) to assess the security of Navy networks through a comprehensive, graded inspection involving all Cyber Security areas, specifically: Leadership Management, Physical Security, Administration, Training, Network Configuration, Network Operations, and Human Factors and Command Operational Behavior.

Reference No. 3	
Name:	Mr. T. Vincent Patenaude
Position:	CODE 56110
Address:	Space and Naval Warfare Systems Center, Atlantic 1 Innovation Drive, North Charleston, SC 29407
Telephone Number:	Commercial: 843-218-4197 Email to: tyrone.patenaude@navy.mil
Project Name:	Security Vulnerability Testing: Army National Guard Electronic Security Systems
Project Description:	Provide support to the Space and Naval Warfare Systems Center, Atlantic and the Army National Guard Bureau by conducting security reviews, vulnerability testing, and supporting documentation for the ARNG ESS System DIACAP Accreditation.

REQUEST FOR QUOTATION

Information Security and Network Vulnerability Assessment

Attachment 2 – Vendor Primary Staff References

Reference No. 1	
Name:	Brian Freedman, MS, CISSP, PMP
Position:	Deputy Program Manager / Sr. Technical Lead
Address:	698 Fishermans Bend Mt. Pleasant, SC 29464
Telephone Number:	843-697-2944 Email to: mbf@securityrs.com
Project Name:	WV PEIA/CHIP Security Risk and Vulnerability Assessment
Project Description:	Security Risk Assessment services included all aspects of information security including, but not necessarily limited to: physical security, IT related systems, policies and procedures, staff training, and third party interaction(s).
Duties Performed:	Lead the team through detailed technical and non-technical vulnerability assessment, including assessment of WV PEIA and WV CHIP infrastructure and associated services provided by WVOT. Assessment includes detailed network discovery, analysis, development of documentation, identification of vulnerabilities, prioritized risk rankings, and mitigation strategies.

Reference No. 2	
Name:	Johnathan Coleman, CISSP, CISM, CBRM, CRISC
Position:	Principal
Address:	698 Fishermans Bend Mt. Pleasant, SC 29464
Telephone Number:	843-442-9104 Email to: jc@securityrs.com
Project Name:	US Cyber Command (USCYBERCOM) Cyber Security Inspections (CSI) Stage II support
Project Description:	Provide support to the US Cyber Command (USCYBERCOM) Command Cyber Security Inspections (CSI) Stage II readiness team. Travel to sites selected for inspection by the FLTCYBERCOM (C10F) Office of Compliance and Assessment (OCA) to assess the security of Navy networks through a comprehensive, graded inspection involving all Cyber Security areas, specifically: Leadership Management, Physical Security, Administration, Training, Network Configuration, Network Operations, and Human Factors and Command Operational Behavior.
Duties Performed:	Supported Navy Medicine (NAVMED) Echelon II, Bureau of Medicine and Surgery (BUMED) M62, in conducting unit-level training and assessment at each of the NAVMED Medical Treatment Facilities (MTFs) as part of Stage II of the CSI and in preparation for the CSI Stage III inspection conducted by United States Cyber Command (USCYBERCOM). CSI Stage II focused on the evaluation of the MTFs emphasis on compliance of the Information Assurance (IA) Controls that are in place in the each of the following areas: Contributing Factors (Leadership Culture, Capability and Conduct), Directives and Policy, Network Infrastructure, System Configuration, IA Vulnerability Management (IAVM), Traditional (Physical) Security, and Workforce Security Awareness and Training.

Reference No. 3	
Name:	Brandon Friesner, MS, CISSP
Position:	Senior Information Assurance Professional
Address:	698 Fishermans Bend Mt. Pleasant, SC 29464
Telephone Number:	843-810-4540 Email to: blf@securityrs.com
Project Name:	Security Vulnerability Testing: Army National Guard (ARNG) Electronic Security Systems (ESS)
Project Description:	Provide support to the Space and Naval Warfare Systems Center, Atlantic and the Army National Guard Bureau by conducting security reviews, vulnerability testing, and supporting documentation for the ARNG ESS System DIACAP Accreditation.
Duties Performed:	Applied unique expertise in ESS Security, risk assessments, NIST Special Publications (including 800-53 and 800-37) to manage risks associated with the Security Certification and Accreditation (C&A) Process. Tested, verified and documented mitigation approaches and technical remediation activities associated with each finding, producing a test report and Plan of Actions and Milestones (POA&M) update on each component. Prepared and delivered an update to the ESS approved hardware/software baseline by facilitating and attending Designated Approval Authority (DAA) meetings and Configuration Control Board (CCB) meetings as the Information Systems Security Officer (ISSO). Developed and delivered an updated systems architecture description document, security configuration guide, CISCO ASA5505 Firewall configurations, and other technical documentation as needed. Provided security expertise in evaluating the integration of Intrusion Detection Systems (IDS) sensors and Environmental Sensors into the ESS architecture. Provide advice and recommendations, as needed, on ESS applicability and implementation at ARNG armories and/or vaults.

Attachment 3 – Attestation and Confirmations

REQUEST FOR QUOTATION

Information Security and Network Vulnerability Assessment

Attachment 3 – Attestation and Confirmations

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

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

REQUEST FOR QUOTATION

Information Security and Network Vulnerability Assessment

Attachment 3 – Attestation and Confirmations

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

Company:	Security Risk Solutions, Inc.
Printed Name:	Johnathan Coleman
Signature:	Johnathan Coleman
Title:	Principal
Date:	18th January, 2015

Attachment 4 – Confidentiality Agreement

Attachment 4

Consolidated Public Retirement Board
Confidentiality and Non-disclosure Statement

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

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

"I, JOHNATHAN COLEMAN the (title) PRINCIPAL of

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

Print Name: JOHNATHAN COLEMAN

Company: SECURITY RISK SOLUTIONS, INC.

Signature: Johnathan Coleman Date: 01/18/2015

Revised 7/05/07 Vendors

Attachment 5 – Vendor Preference Certificate

Rev. 04/14

State of West Virginia

VENDOR PREFERENCE CERTIFICATE

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

1. **Application is made for 2.5% vendor preference for the reason checked:**
____ Bidder is an individual resident vendor and has resided continuously in West Virginia for four (4) years immediately preceding the date of this certification; **or,**
____ Bidder is a partnership, association or corporation resident vendor and has maintained its headquarters or principal place of business continuously in West Virginia for four (4) years immediately preceding the date of this certification; or 80% of the ownership interest of Bidder is held by another individual, partnership, association or corporation resident vendor who has maintained its headquarters or principal place of business continuously in West Virginia for four (4) years immediately preceding the date of this certification; **or,**
____ Bidder is a nonresident vendor which has an affiliate or subsidiary which employs a minimum of one hundred state residents and which has maintained its headquarters or principal place of business within West Virginia continuously for the four (4) years immediately preceding the date of this certification; **or,**

2. **Application is made for 2.5% vendor preference for the reason checked:**
____ Bidder is a resident vendor who certifies that, during the life of the contract, on average at least 75% of the employees working on the project being bid are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or,**

3. **Application is made for 2.5% vendor preference for the reason checked:**
____ Bidder is a nonresident vendor employing a minimum of one hundred state residents or is a nonresident vendor with an affiliate or subsidiary which maintains its headquarters or principal place of business within West Virginia employing a minimum of one hundred state residents who certifies that, during the life of the contract, on average at least 75% of the employees or Bidder's affiliate's or subsidiary's employees are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or,**

4. **Application is made for 5% vendor preference for the reason checked:**
____ Bidder meets either the requirement of both subdivisions (1) and (2) or subdivision (1) and (3) as stated above; **or,**

5. **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**
____ Bidder is an individual resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard and has resided in West Virginia continuously for the four years immediately preceding the date on which the bid is submitted; **or,**

6. **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**
____ Bidder is a resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard, if, for purposes of producing or distributing the commodities or completing the project which is the subject of the vendor's bid and continuously over the entire term of the project, on average at least seventy-five percent of the vendor's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years.

7. **Application is made for preference as a non-resident small, women- and minority-owned business, in accordance with *West Virginia Code* §5A-3-59 and *West Virginia Code of State Rules.***
✔ Bidder has been or expects to be approved prior to contract award by the Purchasing Division as a certified small, women- and minority-owned business.

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

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

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

Bidder: SECURITY RISK SOLUTIONS, INC. **Signed:** Johnathan Coleman

Date: 1/18/2015 **Title:** PRINCIPAL

Attachment 6 – Purchasing Affidavit

RFQ No. CRFQ 0203 CPR1500000001

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

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

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

DEFINITIONS:

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

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

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

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

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: SECURITY RISK SOLUTIONS, INC.

Authorized Signature: [signature] Date: 1/19/2015

State of South Carolina

County of Charleston, to-wit:

Taken, subscribed, and sworn to before me this 19 day of January, 2015.

My Commission expires May 5, 2024.

AFFIX SEAL HERE

NOTARY PUBLIC [signature]

Purchasing Affidavit (Revised 07/01/2012)

Attachment 7 - Certification and Signature Page

CERTIFICATIONAND SIGNATURE PAGE

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

SECURITY RISK SOLUTIONS, INC.

(Company)

Johnathan Coleman JOHNATHAN COLEMAN, PRINCIPAL

(Authorized Signature) (Representative Name, Title)

PHONE: 843 442 9104 FAX NO: N/A DATE: 01/18/2015

(Phone Number) (Fax Number) (Date)

Revised 08/08/2014

Attachment 8 - Addendum Acknowledgement Form

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CPR1500000001

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

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

Addendum Numbers Received:
(Check the box next to each addendum received)

[X]	Addendum No. 1	[ ]	Addendum No. 6
[X]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	Addendum No. 10

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

SECURITY RISK SOLUTIONS, INC.
Company

Johnathan Coleman
Authorized Signature

1/18/2015
Date

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

Revised 08/08/2014

Exhibit A

Pricing Page

Information Security and Network Vulnerability Assessment service for CPRB

Security Risk Solutions, Inc.			Unit of	Unit	Quantity	Extended
Item	**Item Description**	**Description**	**Measure**	**Cost**	**Needed**	**Cost**
1	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 1	per Complete Assesment	$ 63,254.52	1	$ 63,254.52
2	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 2	per Complete Assesment	$ 56,929.07	1	$ 56,929.07
3	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 3	per Complete Assesment	$ 56,929.07	1	$ 56,929.07
4	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 4	per Complete Assesment	$ 56,929.07	1	$ 56,929.07
5	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 5	per Complete Assesment	$ 63,254.52	1	$ 63,254.52
					TOTAL of Assessments	$ 297,296.24

Assessment Cost are <u>firm fixed</u> for each complete Assessments

*** Contrat Award will be for Total of Assessments ***