State of West Virginia

Public Employees Insurance Agency

HIPAA/HITECH Security Risk Assessment

Technical Proposal: Response to Solicitation #: PEI 013002

Submitted by

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

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

KRM ASSOCIATES INC

ACG
Athena Consulting Group

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

SEALED BID ENCLOSED

RFQ Number:	PEI 013002
Buyer:	WV PEIA
Bid Opening Date:	07/11/2013
Bid Opening Time:	1:30pm EST

BID TYPE: [X] Technical

[ ] Cost

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

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

23rd July, 2013

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

Attn: Ms. Krista S. Ferrell, Buyer Supervisor

Proposal for State of West Virginia Public Employees Insurance Agency, HIPAA/HITECH Security Risk Assessment Solicitation #: PEI 013002

Dear Ms. Ferrell,

Security Risk Solutions, Inc. is pleased to acknowledge addendum 2 with respect to solicitation PEI 013002. Our previous proposal, dated 8th July 2013 remains in full effect and is not changed by the solicitation amendment. For reference, that proposal was delivered on July 10th with FedEx tracking number 796176839862. 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 9th 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 printing/shipping our proposal, Addendum No.2 to the RFP has been issued. If, during the time period between shipping and the bid open date/time an addendum is issued, SRS may submit a superseded proposal.
2. Our first proposal, dated June 24th, 2013, may be disregarded. It was superseded by our proposal dated July 8th 2013, delivered via FedEx (tracking number 796176839862) which was shipped prior to the issuance of Addendum #2 but remains valid.
3. Upon award, Security Risk Solutions, Inc is both willing and able to perform the terms indicated in our proposal.
4. We hereby confirm acceptance of all Terms and Conditions as described, incorporated or referenced in the RFQ.
5. We are submitting a Fixed Price proposal.
6. Our proposal will remain in full force and effect for 180 days from the new 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.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: PEI013002

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

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

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

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

Authorized Signature

07/23/2013
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012

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

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

8th July, 2013

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

Attn: Ms. Krista S. Ferrell, Buyer Supervisor

Proposal for State of West Virginia Public Employees Insurance Agency, HIPAA/HITECH Security Risk Assessment Solicitation #: PEI 013002

Dear Ms. Ferrell,

Security Risk Solutions, Inc. is pleased to submit this proposal for solicitation PEI 013002. 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 9th 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 printing/shipping our proposal, Addendum No.1 to the RFP has been issued. If, during the time period between shipping and the bid open date/time an addendum is issued, SRS may submit a superseded proposal.
2. This proposal supersedes our original proposal, dated June 24th, 2013, which may be disregarded.
3. Upon award, Security Risk Solutions, Inc is both willing and able to perform the terms indicated in our proposal.
4. We hereby confirm acceptance of all Terms and Conditions as described, incorporated or referenced in the RFQ.
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.

State of West Virginia

Public Employees Insurance Agency

HIPAA/HITECH Security Risk Assessment

Technical Proposal: Response to Solicitation #: PEI 013002

Submitted by

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

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

KRM ASSOCIATES INC

ACG
Athena Consulting Group

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

VENDOR
SIGNATURE:________________ DATE: 8th July, 2013

Table of Contents

Attachment A: Vendor Response Sheet

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.

Vendor Identification and Qualifications

Table 1: Vendor Identification

	PRIME CONTRACTOR	SUBCONTRACTOR	SUBCONTRACTOR
Organization:	Security Risk Solutions, Inc. (SRS)	Athena Consulting Group, LLC (ACG)	KRM Associates, Inc. (KRM)
Economic Status/ Preferences	• SBA Small Business. • Woman Owned Small Business (WOSB) • WV Preference as an out-of-state WOSB applied for.	• Small Business	• ***WV Certified SBA Small Business.*** • Woman Owned 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	Chris Cotton, CISSP, PMP COO, Athena Consulting Group 4995 LacCross Road, Suite 1250 North Charleston, SC 29406 Tel: (804) 417 7699 chris.cotton@ athenaconsultinggroup.com	Keith McCall KRM Associates, Inc. PO Box 3362, Shepherdstown, WV 25443 Tel: (304) 876-6600 keith.mccall@krminc.com
Website	www.securityrisksolutions.com	www.athenaconsultinggroup.com	www.krminc.com
Incorporation:	S-Corporation (South Carolina)	Limited Liability Corporation (SC)	Sub S Corporation (WV)
Date Founded:	31 December, 2004	24 December, 2004	March 3, 1991
D-U-N-S No:	192835390	171419257	805548757
TIN:	20-8133845	25-1915472	55-0704373

1. Please provide the full legal name of the vendor (person(s), entity, and/or company) that is submitting a bid on this project:
Security Risk Solutions, Inc.

2. Please provide the primary address, telephone number, fax number, and primary contact's e-mail address for the vendor (person(s), entity, and/or company) that is submitting a bid on this project:
Johnathan Coleman, CISSP, CISM
Principal, Security Risk Solutions
698 Fishermans Bend, Mt. Pleasant, SC 29464, USA
Cell:(843) 442-9104
Fax: (843) 416-4881 (call ahead to 843-442-9104 requested)
Email: jc@securityrs.com

3. If the vendor (person(s), entity, and/or company) that is submitting a bid on this project has a website, please provide the URL:

www.securityrisksolutions.com

4. Vendor should provide a brief description of its company and its products and services.

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 Healthcare Information Security Risk Management Services, with a particular expertise with HIPAA/HITECH 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 two experienced and qualified subcontractors: KRM Associates, Inc. (KRM) and Athena Consulting Group LLC (ACG). SRS has been working with KRM and 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 Healthcare IT security and legal compliance with HIPAA/HITECH regulations. KRM Inc., a WV based business, will provide a local presence to the PEIA and other departments in the State of West Virginia. KRM has a long and impressive history of working with state agency departments in WV, and has first-hand experience with many of the leaders and project managers we will support under this program. Their knowledge of the WV PEIA Offices/systems, WV CHIP Offices/systems, 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. The staff at ACG will be supporting the technical execution phase of the project. Their deep experience in penetration testing and technical vulnerability experience complements the SRS capabilities in that area, while providing additional depth for analysis and mitigation planning for identified vulnerabilities.

Team Highlights

- **Highly qualified team of Security Professionals with deep legal and practical understanding of HIPAA/HITECH**
- **Renowned and credentialed subject matter experts in Health IT, Security, Privacy, and Risk Assessment**
- **Staff committed to this effort available from day one and ready to excel**
- **Team includes local staff experienced with WV State Agencies requiring no learning curve to adjust to organizational culture**

KRM Associates, Inc., is a WV certified small, independent woman-owned company that provides information technology and security services and consulting. KRM assists clients in the application of Information Technology (IT) technologies and capabilities through strategic management, technology assessment, and project management, specializing in Healthcare Information Technology (HIT), security and assessments, help-desk environments, risk analysis, technical system design and development, certification and accreditation support, and pilot project and technology development.

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 are industry experts with the ability to combine elegant and innovative technical solutions with best industry and business practices.

5. Vendor should confirm its ability to provide the specific products and services that it is including in their response.

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.

6. Additional Vendor Qualifications and Experience: Vendors should provide information regarding their firm such as, date founded, staff qualifications and experience in completing similar projects; copies of any business or staff certifications or degrees applicable to this project; a proposed staffing plan; descriptions of past projects completed entailing the location of the project, project manager name and contact information, type of project, and what the project goals and objectives were and how they were met.

Date Founded:

As shown in Table 1: Vendor Identification, SRS and ACG were founded in December 2004 and are in their ninth year of business. KRM was founded in March 1991, and is now in its 23rd year of business.

Staff Qualifications and Experience:

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 J.D., and/or internationally recognized security certifications backed with many years of credible and relevant experience. Professional certifications currently held by employees include CISSP, ISSEP, CISM, ITIL, CBCP, CBRM, Security+, CRISC, and PMP. Copies of any staff certifications and degrees applicable to this project are attached at Appendix G, 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 healthcare IT security and compliance. For example, Johnathan Coleman (proposed as the key person responsible for all aspects of the delivery of work under this solicitation) is widely published in HIPAA Security Risk Assessments. His Health IT Security experience pre-dates publication of the HIPAA Security Rule. A more complete list of work by Mr. Coleman is posted online at: http://www.securityrisksolutions.com/publications.html. Examples of his work and credibility include:

- Multiple publications, such as Chapter 6 of the **"HIPAA Program Reference Handbook"** (ISBN: 0849322111 CRC Press, © Auerbach Publications, 2004)

- Key presentations and speaking engagements on behalf of the Government, such as:
  - **"NIST/CMS Workshop on HIPAA Security Rule Implementation and Assurance"** (January 16, 2008; NIST Main Campus, Gaithersburg, MD; and
  - **"Functional Requirements for Security; Authorization, Authentication, Confidentiality, and Credentialing"** - a Presentation on behalf of the Office of the National Coordinator for Health Information Technology (ONC) for the first Nationwide Health Information Network Forum, (June 28-29, 2006; Natcher Center, National Institutes for Health).
  - More recently, Mr. Coleman has presented on Security and Privacy topics behalf of the ONC Chief Privacy Officer at the National HIMSS Conferences in Las Vegas (HIMSS 2012) and New Orleans (HIMSS 2013).
- Provided expert testimony to Federal Advisory Committees which serve as the statutory public advisory bodies to the Secretary of Health and Human Services. At the request of the committees, Mr. Coleman has provided testimony to the Health IT Standards Committee (HITSC), the Health IT Policy Committee and National Committee on Vital and Health Statistics (NCVHS), the National Governors Association (NGA) State Alliance for eHealth, and to the Federal Health Architecture (FHA) Security Strategy Committee. Testimony to the HITSC and HITPC Security and Privacy Work Groups has been instrumental in providing substantial input to certain provisions recently finalized in the HITECH extensions to HIPAA (known collectively as the Omnibus Rule).

Mr. Coleman has experience leading HIPAA/HITECH Security Assessments, Technical Risk Assessments, and Compliance Reviews for numerous projects including large hospitals, distributed networks, and small clinics – both in the public and private sectors. Specific examples of engagements he has led with SRS and its partners are shown in the Project Example summary table (see Table 2) below. **Note that Mr. Coleman has worked on several Security Investigations for cases involving OCR, where he led the team's security audit and inspection activities. In some instances, these investigations were part of a Whistleblower/hotline call, and in other cases they were part of a post-breach remediation activity mandated as part of the OCR sanction under a Corporate Integrity Agreement.** In all cases, including those involving OCR, Mr. Coleman reviewed all the HIPAA Security Policies and Procedures for completeness and accuracy, and also evaluated the organizations' implementation of those policies and procedures. This included a technical investigation of the security posture of the Covered Entity and validation of the security controls described in the appropriate implementation specifications.

> ***"Johnathan Coleman has demonstrated encyclopedic knowledge of security standards and operations, especially with respect to healthcare. SRS has skillfully facilitated large groups of technical experts in reaching consensus conclusions."*** Deborah Lafky, Ph.D., CISSP, Office of the National Coordinator for Health Information Technology, Department of Health and Human Services (HHS/ONC)

All projects were completed successfully, on-time, on-budget, and without any negative action or complaint.

Table 2: SRS and Key Personnel Project Experience

Client/Location	Project Focus	Reference Name/Contact Info	Relevance to Solicitation				
			HIPAA / HITECH Risk Assessment	Technical Vulnerability Assessment	External Penetration Testing	Physical Security Analysis	Policies and Procedures Review
Benefitfocus.com / Charleston SC (Covered Entity)	HIPAA Security Risk Assessment, Applications Assessment	Brian Freedman BrianF@palmettoprimarycare.com Tel: 843-697-2944	✓	✓	✓	✓	✓
Comparative Billing Reports (CBR) Producer System for the Centers for Medicare & Medicaid Services (CMS) /Charleston SC & Washington DC (Covered Entity)	FISMA Audit and Security Risk Assessment	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 (Covered Entity)	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.	Scott West david.s.west8.civ@mail.mil Tel: 011-49-151-544-49850	✓	✓	✓	✓	✓
Memorial Sloan-Kettering Cancer Center (MSKCC)/ NY City (Covered Entity)	HIPAA Security Risk Assessment	Richard Jankowski jankowsr@mskcc.org Tel: (212)-639-6561	✓	✓	N/A	✓	✓
Community Health Network of CT (CHNCT) / Wallingford, CT (Covered Entity)	HIPAA Security Risk Assessment	Cornelia Dorfschmid cdorfschmid@strategicm.com Tel: (703) 683-9600, x.419	✓	✓	N/A	✓	✓
Georgetown University Medical Center (GUMC)/ Washington DC (Covered Entity)	HIPAA Security Risk Assessment	Jeff Collmann, PhD collmanj@georgetown.edu Tel: (202)-870-2196	✓	✓	N/A	✓	✓
US Physical Therapy (USPh)/ Houston, Texas (Covered Entity)	HIPAA Security Risk Assessment	Cornelia Dorfschmid cdorfschmid@strategicm.com Tel: (703) 683-9600, x.419	✓	✓	N/A	✓	✓
Rapid City Regional Hospital/ Rapid City, SD (Covered Entity)	HIPAA Security Risk Assessment	Archie Andrews archieasc@gmail.com	✓	✓	N/A	✓	✓
Princeton Healthcare System/ Princeton, NJ (Covered Entity)	HIPAA Security Risk Assessment,	Cornelia Dorfschmid cdorfschmid@strategicm.com Tel: (703) 683-9600, x.419	✓	✓	N/A	✓	✓
Department of Veterans'	Large-Scale Program Risk	Patrick Burnette	✓	✓	N/A	N/A	✓

Client/Location	Project Focus	Reference Name/Contact Info	Relevance to Solicitation				
			HIPAA / HITECH Risk Assessment	Technical Vulnerability Assessment	External Penetration Testing	Physical Security Analysis	Policies and Procedures Review
Affairs (VA) Post 9/11 Veterans Benefits Program (Chapter 33), and Joint Federal Health Care Center (FHCC)/ Washington DC/ Charleston SC/ Chicago IL (Covered Entity)	Management for major systems ($250M project)	GUS.P.BURNETTE@saic.com Office: (843) 609 7543					
National Institutes of Health (NIH) / Bethesda, MD (Covered Entities)	Federal Safety Reporting Portal (SRP) Technical Risk Assessment and Certification & Accreditation	Latif Khalil LKhalil@JBSInternational.com Tel: (240) 645-4124	✓	✓	✓	✓	✓
Defense Healthcare Information Assurance Program (DHIAP) for Military Health System / Washington DC (Covered Entities)	HIPAA Security Training, Testing, and Risk Assessment for 200+ Healthcare Facilities Worldwide	Jeff Collmann, PhD collmanj@georgetown.edu Tel: (202)-870-2196	✓	✓	N/A	✓	✓
Alabama Regional Extension Center (AL-REC) / Mobile AL (Covered Entities)	HIPAA/HITECH Meaningful Use Security and Privacy Services	Deborah Lafky, Ph.D, CISSP, dlafky@southalabama.edu Tel: (251) 461-1812	✓	✓	N/A	N/A	✓
Office Of The National Coordinator For Healthcare Information Technology (ONC), Office Of The Chief Privacy Officer (OCPO): Program Support For The Data Segmentation For Privacy Initiative	Security and Privacy Standards and Interoperability for HIPAA/HITECH Meaningful Use	Scott Weinstein, J.D. scott.weinstein@hhs.gov Tel: (202) 690-3895	✓	✓	N/A	N/A	✓

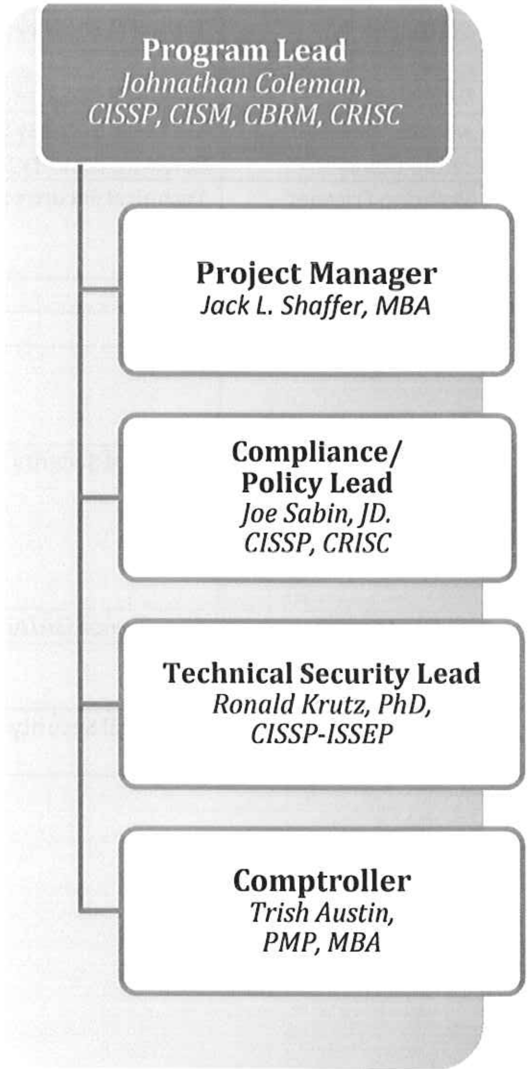
Staffing Plan:

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 PEIA Offices, WV CHIP Offices, and WV Office of Technology Offices, and organize the data in such a way that is usable and informative for the risk assessment. Our technical staff is well versed in network discovery, vulnerability assessment, penetration testing and physical security reviews. Our HIPAA 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. As shown in Figure 1, our staffing plan consists of an experienced and proven HIPAA/HITECH Expert Program Lead, a WV-based project manager, several Subject Matter Experts (including HIPAA security, privacy & policy experts, and technical security experts), and the necessary program support staff.

Figure 1: Staffing Plan

KEY PERSONNEL PRIMARY FUNCTIONS

- **Program Lead:** Responsible for successful completion of all aspects of the project. Has deep experience managing large scale projects and conducting HIPAA/HITECH Security Risk Assessments. As a recognized industry expert, program lead will also direct assessment activities and lead mitigation planning / roadmap development tasks.
- **Project Manager:** Supports Program Lead with local outreach and client liaison activities. Participates in assessment activities (such as knowledge elicitation interviews) and provides daily on-site updates. Leverages understanding and familiarity with client organizational culture to coordinate daily assessment activities without disrupting normal operations.
- **Technical Security Lead:** Provide technical oversight and quality control to all aspects of Security testing, including network discovery, vulnerability detection, false-positive determination and technical writing.



Program Lead
Johnathan Coleman, CISSP, CISM, CBRM, CRISC

Project Manager
Jack L. Shaffer, MBA

Compliance/ Policy Lead
Joe Sabin, JD. CISSP, CRISC

Technical Security Lead
Ronald Krutz, PhD, CISSP-ISSEP

Comptroller
Trish Austin, PMP, MBA

The labor matrix in Table 3 demonstrates the qualifications and certifications held by individuals proposed and available to support this project.

Table 3: Staff Qualification Matrix

Name	**Proposed Role** ***(* denotes key personnel)***	**Employer**	**Certification(s)**	**Degree/Professional Training**
Johnathan Coleman	Program Manager*	SRS	CISSP, CISM, CBRM, CRISC	BEng, Aeromechanical Systems Engineering
Jack Shaffer	Project Manager*	KRM		MBA
Ronald Krutz	Technical Security Lead*	SRS	CISSP, ISSEP	PhD, Electrical and Computer Engineering
Joe Sabin	Compliance/Policy Lead*	SRS	CISSP, FQNV, CBCP, CRISC	JD, Communications Law and Policy
Trish Austin	Financial Comptroller*	SRS	PMP	MBA, Finance
Jeanne Burton	HIPAA Privacy SME/QA	SRS	PMP	Trained US Navy Cryptologist
Ellis Callicoat	Software Security SME	SRS	PMP, Security+, CSM	BS, Computer Science
Cotton, Chris	Technical Security SME	ACG	CISSP, CPHIMS, PMP, FQNV	MS, Healthcare Administration
William Crowe	Technical Security SME	ACG	CISSP, Security +	MS, Network Security
Michael Davino	Technical Security SME	SRS	CISSP, FQNV	MS, Computer Science
Jamie Doyle	Software Security SME	KRM		BS, Computer Science
Brandon Friesner	Technical Security SME	SRS	CISSP, Security+, CCNA, DAWIA IT Level 1	MS, Systems Engineering
David Graham	Analyst	SRS	PMP, Security +	MBA, Finance
Linda Jensen	Analyst	KRM		BS, Information Technology
Ryan Knight	Analyst	ACG	CISSP, C|EH, ILNV, OSCP, MCSA, Security+	BS *(in progress)*, Information Assurance and Security
Chad Litoborski	Technical Security SME	ACG	CISSP, FQNV, MCSA, CCNA, A+, Network+, Security+, Six Sigma Greenbelt	BS *(in progress)*, Information Assurance and Security
James McAlister	Compliance QA/Analyst	SRS	PMP, Security+	MSc, International Relations
Shane McClaughry	Analyst	KRM	Security+, CCNA	BS, Network and Data Communications
Bret Peresich	Technical Security SME	ACG	CISSP, CISA, FQNV, OSCP	BS, Computer Information Systems and Security

7. The vendor should provide at least three (3) references from organizations of similar size and scope to the State of West Virginia, the WV Office of Technology, WV PEIA and WV CHIP that they have provided service(s) to in the past three (3) years. Vendor should include the name and contact information for a person at those organizations that can be used as a professional reference and supply the name, title, address, email, telephone and fax numbers of the contact for your proposal. Please advise that person that they will be contacted by the State of West Virginia for reference verification.

The following past performance references are provided for consideration:

a) 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.

b) NIH/FDA Federal Safety Reporting Portal, Genetic Modification Clinical Research Information System, and The Institutional Biosafety Committee Registration Management System.

c) Strategic Management Systems/Integrity Management Services Inc. Multiple security assessments and penetrations tests for: Comparative Billing Reports (CBR) Producer System, Community Healthcare Network of CT and Princeton Healthcare System.

d) Alabama Regional Extension Center (ALREC): Meaningful Use – Privacy and Security Risk Assessments for Covered Entities and Eligible Professionals.

Table 4: Past Performance 1: Navy Medicine

Security Risk Solutions (SRS): **Navy Medicine Information Systems Support Activity (NAVMISSA)**			
Contracting Organization	Department of Defense/US Navy		
Contract #:	N65236-07-D-7880 N65236-08-D-5801	**Contract Type**	Time and Materials
Contract Value	$1,164,306.68 on N65236-07-D-7880 $ 852,163.10 on N65236-08-D-5801 $ 998,186.33 on N65236-11-D-3854	**Performance Period:**	August 2008 – Sep 30, 2013
Description and relevance to solicitation requirements:			
SRS is tasked with providing Security Risk Management, Compliance, Mitigation, 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 providing technical, security, and healthcare related Subject Matter Expertise to Navy Medicine. This includes conducting reviews, analysis, and providing input to a variety of healthcare policy and technical specifications such as FISMA CyberScope Reporting (XML Schemas for compliance reporting), HIPAA/HITECH Subject Matter expertise relating to standards, interoperability requirements, and healthcare security requirements, Development and Support for Security Technical Implementation Guides (STIGs) such as the Medical Device STIG, and research and subject matter expertise in support of Interoperability Pilots and Regional Health Information Exchanges.			
Points of Contact:			
Primary POC:	Name	Scott West	
	Address	SPAWAR Systems Center CMR 489 Box30 APO AE 09751	
	Phone	+49-151-544-49850	
	Fax	None	
	E-mail	david.s.west8.civ@mail.mil	

Table 5: Past Performance 2: NIH/FDA

Security Risk Solutions (SRS): Federal Safety Reporting Portal			
Contracting Organization	National Institutes of Health (NIH) with FDA Collaboration		
Contract #:	HHSF223200550525G	**Contract Type**	Time and Materials
Contract Value	Ceiling TBD	**Performance Period:**	Sep 2007 – present

Description and relevance to solicitation requirements

Security Risk Solutions is providing security testing, requirements validation, and policies and procedures development for security to the Food and Drug Administration (FDA) and the National Institutes of Health (NIH), as a subcontractor. In one example project, The Safety Reporting Portal (SRP), SRS has provided all aspects of security testing to ensure the system met all Federal security guidelines and conformed with Agency security policies and procedures. The system streamlines the process of reporting product safety issues to FDA and NIH by automating the receipt of reports pertaining to vaccine recalls, medical device malfunctions, other medical adverse events, food safety, and other products. SRS has worked on this inter-agency program for several years, providing technical leadership, security strategy, and technical services including validation throughout the lifecycle from inception through deployment to sustainment. This multi-year program has resulted in a more timely way to identify safety issues, ultimately improving the ability of FDA to efficiently instigate safety recalls. Currently the portal can be used to report safety problems related to foods, animal drugs, and adverse events occurring on human gene transfer trials. The Safety Reporting Portal was placed into production in May 2010 and is operational at www.safetyreporting.hhs.gov. Under subcontract to JBS International, Security Risk Solutions Inc., serves as security Subject Matter Experts and project security officer. This includes review of technical specifications, development of all Certification and Accreditation artifacts, helping development and design teams ensure regulatory requirements are adhered to, and that the security requirements are appropriately designed into the portal development as functional requirements. Security Risk Solutions helped ensure that the tool was designed in a manner which was scalable and secure.

The Institutional Biosafety Committee Registration Management System: (IBC-RMS)

Institutional Biosafety Committees (IBCs) are the cornerstone of institutional oversight of recombinant DNA research. The IBC-RMS is designed to assist the NIH Office of Biotechnology Activities in performing its role of monitoring Institutional Biosafety Committees to ensure every research site conducting recombinant DNA research has a properly constituted and registered IBC. The IBC-RMS is a new system under development. SRS has been tasked to conduct a technical security review of the system and provide System Security Certification and Accreditation documentation, to include: System Security Plan, eAuthentication, Security Test Plan, Security Test and Evaluation Results and Risk Assessment results. Under subcontract to JBS International, Security Risk Solutions Inc., serves as security Subject Matter Experts. This includes review of technical specifications, development of all Certification and Accreditation artifacts, helping development and design teams ensure regulatory requirements for HIPAA/HITECH are adhered to, and that the security requirements are appropriately designed into the portal development as functional requirements.

Genetic Modification Clinical Research Information System (GeMCRIS):

The NIH/FDA Genetic Modification Clinical Research Information System (GeMCRIS) is a comprehensive information resource and analytical tool for scientists, research participants, sponsors, institutional oversight committees, federal officials, and others with an interest in human gene transfer research. GeMCRIS allows public users to access basic reports about human gene transfer trials registered with the NIH and to develop specific queries based on their own information needs. SRS has been tasked to conduct a technical security review of the system and provide System Security Certification and Accreditation documentation, to include: System Security Plan, eAuthentication, Security Test Plan, Security Test and Evaluation Results and Risk Assessment results.

Prime Contractor or Client/Contracting Officer Technical Representative	Name	Latif Kahil, Director, Software Development
	Address	JBS International, Inc., 5515 Security Lane, #800, N.Bethesda, MD 20852
	Phone	Office: (240) 645-4124 Cell: (301)-529-1218
	E-mail	LKhalil@JBSInternational.com

Table 6: Past Performance 3: Risk Assessments for CMS, CHNCT, PHCS, CCTA

Security Risk Solutions (SRS): Strategic Management Systems, Inc. (SMS) / Integrity Management Services, LLC (IMS)			
Contracting Organization	Strategic Management Systems, Inc. (SMS) / Integrity Management Services, LLC (IMS)		
Contract #:	Master Services Agreement	**Contract Type**	Time and Materials
Contract Value	Ceiling TBD	**Performance Period:**	May 2010 – present

Description and relevance to solicitation requirements

Security Risk Solutions Inc. (SRS) serves as security Subject Matter Experts for the Comparative Billing Reports (CBR) Producer System project under subcontract to Strategic Management Systems, Inc. (SMS) / Integrity Management Services, LLC (IMS); for the Centers for Medicare & Medicaid Services (CMS) under the Department of Health & Human Services USA (DHHS). This task includes 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. In these efforts 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. In culmination; Security Risk Solutions ultimately helped ensure that the documentation was sufficiently completed and the Approval to Operate Request was granted by the Designated Approval Authority.

SRS has been working with Strategic Management Systems, Inc. (SMS) / Integrity Management Services, LLC (IMS) in a variety of capacities for several years and continues to provided leadership, security strategy and technical services throughout the lifecycle from inception through deployment to sustainment of various projects. Specific HIPAA Security Risk Assessment engagements included the complete review of all HIPAA Security Requirements, Policies, Procedures, Technical Control validation, compliance audit, and development of detailed recommendations and corrective action plans. For example, the findings and recommendations for the risk assessments included specific cost estimates, staff resources and timelines for mitigation actions to bring the organizations into compliance. Customers SRS and SMS collectively assessed include large Covered Entities, and Health Plans.

Points of Contact

Prime Contractor or Client/Contracting Officer Technical Representative	Name	Cornelia M. Dorfschmid, Ph.D. Executive Vice President, Strategic Management (703) 683-9600, x. 419 (703) 836-5255 (fax)
	Address	5911 Kingstowne Village Parkway, Suite 210 Alexandria, VA 22315
	Phone	703) 683-9600, x. 419
	Fax	(703) 836-5255
	E-mail	cdorfschmid@strategicm.com

Table 7: Past Performance 4: HIPAA/ HITECH Security for Alabama Regional Extension Center

Security Risk Solutions (SRS): Alabama Regional Extension Center (AL-REC)			
Contracting Organization	University of South Alabama		
Contract #:	Master Services Agreement	**Contract Type**	Time and Materials
Contract Value	Ceiling TBD	**Performance Period:**	2 Sept 2012 to present

Description and relevance to solicitation requirements

SRS has been tasked with providing services encompassing sharing and contributing subject matter expertise in the area of Health IT Security and Privacy, with a particular focus on HITECH and HIPAA Security and Privacy Rules, to the University of South Alabama, the Regional Extension Center (ALREC) and approximately 500 healthcare providers throughout Alabama. The tasking includes a comprehensive review of the risk assessment tools in use by ALREC to provide analysis of what is sufficient and what might be improved. Specifically, this includes Policies and Procedures review, HIPAA/HITECH Security and Privacy training for Meaningful Use Risk Assessment Attestation requirements, development of templates, and providing HIPAA/HITECH Security and Privacy subject matter expertise.

Under this tasking, SRS is reviewing the HIPAA Security policies and procedures used internally by ALREC and providing written comment and/or recommendations for updates. In particular, the policies and procedures are being reviewed to assess their completeness and suitability for addressing requirements of the HIPAA Security Rule. Deliverables include marked up policies and procedures (change tracking enabled) with recommendations for changes included in the document. Additional recommendations not specific to any one particular policy or procedure document are included with marked documents. SRS is also reviewing the document template bundle provided by ALREC to assist individual members and provider organizations with the preparation of their HIPAA Security Rule related policies and procedures. Specifically, SRS is providing recommendations for updates and/or improvements for each of the policy or procedure documents. Additionally, SRS is providing subject matter expertise on Security and Privacy related matters, such as the HIPAA Security Rule, changes resulting from the HIPAA/HITECH Omnibus rule, and upcoming requirements still under development at ONC or CMS (such as Meaningful Use requirements).

Points of Contact		
Prime Contractor or Client/Contracting Officer Technical Representative	Name	Deborah Lafky, Ph.D, CISSP, Assistant Dean and Director, Center for Strategic Health Innovation
	Address	Center For Strategic Health Innovation University of South Alabama 775 N University Blvd, TRP II, Suite 250 Mobile, AL. 36608
	Phone	(251) 461-1812
	Fax	None
	E-mail	dlafky@southalabama.edu

8. Vendor should provide a list of the key staff who will be working on this contract including resumes and brief bios that describes their education and experience. Include the amount of time based on percentages that those staff will be assigned to work on this project. Please include the steps that your company takes to ensure the integrity and experience of its staff, e.g., background checks, drug testing, etc.

Key Personnel Biographies:

A brief biography of key personnel is included below. Please refer to the detailed resumes attached as Appendix G for full details.

Johnathan Coleman, CISSP, CISM, CBRM, CRISC is proposed as overall Program Manager for this effort. He graduated from the Royal Military College of Science in the United Kingdom with a Bachelor's Degree in Aeromechanical Systems Engineering, was accepted into the Royal Military Academy, Sandhurst, and commissioned into the British Army. Professional training and certification includes Information Security training (6 Military Intelligence group, UK) and Cryptography and Information Security. He served for 18 months as the Initiative Coordinator for the Data Segmentation for Privacy Initiative at the Office of the National Coordinator for Health IT (ONC) at the Department of Health and Human Services, which is developing security and privacy specifications in support of the National agenda for Meaningful Use adoption of Certified Electronic Health Records systems. This work helped inform the "self-pay" provisions of the recent HITECH/HIPAA Omnibus rule. He has provided testimony to Federal Advisory Committees (HITSC and NCVHS), to the National Governors Association (NGA) State Alliance for eHealth, to the Federal Health Architecture (FHA) Security Strategy Committee, and was an invited speaker at a NIST/CMS seminar on HIPAA Security Rule Implementation and Assurance. Previous experience includes HIPAA Security assessments and investigations for large publicly traded healthcare organizations, private hospitals, VA and DoD Treatment Facilities. Mr. Coleman was appointed co-chair of the Healthcare Information Technology Standards Panel (HITSP) Security, Privacy and Infrastructure tiger team and served as facilitator for the Electronic Health Records Technical Committee. He worked as a visiting scientist at the Networked Systems Survivability department of the Software Engineering Institute CERT® Coordination Center (SEI/CERT) at Carnegie Mellon University. Mr. Coleman supports the Navy Medicine Information Systems Support Activity (NAVMISSA) as a Technical Risk Management SME and is a Fully Qualified Navy Validator for the US Navy Certification Authority. In this capacity he conducts HIPAA risk assessments at various government hospitals and treatment facilities and advises enterprise leadership on technical and strategic HIPAA/HITECH related risks and mitigations.

Jack L. Shaffer, MBA is proposed as Project Manager for this task, and will remain local in West Virginia where he currently lives and works. Mr. Schaffer holds both a Master's Degree in Business administration and A Bachelor of Science Degree in Computer Information Systems from the University of Charleston, Charleston, WV. His career has spanned more than 25 years of deploying secure, functional, and compliant information systems for energy and healthcare businesses. As the CIO of the Community Health Network of West Virginia (CHNWV), he salvaged and reengaged a struggling electronic medical records project that was designed to create new profit center for the organization. The CHNWV began its implementation of the Indian Health Services Resource Patient and Management System (RPMS) EHR – a derivative of the Veterans Administration's VistA EHR - to its member rural health clinics in 2006. In four years, the centrally hosted RPMS-EHR system was deployed in nearly 50 clinical locations and contained more than 190,000 unique patients – over 10% of West Virginia's total population - making it one of the largest EHR's deployed in the State of West Virginia at that time. In his role as CIO, Mr. Shaffer designed and architected the technology infrastructure necessary to support the operation and was responsible for the entire RPMS-EHR application and its implementation.

Ron Krutz, PhD, CISSP, ISSEP, is proposed as the Technical Security Lead for this solicitation. He is the Chief Scientist for Security Risk Solutions. Dr. Krutz holds B.S., M.S., and Ph.D. degrees in Electrical and Computer Engineering and is a Senior Fellow of the International Cyber Center of George Mason University. Dr. Krutz has over thirty years of experience in distributed computing systems, computer architectures, information assurance methodologies, industrial automation and control systems, and information security training. He has been a Senior Information Security Consultant at Lockheed Martin, BAE Systems, and REALTECH Systems Corporation, an Associate Director of the Carnegie Mellon Research Institute (CMRI), and a professor in the Carnegie Mellon University Department of Electrical and Computer Engineering. He was also a lead instructor for (ISC)2 in their Certified Information Systems Security Professionals (CISSP) training seminars. Dr. Krutz founded the CMRI Cybersecurity Center and was founder and Director of the CMRI Computer, Automation and Robotics Group He co-authored the CISSP Prep Guide for John Wiley and Sons and is co-author of the Wiley Advanced CISSP Prep Guide, the Security + Certification Guide, Cloud Computing Security, Web Commerce Security, and 8 additional texts in the information system security field. Dr. Krutz has seven patents in the area of digital systems and has published over 40 technical papers. He also developed the HIPAA-CMM, adapting the HIPAA Privacy, Security, and Code Sets Rules to the Capability Maturity Model paradigm. Dr. Krutz is a Registered Professional Engineer, a Lifetime Senior Member of the IEEE, and a Consulting Editor for John Wiley and Sons Information Security Certification Series.

Joseph Sabin, Esq., CISSP, CBCP, ITIL is proposed as Compliance/Policy Lead. He has served in both military and professional capacities with twenty years combined experience. Notable active duty assignments include the American Forces Korea Network (AFKN) and the White House Communications Agency (WHCA). Mr. Sabin has a Bachelor's Degree from George Mason University, and graduated from The Catholic University of America, Columbus School of Law with a Juris Doctor and Post Graduate Certificate in Communications Law and Policy. Mr. Sabin has specific and demonstrable experience supporting and/or leading activity within Information Assurance (IA) law, policy, process, and security control compliance initiatives for healthcare programs. This includes risk assessment, strategic design and tactical process support for Health and Human Services (HHS) Centers for Disease Control and Prevention's (CDC) and the Navy Medicine Information Systems Support Activity (NAVMISSA) where he serves as the Compliance/IAVM lead. He is a Fully Qualified Navy Validator for the US Navy Certification Authority. In this capacity he contributes to the overall compliance of Medical Treatment Facilities with Agency requirements for Information Security, including the development of mitigation plans and corrective action plans for systems or facilities.

Trish Austin, MBA, PMP is the Comptroller at SRS and is proposed as Financial Comptroller for this program. She has a B.S. (Bachelor of Science) in Accounting from the State University of New York at Geneseo, and an MBA (Masters of Business Administration) with a concentration in Finance from Oklahoma City University. While employed at the South Carolina Research Authority (SCRA) and its affiliate, the Advanced Technology Institute (ATI), she served as a

Project Manager on the 22 million dollar Healthcare Information Technology Standards Panel (HITSP) program. She developed Monthly Status Reports, performed Earned Value Management (EVM), and provided monthly financial analysis to the American National Standards Institute (ANSI) and the Office of the National Coordinator (ONC), in accordance with the HITSP contract. Ms. Austin has over fifteen years of proven experience in financial management, budgeting, and forecasting revenue and expenses. She holds a Project Management Professional (PMP) certification and is a member of the Project Management Institute, Charleston SC Chapter.

Time Commitment of Key Personnel on this Project:

SRS and its subcontractors will make this program our top priority. The percentage of time dedicated to the project, shown in Table 8 below, is for key personnel and recognizes that along with their seniority and experience comes corporate responsibility. Our team fully commits to provide the resources necessary to complete the task with upmost professionalism and to the highest standards. Our key personnel are always available to customers, and will be highly visible to the customer throughout the engagement.

Table 8: Key Personnel Time Commitment

Name	Key Personnel Role	Employer	Percentage of Time Dedicated to Project
Johnathan Coleman, CISSP, CISM, CBRM, CRISC	Program Manager	SRS	50%
Jack Shaffer, MBA	Project Manager	KRM	75%
Ronald Krutz , PhD, CISSP, ISSEP	Technical Security Lead	SRS	50%
Joe Sabin, JD, CISSP, FQNV, CBCP, CRISC	Compliance/Policy Lead	SRS	25%
Trish Austin, MBA, PMP	Financial Comptroller	SRS	25%

Personnel Security & Background Checks:

SRS and its subcontractors take personnel security very seriously. SRS conducts detailed background checks on all employees, and requires its subcontracts to do the same. Our staff are all experienced, well known experts in their particular field, and their work experience is readily verifiable. In addition, our staff turnover rate is impressively low – only 3 employees in over eight years - so clients can be assured that the staff working on their projects fully reflect the ethics, professionalism, and caliber that one can expect from SRS.

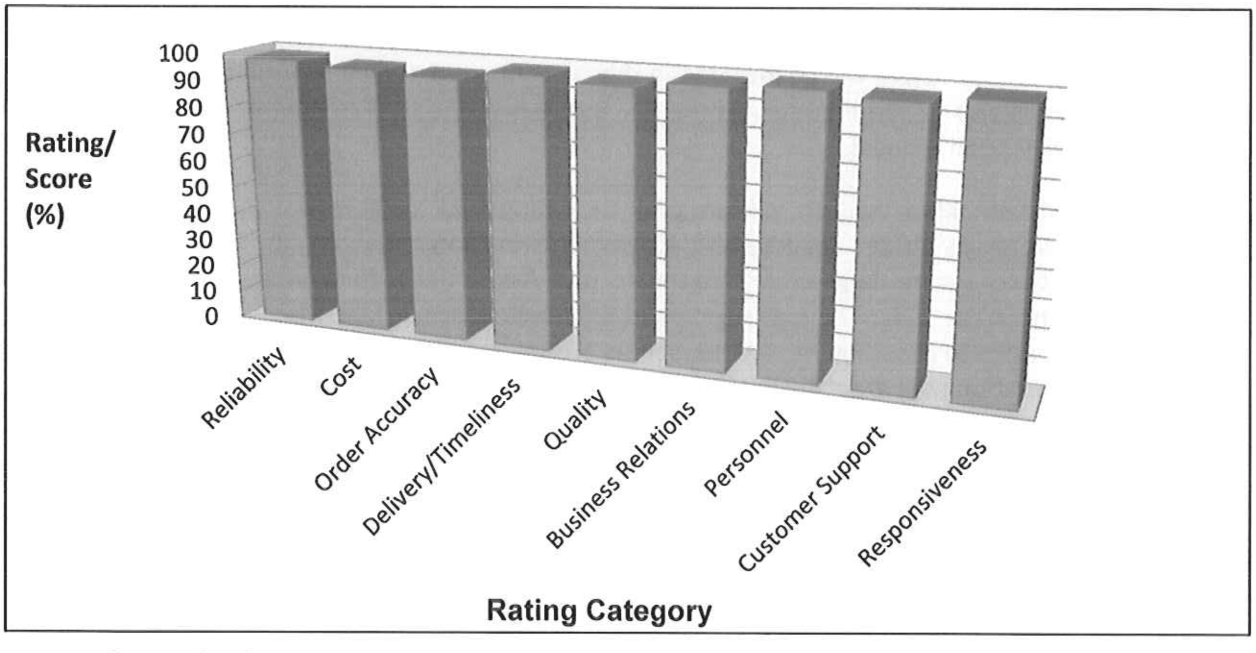
SRS is used to working in highly sensitive environments, where the risk of harm to third parties is substantial, should any sensitive information be improperly handled. Additionally, there is nothing more important than the safety and security of our clients and employees. To that end, SRS conducts detailed criminal background checks on all employees, including credit checks, and where applicable, drug testing. As a testament to our rigor in this regard, SRS holds a Department of Defense Top Secret facility security clearance. All SRS key personnel proposed for this effort hold DoD SECRET or TOP SECRET clearances, which were only granted by the Defense Security Service after extensive background checks and interviews with colleagues, neighbors, lifestyle reviews, and in some cases even polygraph tests. SRS maintains a zero tolerance drug-free workplace, and is often called upon to demonstrate compliance for specific project with drug tests (urinalysis and/or hair samples). SRS maintains a substantial personnel security program, which includes detailed quarterly reviews of our security policies and procedures, bi-weekly security awareness bulletins, annual employee security awareness and training, and project specific clearance processing. In a recent Federal audit of our personnel and facility security program, SRS was given significant praise and graded "commendable", which is among the hardest grades to achieve.

9. Vendor should provide summary information describing its current base operation and share any satisfaction measures and results that it collects and/or maintains.

For every project we have conducted, SRS has provided exemplary services which exceeded expectations for quality and performance. Our deliverables are always reviewed for quality prior to submission to ensure the highest standards of workmanship. Our adherence to sound program and project management principles, consistent with the Project Management Institute's Project Management Body of Knowledge (PMBOK®), ensures projects have sound administration, including schedule management, communication management, risk management, financial control and contract administration. We always deliver high quality products and services on or ahead of schedule.

SRS has a history of customer satisfaction and for going above and beyond what is required to ensure program success, while being respectful of the often limited time our clients have to dedicate to the program. We aim to provide clear, concise and relevant services, fulfilling our customers' needs and instilling confidence in our customers and other project participants alike. As further evidence of our commitment to quality, performance and customer satisfaction, SRS contracted Dunn and Bradstreet (D&B) to contact our customers and provide an independent review of their level of satisfaction with our services. The resulting D&B Open Ratings Past Performance Report (Figure 2 below) showed an average score of 97% across the range of performance measures evaluated, including responsiveness, quality, timeliness, customer support and business relations.

Figure 2: D&B Open Ratings past Performance Report



From a financial solvency stand-point, SRS base operations are in excellent shape. We have strong working capital and an adequate emergency fund to cover all liabilities such as payroll, insurance and operating costs without concern. Now in its 9th year of business, SRS has a 100% track record of paying vendors and subcontractors on time, and paying all Federal, State and local taxes and withholdings. SRS is privately held and debt-free, so there are no loans or capitol investors to be reimbursed. Recent financial audits by the General Services Administration, a State Tax Agency, and an independent financial auditor (hired by SRS to conduct a self-evaluation of our financial health) all reported favorable results. The reports indicated our accounting practices we fiscally sound, cost control was very good, and accounting principles followed Cost Accounting Standards (CAS) and were in keeping with Federal requirements as established by the Defense Contract Audit Agency (DCAA).

Awards/Commendations:

SRS has received several company awards, commendations, and customer accolades. For example, SRS staff received coveted "Bravo-Zulu" commendations from the Navy Medicine Information Assurance director for their outstanding work in getting all 23 major hospital networks successfully accredited (note: accreditation activities include full system security vulnerability testing, remediation, policies and procedures validation, physical security assessment, and IT contingency plan testing).

> ***"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, impressive."***
> David C. Lewis, CISSP, Information Security Officer, IESO

10. Vendor should list and detail all relationships with any and all third party vendors and/or subcontractors who may be included in its proposed solution(s) or that may perform work on this project.

As described in our response to Question #4, Security Risk Solutions Inc. (SRS) is proposed as prime contractor for this project, with KRM Associates Inc. and Athena Consulting Group LLC (ACG) as subcontractors. SRS has fully executed, legally binding Teaming Agreements and Non-Disclosure Agreements in place with each subcontractor. SRS has signed the WV Business Associate Agreement (BAA) and included it as Appendix E to the proposal. SRS understands the importance of ensuring all information is adequately protected. All requirements of the HIPAA Security Rule that apply to Business Associates and Subcontractors will be included in the subcontract agreements with the subcontractors. Subcontractors will also be required to sign the WV Business Associate Agreement. A copy of each will be provided to WV upon request.

SRS has worked with KRM Inc., on various projects dating back eight years, including support for Department of Veterans' Affairs Security Risk Assessments in Morgantown, WV. SRS has also worked closely with ACG on several large-scale Healthcare Risk Assessments for various Medical Treatment Facilities throughout the USA. The experience and tight-knit trust our teammates share has proven to be an invaluable asset to ensuring the right personnel are selected for the task a – regardless of which of our team's organization they are employed by.

SRS is not a reseller of any third party products, so there is no chance of any profiteering or promotion of products that are not needed or considered "best for purpose". Each of the scanning tools used to assist with the assessment is purchased or licensed directly by SRS (e.g. NESSUS Professional). Any other specialty tools or products that may be recommended as a result of the assessments are either purchased directly by the client, or purchased by SRS on behalf of the client (after client approval) and delivered with zero indirect or pass-through costs.

All travel is reimbursable according to the client travel policies. In the absence of such a travel policy, SRS uses standard Joint Travel Regulations as required under Federal Government contracts. This ensures the most cost effective travel and requires pre-approval of all travel and other direct costs. Once again there are no indirect or other pass-through charges applied to any travel or other direct costs.

Contract Management:

Mr. Johnathan Coleman, the SRS Program Manager, will be directly responsible for fulfillment of all areas of the contract. With support from the SRS Comptroller, this includes:

- **Accountability:** Remaining accountable to the client for schedule, budget, and quality of all program elements. Escalating decisions to executive sponsors to the Contracting Officer/Contracting Officer's Technical Representative (COTR) as necessary.
- **Management**: Planning and administering the overall program and delivery of work specified in the Statement of Work.
- **Financial Management**: Implementing fiscal practices and cost control.
- **Infrastructure:** Ensuring the program office, technology, and other factors in the work environment supporting the program effort are available and appropriate.
- **Planning:** Performing activities that take place at multiple levels. Leading development of program plan, Work Breakdown Structure (WBS) and schedule development.
- **Outreach and Communication:** Ensuring effective communication with the government, team members, community stakeholders, and other entities (such as audit agencies) as needed. Serving as the communications conduit to executive sponsors and conducting periodic briefings/status updates.
- **Budget Administration and Procurement:** Working with the COTR to ensure timely and appropriate budget administration, tracking against the WBS, and contract actions.
- **Risk Management:** Conducting periodic risk review meetings, tracking risks, issues, triggers, and coordinating the development of mitigation strategies. Providing risk status reports, metrics and measures to the COTR.
- **Status Reporting Management:** Utilizing a Program Analyst and/or Comptroller to track deliverables against milestones and support collection of data for effective status reporting.
- **Quality Assurance:** Instituting quality processes for work products to include configuration management, control, ownership, and review. Implementation of Quality Assurance Surveillance Plan (QASP) criteria to measure internal performance against project milestones and deliverables.
- **Configuration:** Implementing version control and configuration management of contract deliverables (e.g. the project plan) and community developed artifacts (e.g. Test Procedures).
- **Work Breakdown Structure:** Development of WBS items, mapping and including WBS items in the Project plan, and tracking progress and effort against each WBS item.
- **Resource Management:** Ensuring appropriate internal resources are available, coordinating schedules and delivery of services around Federal and State holidays and other events (such as conferences which may affect client resource availability).

11. Please describe your approach to initial engagement with the customer and what expectations you have of the customer in order to begin work on the project. Include time and resource expectations, logistical considerations, etc.

Contract Award:

Immediately upon award, SRS will work with the client to schedule a project kick-off meeting. This meeting will be face-to-face and will address all aspects of program management to establish expectations for execution and delivery of the services. Prior to the meeting, SRS will provide the customer with a "document request list" and discuss via conference call the artifacts that will be requested. These artifacts will allow SRS to retroactively review work completed thus far by the client. Examples include reports from previous as assessments and existing policies and procedures. This review will ensure the Program Manger and customer representatives share a common understanding of the project's history, the customers' resources available to support the planned activities, and the roles of other project team members and stakeholders.

Upon award, SRS will also conduct a complete review of the West Virginia business requirements and ensure that any pending State registrations, business licenses, and other enrollments legally required by WV are complete. Additionally, SRS will promptly notify our insurance agents of the project and obtain any insurance certificates – indemnifying and listing the client as additionally insured – prior to beginning work on the project. SRS will provide written notice to the client that all legally required registrations and licenses have been obtained.

Post Kick-Off Award Meeting:

SRS will prepare draft materials (such as a Work Breakdown Structure, Detailed Project Plan, etc) and facilitate the post-award meeting with the COTR and client representatives within two weeks after award. During the meeting, SRS will present the draft WBS, schedule/project plan, and identify any concerns or information gaps needed for effective planning. SRS typically conducts post award project kick-off meetings in person. If the customer prefers a virtual meeting environment, SRS has an established process and proven ability to effectively collaborate in a virtual environment.

Additional discussion items recommended for the post-award meeting agenda include:

- Communication protocol, including identification of client preferences for communication with other Agency representatives (e.g., conditions for working through State of West Virginia Public Employees Insurance Agency versus direct communication with other parties).
- Format/frequency of reporting and recurring touch-point calls.
- Review of a draft monthly report format for financial and monthly status reporting.
- Review of the proposed Labor Matrix and confirmation/contact information for individuals to be assigned to the project.
- Anticipated travel schedule/black-out dates for no travel due to holidays, conferences etc.

Project Work Plan:

Within ten (10) working days of the post-award meeting, SRS will provide the detailed work plan containing WBS elements, plan of action and milestones, schedule of interim and final deliverables, and a spend plan tied to deliverables and WBS elements. The work plan will explicitly identify any critical dependencies between tasks, on external parties, or on the Government and will provided in MS Word. Additionally, Gantt chart representations of the project plan will be provided in MS Project and .pdf formats, and once approved will serve as the initial baseline for milestone tracking. SRS will request approval to proceed with the activities included in the project plan. During execution of the plan, if additional tasks or activities are identified or changes to the original plan become necessary, SRS will treat such items as change requests requiring Contracting Officers Representative (COR) approval.

Processes for quality assurance for document deliverables will include sufficient time for internal review and Government review of draft or interim deliverables.

All subsequent additions or material changes to the project plan will go through a change control process. Change requests will be submitted electronically using a change request form which will be provided to the COTR upon the first change request. The initiator completes his/her portion of the form and passes it to the SRS team Program Manager and a request number is assigned. The SRS team reviews the request, researches the impact and risk, formulates and documents a response including the impact on the project schedule and cost, and returns the request to the COTR for approval or rejection. Any approved change requests will be incorporated into the performance baseline and project management plan as appropriate.

Technical Capabilities: Approach & Methodology

12. Describe how the vendor will provide the Covered Entities with thorough documentation of their IT Environments including interfaces and an overall system map. Provide sanitized examples of documentation, such as, architectural/infrastructure design documents, entity relationship diagrams and other artifacts that the vendor would typically uses to describe the environment.

The SRS team is highly experienced in documenting IT environments, and has a proven methodology and recognized credibility in performing this task with accuracy. For example, SRS and ACG work together to validate the Navy Medicine networks for over 140 different facilities world-wide, which include 29 Major medical facilities. Our team routinely conducts independent verification and validation of the security posture of these networks, and the first technical step in each instance is that of network discovery.

The following bullet points provide an example of our repeatable and proven processes for network discovery and documentation:

- Enumerate devices using tools such as Hyena, which shows domain controllers, networks and external interfaces.
- Use network assessment tools such as Nessus to discover all active devices within the entire range of assigned IP address space, to enumerate additional devices. These results are then cross-referenced with the Hyena discovery results to validate findings. Anomalies are investigated further and manually enumerated.
- Interviews with technical staff are conducted to better understand the network architecture, including items not readily discoverable through scanning tools such as techniques for achieving defense-in-depth, firewall configuration techniques and best practices, VLAN configuration and remote access solutions.
- In some instances, auto-mapping tools can be used to develop engineering topology diagrams, however it is our experience that that in most cases, diagrams created manually using information gathered in the steps previously described produce cleaner, more accurate and visually more understandable topology diagrams. SRS prefers the use of Visio for documenting topology diagrams, but also uses Enterprise Architect and the Unified Modeling Language (UML) - which is standardized under ISO / IEC 19501:2005 – to depict information flows related to system behavior between information systems.

We hold the confidentiality of our customers' data in the highest regard, and therefore provide the following two diagrams only as representative examples of the type of documentation the SRS team typically provides. The first, shown at Figure 3 **Error! Reference source not found.**, shows a diagrammatic representation of server room equipment and connectivity to third party systems through the network interfaces. The second, Figure 4: Example of One Section of Network Topology Diagram Figure 4, shows only a portion of a network topology diagram created as part of a set of diagrams used to document a different client network. Note that in each case, supporting detail has been deleted, redacted, and components architecturally modified in order to ensure the confidentiality and integrity of client data is maintained.

Figure 3: Representative Example of Server Room Detail with WAN Connectivity

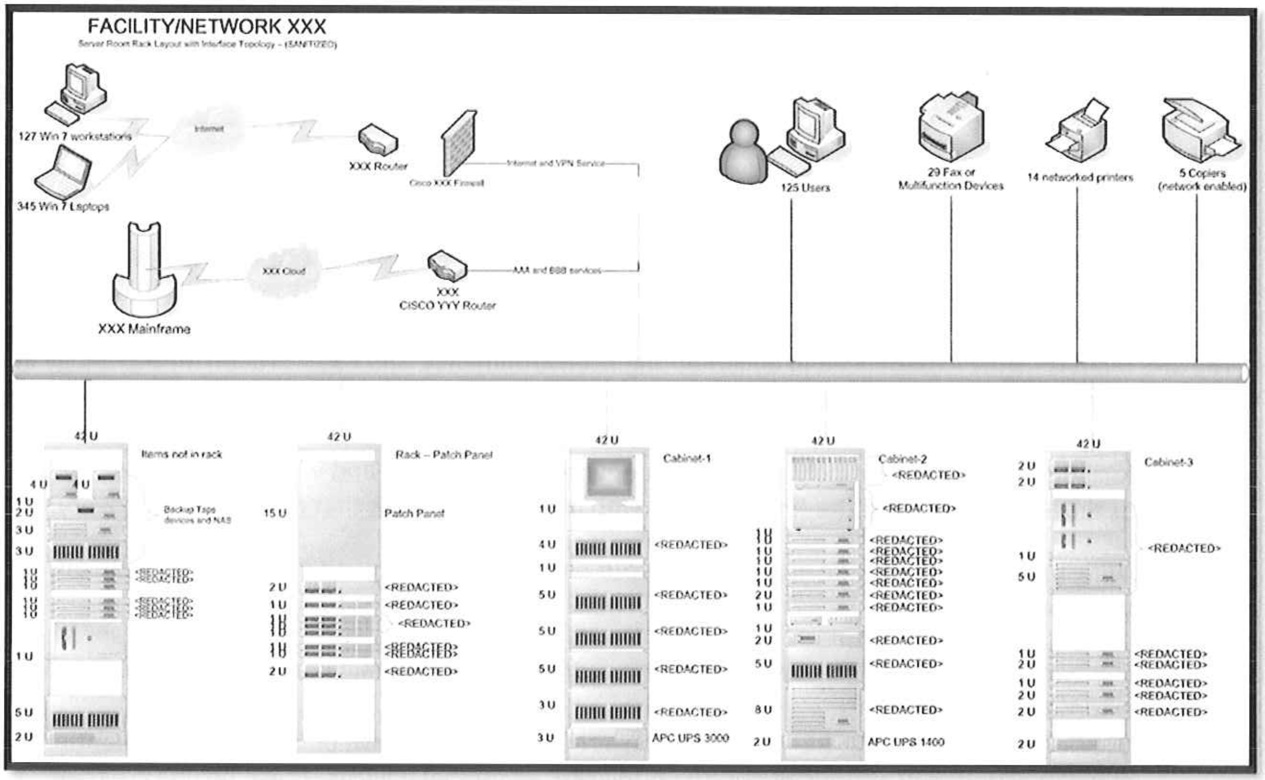
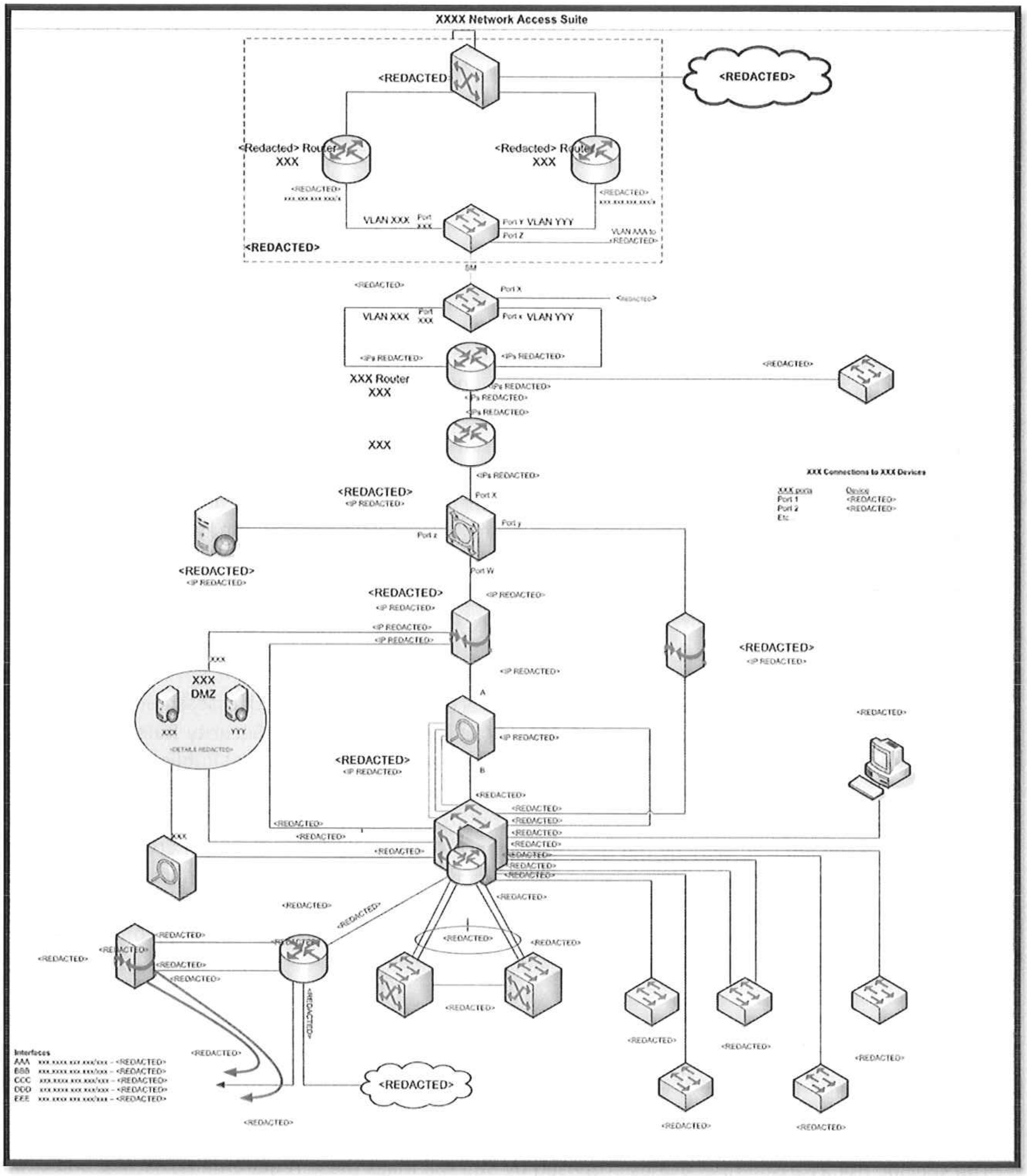


Figure 4: Example of One Section of Network Topology Diagram



13. Describe how the vendor will review and identify any and all internal and external information security vulnerabilities (actual and potential) in the context of best practices, standards and regulations. The requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), National Institute of Standards and Technology (NIST), and International Organization for Standardization (ISO) should be addressed. If new requirements are identified as part of the HITECH Act as set forth in the American Recovery and Reinvestment Act (ARRA) of 2009, HIPAA related or other, prior to the completion of the Information Security Assessment, the new requirements should be reviewed and included as part of the final deliverable review and identify internal and external protected data.

Basis for the Assessment Approach:

The base approach used by SRS for conducting Risk Assessments is exactly that approach published in Guidance by the Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare & Medicaid Services (CMS). On February 17, 2009, the President signed the American Recovery and Reinvestment Act of 2009 (ARRA). This statute includes The Health Information Technology for Economic and Clinical Health Act of 2009 (the HITECH Act) that sets forth a plan for advancing the appropriate use of health information technology to improve quality of care and establish a foundation for health care reform. The HITECH Act authorizes CMS to administer incentives to eligible professionals (EPs) and hospitals for meaningful use of certified electronic health records (EHRs). These incentives are anticipated to drive adoption of EHRs needed to reach the goal of all Americans having secure EHRs by 2014. In addition, certain aspects of the HITECH Act were also the basis for extensions to the HIPAA Security Rule, including processes for Breach Notification Determination, Safe Harbors for Breach Notification, Updates to the standard definitions used to trigger breach notification, and to extend certain provisions of HIPAA to certain subcontractors of Business Associates (thereby making them liable).

SRS Risk Assessment methods follow the eight step process for conducting risk assessments in a manner that meets the requirements set forth at 45 CFR 164.308(a)(1) - the HIPAA Security Rule - and remains consistent with NIST Special Publication 800-30 revision 1 and other NIST Special Publications. SRS has a thorough and longstanding working knowledge of NIST special publications and Federal Information Processing Standards. For example, SRS was requested to participate in the development of the security overlays recommended to NIST by the DoD/Intelligence Community for inclusion in Special Publication (SP) 800-53 revision 4. The SRS Risk Management Framework, described in more detail in response to Question #17, contains a comprehensive mapping of all the NIST SP800-53r4 security controls with the implementation specifications of the HIPAA security rule, the DoD 500.2 security control set, and supporting other NIST Special Publications (including NIST SP800-37, SP800-30, and SP800-18).

A key component of "meaningful use" is the Core Objective for Privacy and Security, which requires Eligible Professionals to conduct a security risk analysis in accordance with the requirements under §164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

The specific risk assessment activities proposed by SRS will meet these requirements. At the end of the assessment, the client organization will have not only met the requirements of §164.308(a)(1), but will have a prioritized list of recommended actions and mitigations strategies which will serve as a compliance roadmap. The risk assessment will include a detailed review of the following:

a) Policies and Procedures Gap Analysis: Review of HIPAA Security policies and procedure to determine if they are complete and appropriately implemented.

b) Security Rule Implementation Specifications Gap Analysis: A complete review of the Administrative, Physical and Technical implementation safeguards as specified in of §164.308(a)(1). This will included a comprehensive technical vulnerability assessment of the technical infrastructure and a physical security review of the identified locations.

c) The technical and organizational risk assessment following eight step process as described in HHS/CMS guidelines:

    1. Identify the scope of the analysis.
    2. Gather data.
    3. Identify and document potential threats and vulnerabilities.
    4. Assess current security measures.
    5. Determine the likelihood of threat occurrence.
    6. Determine the potential impact of threat occurrence.
    7. Determine the level of risk.
    8. Identify security measures and finalize documentation.

d) These activities will feed the development of a prioritized list of recommendations – constituting a "compliance roadmap". The list will include mitigation recommendations for identified risks and corrective action suggestions for any mandatory requirements deemed to be incomplete.

Technical Assessment:

In addition to the HIPAA / HITECH compliance gap analysis and security risk assessment, SRS will include a comprehensive technical assessment of the network infrastructure. The techniques used for this phase of the assessment satisfy the "evaluation" requirements of the HIPAA Security Rule, 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 the HIPAA Security Rule are in scope for the assessment, and compliance is measured against NIST special publications, ISO standards, CVE vulnerability database information, and regulatory language in appropriate Federal Register preamble and document entries.

External Assessments are also utilized to identify interfaces with third party systems, including internet facing applications and services such as VPN endpoints, remote access interfaces for users and administrators, and demarcation points for EDI systems. False positives are identified and removed as risks from the report.

We refer to the technical phase of the HIPAA Risk Assessment as the Security Test and Evaluation (ST&E) phase. 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 eight years, and also in conducting technical security evaluations for Covered Entities as part of their ongoing evaluations, or as part of an OCR directed Corporate Integrity Agreement resulting from a reported breach. The team recognizes the need for conducting comprehensive ST&Es as a part of the required assessment of security controls on a given system or network. The ST&Es have been conducted using Government approved standardized operating procedures (SOPs) and scoring methodology in accordance with Federal, 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 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.

Tailoring the Methodology:

SRS has a well-established process for conducting Risk Assessments that are in compliance with Federal requirements and follow international standards and best practices. We also recognize that no two organizations are alike, and one key to success is knowing how to tailor the assessments to suit the technical and operational environment. In fact, SRS has conducted sufficient HIPAA Security Risk Assessments that it has been able to publish research based on experiences learned; including methodology tailoring techniques, best practices for conducting evaluations, and efficient ways to develop and implement mitigation strategies to address common risks. This research has been presented at conferences, and taken as input to best-practice publications and instructional materials. Specifically, SRS was instrumental in tailoring the Risk Assessment Methodology published by the Software Engineering Institute (SEI) at Carnegie Mellon University to suit the needs of Federal Agencies and their partners. SRS helped the Social Security Administration (SAA) tailor the Operationally Critical, threat, Asset and Vulnerability Evaluation (OCTAVE) method to meet Federal Requirements as described in NIST Special Publication 800-30. SRS is recognized in several SEI/CMU Technical Notes and Publications as important contributors to the work.

For large, complex, and widely spread organizations, SRS has been highly effective in creating and implementing an iterative and distributed approach to the data gathering phases of the risk assessment. For example, SRS has utilized web-survey capture mechanisms to gather data from physicians and network users at remote locations, consolidating this data and performing analysis to help identify common concerns and risks across the enterprise. Additionally, new tools and guidance has been published by ONC; such as the OCIL based HIPAA Self-Assessment tool. These tools are provided by the Government and are freely available.

It should also be noted (and expected) that not all risks identified during a risk assessment will be technical in nature. For example, one commonly occurring operational and procedural risk is attributed to HIPAA Business Associates (BAs) (and now under the HIPAA Omnibus Rule certain subcontractors of BAs) who have failed or refuse to sign a Business Associate Agreement (BAA). SRS has worked with legal counsel for various providers and entities affected by this risk, as well as through informal discussions with representatives from the Office of Civil Rights (OCR) who are responsible for compliance and enforcement actions. These types of guidance and first-hand experience in developing mitigation strategies to complex problems – which are often times policy or legal problems – set us apart from vendors who are more focused on "point-in-time" vulnerability analysis.

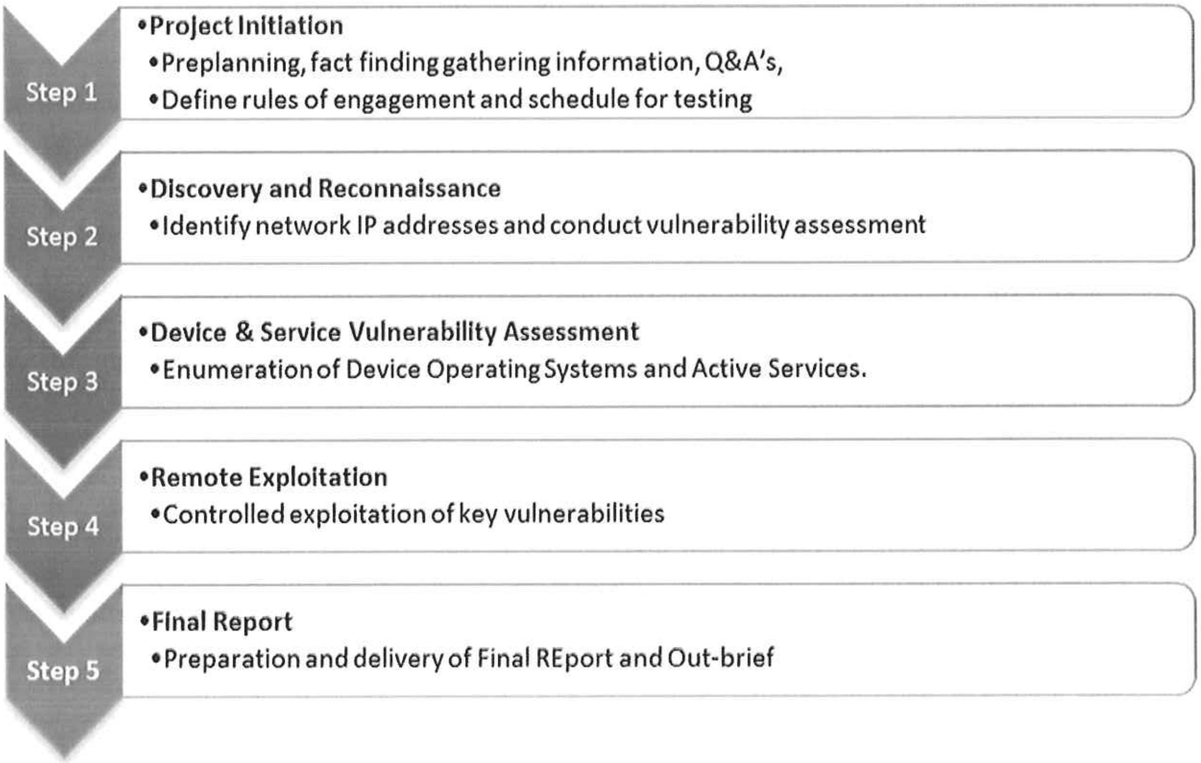
Finally, it should be noted that SRS works very closely with ONC and helps to inform rule-making and strategies for Security and Privacy, such as the Data Segmentation aspects of the "Self-Pay" requirements published in January 2013 as part of the HIPAA Omnibus Rule. This close working relationship with ONC is a testament to our credibility, current and relevant experience, and rational consideration when addressing difficult policy and technical challenges with our clients.

14. Identify how the vendor will provide to the Covered Entities a description of how it will identify and evaluate access points, e.g., web sites, ftp site(s), interfaces, etc. for real and/or potential security vulnerabilities.

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 vulnerability assessments on clinical systems and general support systems, and are experienced in performing disciplined and rigorous penetration tests.

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 the Comparative Billing Reports (CBR) Producer System for the Centers for Medicare & Medicaid Services (CMS). 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 for CMS. The penetration testing portion of the ST&E task consisted of 5 primary steps as shown in Figure 5:

Figure 5: Penetration Testing Methodology Overview



Step 1

- Project Initiation
  - Preplanning, fact finding gathering information, Q&A's,
  - Define rules of engagement and schedule for testing

Step 2

- Discovery and Reconnaissance
  - Identify network IP addresses and conduct vulnerability assessment

Step 3

- Device & Service Vulnerability Assessment
  - Enumeration of Device Operating Systems and Active Services.

Step 4

- Remote Exploitation
  - Controlled exploitation of key vulnerabilities

Step 5

- Final Report
  - Preparation and delivery of Final REport and Out-brief

Example of Penetration Testing Methodology Utilized by SRS on a Covered Entity:

- 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 less than 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.

15. Describe how the vendor will prepare and deliver a formal presentation and written documentation describing the assessment approach, findings, risk, impact and recommendations to correct or mitigate weakness and vulnerabilities. The vendor should provide a sample executive summary including a detailed technical report.

SRS will prepare the Risk Assessment report iteratively, throughout the project. As each project step is complete (e,g, Discovery, Vulnerability Assessment, Threat Analysis, etc) a corresponding section of the report will be written and vetted with the customer. SRS will ensure that the completed DRAFT report is 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 the draft report will be updated to reflect the outcomes of the discussions. Only then will the report be considered final and submitted to the customer for acceptance. Along with delivery of the report is a final-report out-brief and Question/Answer discussion. This gives executives, sponsors and other stakeholders an opportunity to ask questions, dig deeper into findings or recommendations, and garner clarity and context which may not have been readily apparent.

A sample Executive Summary Report is included at Appendix H: Sample Executive Summary Report with Technical Information. Naturally, this report is provided as an example only, and is an excerpt from an actual report that followed an outline agreed to by that particular client. SRS fully expects and looks forward to customizing the report structure to specifically suit the needs of the West Virginia Public Employees Insurance Agency.

16. Describe how the vendor will provide realistic action plan supported by a cost analysis in the context of the agencies, environment(s) and available resources. Action plans need to include 'projected capital and operating expense required, as well as estimated level of effort by internal resource type and estimated duration of effort.

A critical part of the Risk Assessment activity is mitigation planning. 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 over the last ten years of conducting HIPAA Security Risk 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). Those mitigation strategies that are considered by the customer as viable and are selected for further planning will be validated with a deeper and more comprehensive cost estimate. This often requires requesting quotes from third parties (e.g. in the event that hardware or software procurement is necessary), or working with the client to create innovative ways to repurpose existing project activities to address identified risks.

17. Describe how the vendor will describe the benefits the State of West Virginia, WV PEIA and WV CHIP will achieve through partnering with its company. Where possible, quantify the expected benefits. This may include the results of other benefit analysis performed or client contact names that may be referenced.

The State of WV and its constituent departments will benefit from our team expertise and experience in conducting risk assessments in a number of ways which we believe to be differentiators. Table 9 below, summarizes just a few of these benefits. This information is in addition to complimentary, supporting information included in our response to Question #20.

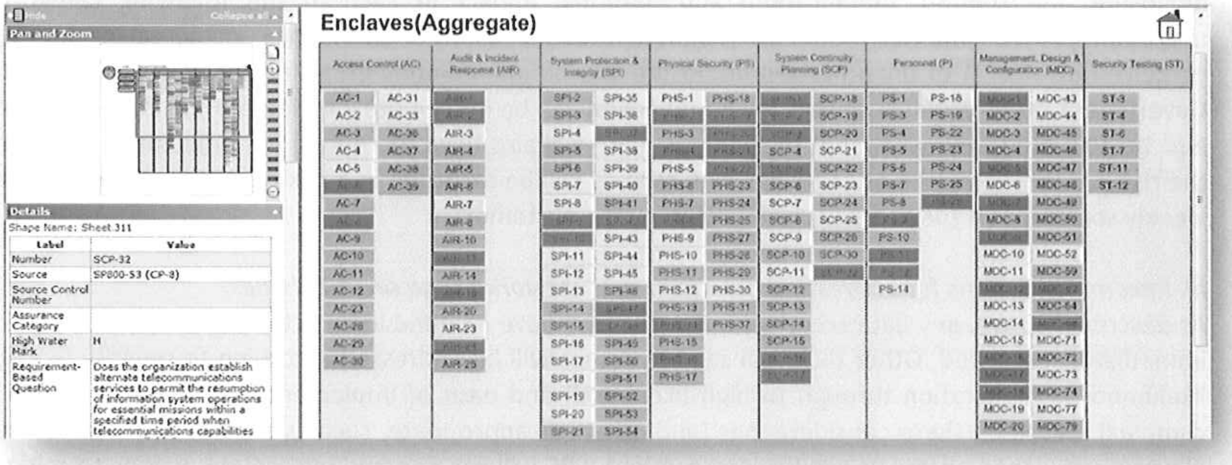
Table 9: Benefits of the SRS Team

Differentiator	Benefit to Client
Expert facilitators of a variety of different methods for conducting HIPAA Security Risk Assessments.	Finely tuned Risk Assessment methodology introduces efficiency and cost savings to the process. For example, a "standard" OCTAVE based assessment can take up to 3 months to perform, while the SRS "tailored" approach generates superior results in half the time.
Vast experience conducting HIPAA Security Risk Assessments	Visibility to a huge number of threats/risks identified during 10 years of risk assessments allows us to help WV ensure that unanticipated risks/unfamiliar threat vectors are not overlooked.
Purposeful Knowledge Transfer	We lead and facilitate risk assessments in a manner that ensures knowledge transfer to all participants. This fosters learning and customer ownership the results, which in turn helps focus appropriate attention to mitigation activities and improves the overall risk posture of the organizations.
Comprehensive Requirements Traceability Matrix	SRS has developed a comprehensive mapping of all the HIPAA/HITECH Security Controls to the relevant NIST Special Publications (including 800-53rev4 and 800-30rev1)and other Federal requirements. This comprehensive mapping is used to make the assessment data gathering steps highly efficient (by mapping duplicative requirements from different regulations to a single control measure). It also presents a near real-time risk snap shot, color coded by risk and organized in families of controls to present an executive level dashboard with "drill-down" capabilities to see the detail. This was developed in-house to help with analysis and reporting, and is therefore NOT commercially available. SRS will use this tool during the engagement and provide monthly risk snapshots to the customer as part of the ongoing task. This tool allows us to conduct more detailed analysis, including risk trending, at no additional cost.
Cohesive team of industry recognized experts	The SRS team have been working together on risk assessments for many years, presenting a cohesive team that is well prepared, expertly facilitated and providing a very low-risk choice to the client. Our expertise in HIPAA and Security is well renowned. The staff proposed on this project include National and International Experts in their field, often called upon by rule-makers to provide real-world opinion during rule making processes. WV can rest assured our services will be comprehensive, yet efficient. Our close ties to the broader Health IT and rule-making communities position us well to convey the very latest in direction ,vision, and focus areas of ONC/CMS/OCR pertaining to regulatory compliance.

Risk Management Framework and Regulatory Requirements Analysis:

As a matter of consistent practice, SRS deliverables and operational activities conform to applicable Federal standards and parameters. For example, SRS has conducted a comprehensive evaluation of Federal requirements for Information systems and programs, and mapped each individual requirement (including specific technical controls) into a Federal information security requirements traceability matrix; we call the Risk Management Framework (RMF). An example representation/snapshot of the SRS RMF dashboard is shown in Figure 6.

Figure 6: Risk Management Framework Tool (Snapshot)



Shape Name: Sheet.311

Label	Value
Number	SCP-32
Source	SP800-53 (CP-8)
Source Control Number	
Assurance Category	
High Water Mark	H
Requirement-Based Question	Does the organization establish alternate telecommunications services to permit the resumption of information system operations for essential missions within a specified time period when telecommunications capabilities

Enclaves(Aggregate)

Access Control (AC)		Audit & Incident Response (AIR)	System Protection & Integrity (SPI)		Physical Security (PS)		System Continuity Planning (SCP)		Personnel (P)		Management, Design & Configuration (MDC)		Security Testing (ST)
AC-1	AC-31	AIR-1	SPI-2	SPI-35	PHS-1	PHS-18	SCP-1	SCP-18	PS-1	PS-18	MDC-1	MDC-43	ST-3
AC-2	AC-33	AIR-2	SPI-3	SPI-36	PHS-2	PHS-19	SCP-2	SCP-19	PS-3	PS-19	MDC-2	MDC-44	ST-4
AC-3	AC-36	AIR-3	SPI-4	SPI-37	PHS-3	PHS-20	SCP-3	SCP-20	PS-4	PS-22	MDC-3	MDC-45	ST-6
AC-4	AC-37	AIR-4	SPI-5	SPI-38	PHS-4	PHS-21	SCP-4	SCP-21	PS-5	PS-23	MDC-4	MDC-46	ST-7
AC-5	AC-38	AIR-5	SPI-6	SPI-39	PHS-5	PHS-22	SCP-5	SCP-22	PS-6	PS-24	MDC-5	MDC-47	ST-11
AC-6	AC-39	AIR-6	SPI-7	SPI-40	PHS-6	PHS-23	SCP-6	SCP-23	PS-7	PS-25	MDC-6	MDC-48	ST-12
AC-7		AIR-7	SPI-8	SPI-41	PHS-7	PHS-24	SCP-7	SCP-24	PS-8	[illegible]	MDC-7	MDC-49	
AC-8		AIR-8	SPI-9	SPI-42	PHS-8	PHS-25	SCP-8	SCP-25	PS-9		MDC-8	MDC-50	
AC-9		AIR-10	SPI-10	SPI-43	PHS-9	PHS-27	SCP-9	SCP-26	PS-10		MDC-9	MDC-51	
AC-10		AIR-11	SPI-11	SPI-44	PHS-10	PHS-28	SCP-10	SCP-30	PS-11		MDC-10	MDC-52	
AC-11		AIR-14	SPI-12	SPI-45	PHS-11	PHS-29	SCP-11	SCP-32	PS-12		MDC-11	MDC-59	
AC-12		AIR-19	SPI-13	SPI-46	PHS-12	PHS-30	SCP-12		PS-14		MDC-12	MDC-62	
AC-23		AIR-20	SPI-14	SPI-47	PHS-13	PHS-31	SCP-13				MDC-13	MDC-64	
AC-26		AIR-23	SPI-15	SPI-48	PHS-14	PHS-37	SCP-14				MDC-14	MDC-68	
AC-29		AIR-24	SPI-16	SPI-49	PHS-15		SCP-15				MDC-15	MDC-71	
AC-30		AIR-25	SPI-17	SPI-50	PHS-16		SCP-16				MDC-16	MDC-72	
			SPI-18	SPI-51	PHS-17		SCP-17				MDC-17	MDC-73	
			SPI-19	SPI-52							MDC-18	MDC-74	
			SPI-20	SPI-53							MDC-19	MDC-77	
			SPI-21	SPI-54							MDC-20	MDC-79	

The requirements in the framework include a comprehensive mapping of those established under Office of Management and Budget (OMB) A-130, and the National Institute of Standards and Technology (NIST). The RMF is maintained and updated to reflect changes in requirements (e.g. the adoption of NIST SP800-53 Revision 4), as well as any domain related requirements (e.g. HIPAA/HITECH requirements). This is important in order to ensure services and materials conform to Federal guidelines for efficient and consistent resource management. If WV PEIA desires, SRS can utilize our RMF as a tool for expediting analysis of technical risks and as the basis for submitting periodic risk reports of the constituent organizations being assessed.

18. Describe in detail how your product or service would meet and/or provide the following expected deliverables:

i. Copies of collected notes, raw data, and raw logs collected during the course of the assessment:

The SRS team will keep copies of all completed checklists, interview notes, and raw data created or obtained during the assessment. Blank notepads will be issued to each consultant at the beginning of the engagement, which will be used exclusively for the purposes of the assessment. All notes will include a record of the date, consultant, and context of the notes (e.g. interview details, physical walk-through etc). All information will be retained by SRS and returned to WVPEIA upon request.

Electronic information created or collected (e.g. checklists, draft reports, screen-captures, photographs, scan results, etc) will all be indexed, stored on secure media (e.g. encrypted laptop) with an exact retrievable copy also stored in encrypted form in a remote location. SRS will ensure backups are created daily and stored offsite weekly.

ii. Summary of discovery findings and business impact.

During the on-site assessment activities, SRS staff will meet at the conclusion of each day's activities to ensure that notes are consolidated, recorded, archived and discussed. The discussion will include the capture of key findings into a summary findings log. Each finding will have a preliminary impact assessment determination. The impact determination includes potential outcome (e.g. loss/destruction, disclosure, interruption, modification) and potential impact in each of the following categories: Life/Health, Fines, Financial, Productivity, and Reputation/Customer Confidence. All actual instances (or perceived instances) of unauthorized disclosure will be immediately escalated for discussion with the Government representative so that follow-up action can be immediately initiated. High impact risks will also be discussed each week, but the analysis team will also have the option of immediate escalation if the risk is deemed imminent. Findings and impacts will be recorded in a risk register and reported in a weekly status report (or as otherwise directed by the customer).

iii. Recommendations for addressing data flow and network usage security issues.

As described above, any data security issues that may have resulted in an actual security breach will be immediately escalated. Other technical security issues will be addressed according to severity (e.g. low likelihood of exploitation through to high likelihood) and ease of implementation (easy to exploit vs complex). Based on these considerations (and others as appropriate, such as exploits that can result in elevated privileged access vs service interruption), SRS will recommend immediate actions to mitigate the exposure, as well as medium to long term actions to address root cause and ensure the underlying processes that resulted in the vulnerability are addressed. Examples include employee training, network architecture changes, etc.

iv. Summary of an organizations monitoring and response program and its effectiveness on outside sources.

SRS utilizes multiple methods for testing, evaluating and measuring incident response procedures. The methods are tiered, and are mutually supportive. The first tier is to review the organizations' policies and procedures for incident response, continuity of operations, disaster recovery, and IT contingency planning (including backup procedures). The SRS team is extremely adept at evaluating all facets of this domain. For example, for the last four years, SRS has been leading the Navy Medicine's IT contingency planning team which has developed and tested contingency plans for 29 Covered Entities throughout the US and overseas. Incident response procedures must contain the mandatory requirements for breach notification determination and reporting as described in the Omnibus updates to the HIPAA Security Rule and Breach Notification Rules. Additional tiers include verification of staff members roles and responsibilities with respect to execution of the plan, and the related test, training and exercise of the plans. SRS also uses the technical assessment portion of the Risk Assessment to verify the client's technical staff are able to correctly observe intrusion attempts from internal network sources and external network sources. Collectively, these items will provide a thorough assessment of the response capabilities of the client organization.

v. A risk rating of existing vulnerabilities and exploits.

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®) schema to baseline initial risk rankings. In the past, the default risk ratings for scanning tools were often times incorrect or inappropriate for the environment. Although things have improved, the SRS team still 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 medical device in a segmented VLAN with network traffic restricted to "outbound only").

vi. Summary of security measures in place and their effectiveness in securing the network and minimizing intrusions and vulnerabilities.

The SRS methodology includes a thorough review of the mandatory policies and procedures specified in the HIPAA Security Rule. These policies and procedures, in turn, should address the security measures in place to protect the Covered Entity. SRS uses its own test procedures and checklists to measure completeness and effectiveness of the security controls. For example, the security rule requires unique identifiers for user accounts. SRS uses Hyena as a tool to quickly query a list of usernames from domain controllers and active directory servers. This is done by groups, beginning with administrator accounts and then moving to other user roles with elevated privileges. The SRS team reviews the query results for obvious violations (e.g. shared user accounts such as TRAINER, ADMIN, TEST etc). The next step is to review correct and appropriate implementation of password policies for all user roles (except system service accounts such as SQL process accounts). The technical validation and review of all aspects of the security rule requirements are evaluated using tools and manual methods. Results are captured on a high level score-card and mapped to the security rule. Supporting detailed artifacts are of course also retained.

vii. Identification of network security best practices and identify needed technology, policies, etc. to provide a secure environment. Please include a detailed description of how the "real world" environment compares to adopted policies and/or procedures. Simply put, describe what is being done versus what is supposed to be occurring.

The SRS HIPAA Security Assessment methodology incorporates a comprehensive Gap Analysis of the Security Rule requirements against the current implementation. Beginning with the requirements for Security Management Processes under §164.308(a)(1), which includes Risk Analysis and Risk Management, our team conducts a comprehensive review to determine:

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

These three items - which may include technical procedures - will address those items minimally required under the regulation. 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 deliverables. Any additional recommendations emerging from threats identified during the risk analysis will be prioritized according to likelihood and impact, and included in the recommendations accordingly.

viii. Details on all client systems connected to the networks that are discovered in the course of the engagement, including all information discovered about those systems (i.e. operating system, available services, interfaces, portals/links, version information, etc.).

The network discovery process summarized in our response to item #12 will be used to identify all systems within the network. 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 ePHI. 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).

ix. Recommendations for enhancements in regards to overcome potential physical vulnerabilities.
Physical security reviews will be conducted for all three primary facilities listed in the RFP, and for select satellite/remote facilities as needed. SRS will utilize its physical security checklist for the evaluation, which contains all of the physical security requirements as specified in the HIPAA security rule, as well as best practices for physical security as described in the physical security section of NIST SP800-53 revision 4. Table 10, below, contains an excerpt of a physical security assessment checklist that constitutes the basis of our plan to assess the physical facilities determined in the RFP and project kick-off meeting to be in-scope for the assessment.

Table 10: Sample Physical Security Assessment Plan Checklist

CFR Part	CFR Subpart	Standard/Specification
§ 164.310 Physical safeguards.		
164.310		A covered entity must, in accordance with § 164.306:
164.310	a.1	**(a)(1) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.**
		Do policies and procedures exist regarding access to and use of facilities and equipment?
		Are employees aware of and familiar with the policies and procedures?
		Are the policies and procedures complete, appropriate, and fully implemented?
164.310	a.2	(2) *Implementation specifications:*
164.310	a.2.i	**(i) *Contingency operations* (Addressable).** Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
		Is there a contingency plan in place?
		Is it complete, appropriate, and fully implemented?
		Has it been reviewed within the last 12 months?
		Has it been tested within the last 12 months?
164.310	a.2.ii	**(ii) *Facility security plan* (Addressable).** Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
		Is there a documented physical security plan available?
		Is it complete, appropriate, and fully implemented?
		Are there appropriate measures to provide physical security protection for ePHI?
		Are workstations protected from public access or viewing?
		Are entrances and exits that lead to locations with ePHI secured?
		Do normal physical protections exist? (Locks on doors, windows, etc., and other means of preventing unauthorized access.)
		Are there current procedures for securing the facilities (exterior, interior, equipment, access controls, maintenance records, etc.?
		Are the following physical protection mechanisms in place to help prevent, detect and recover from physical threats to computing areas (e.g. data centers)
		Fire detection system?
		Fire suppression system (halon, dry pipe etc)?
		Water sensors with alarms?

		Overhead drip pans?
		Is equipment raised 4" off floor?
		Are UPS/Surge protectors in place?
		Is an alternate power source available and tested?
		Are climate control systems in place (a/c, humidity etc) and alarmed?
164.310	a.2.iii	**(iii) *Access control and validation procedures* (Addressable).** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
		Are there written procedures to provide facility access to authorized personnel and visitors, and exclude unauthorized persons?
		Are the procedures fully implemented?
		Is physical access to data centers restricted and protected?
		Is access to controlled areas logged, monitored and/or recorded?
164.310	a.2.iv	**(iv) *Maintenance records* (Addressable).** Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).
		Do policies and procedures for controlling repairs and modifications to physical components exist?
		Are records of repairs maintained?
		Has responsibility for maintaining these records been assigned?
164.310	b	**(b) *Standard: Workstation use.* Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.**
		Are policies and procedures for the proper use and performance of each type of workstation and workstation device in place?
		Are the policies and procedures complete, appropriate, and fully implemented?
		Do policies and procedures prevent or preclude unauthorized access of unattended workstations, limit the ability of unauthorized persons to view sensitive information, and erase sensitive information as needed?
164.310	c	**(c) *Standard: Workstation security.* Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.**
		Are any workstations in areas that are more vulnerable to unauthorized use, theft or viewing of the data they contain?
164.310	d.1	**(d)(1) *Standard: Device and media controls.* Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.**
		Do policies and procedures already exist regarding device and media controls?
		Are the policies and procedures complete, appropriate, and fully implemented?
164.310	d.2	(2) *Implementation specifications:*
164.310	d.2.i	**(i) *Disposal* (Required).** Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
		Is there a process for destroying data prior to disposal or repurposing of equipment?
164.310	d.2.ii	**(ii) *Media re-use* (Required).** Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
		Do policies and procedures already exist regarding reuse of electronic media (hardware and software)?

		Are the policies and procedures complete, appropriate, and fully implemented?
164.310	d.2.iii	**(iii) *Accountability* (Addressable).** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
		Do procedures exist regarding tracking of hardware and software within the company?
		Are the procedures complete, appropriate, and fully implemented?
164.310	d.2.iv	**(iv) *Data backup and storage* (Addressable).** Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.
		Are backup files maintained offsite to assure data availability in the event data is lost while transporting or moving electronic media containing ePHI?
		Does the organization take steps to ensure that an exact, retrievable copy of the data is retained and protected before movement of equipment?

This review also includes relevant administrative requirements of the security rule which have applicability to restricted areas (e.g. visitor control for server room environments). SRS will provide recommendations to reduce the potential impact of any identified risks. Examples include recommendations for better placement of physical security surveillance cameras and motion detectors, placement of drip-pans over server racks, and review of capability and readiness of any UPS/alternate power sources.

x. Recommendations for heightened awareness and additional training.

The complete set of WV PEIA HIPAA Security Training materials will be reviewed for completeness, relevance, and overall quality as it pertains to the HIPAA Security Program. SRS has a long track record of providing high quality training on HIPAA security and general protection of ePHI. For example, the Program Manager proposed under this effort was the lead instructor for the SEI/CMU OCTAVE Risk Assessment training deliveries at SEI/CERT, and Dr. Ronald Krutz was the lead instructor for the (ISC)2 CISSP Security Review seminars. In addition to the training materials, SRS will review the security awareness policies and procedures and assess the effectiveness of the security program by conducting spot-checks with employees throughout the engagement. SRS will document all findings and provide appropriate recommendations. Examples may include the development of an awareness schedule with bi-monthly factoids, splash pages with security bullet points on the intranet login site, security reminders added in the notes section on employee paystubs, etc.

xi. A detailing of all security findings and existing vulnerabilities to include a detailed analysis of the vulnerabilities, potential risk they present to the systems and the network, and regulatory compliance, documenting of the date, time, systems accessed, and the methodology utilized to do so.

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.

xii. A prioritized list of vulnerability mitigation recommendations rated from high to low.

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.

xiii. Identification of network strengths and areas of improvement and where appropriate correlated with affected regulations.

SRS will be sure to highlight areas of excellence and recommend that effective security practices be leveraged to strengthen weaker areas as appropriate. The HIPAA Security Rule Gap Analysis will be used as the primary benchmark for establishing compliance, however full traceability will be maintained to specific regulatory sections and subsections to those specific areas of regulation can be pinpointed. This may include other pertinent regulations, such as Title 38, Section 7332, USC, 42 CFR Part 2, or the new "self-pay" rule at 45 CFR Part 164.522(a)(1)(iv).

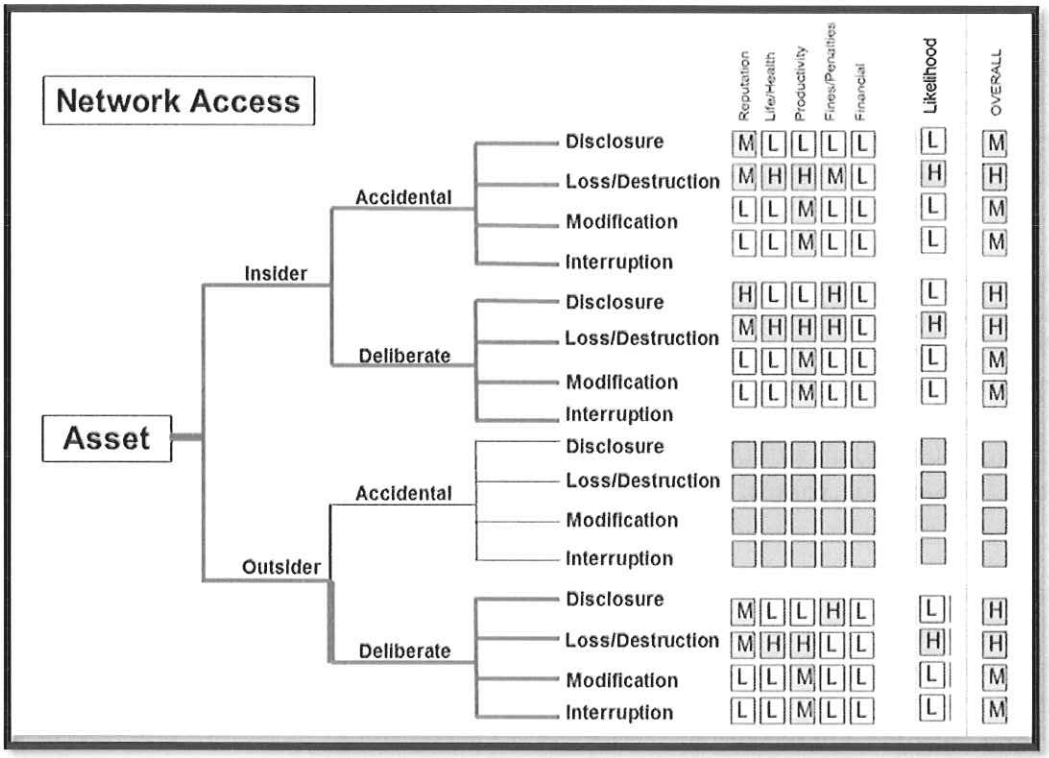
xiv. Upon completion of the discovery and testing activities, develop cost analysis for mitigation steps to improve security. The cost analysis should be categorized into a risk versus benefit format that addresses likelihood of threat and/or vulnerability and potential consequences should that threat and/or vulnerability be exploited either accidentally or maliciously.

As described in our response to item #16, a critical part of the Risk Assessment activity is mitigation planning. In order to help conduct a risk/benefit analysis, SRS will work with WV PEIA to validate a Risk Evaluation Criteria. The criteria contain thresholds for "High", "Medium", and "Low" impact in the categories of:

- Life/Health/Safety.
- Fines/Legal Penalties.
- Other Financial Considerations.
- Productivity.
- Reputation / Customer Confidence.

All risks are evaluated against the criteria, and threat trees are used to model the potential impact of each identified threat using a values scoring system. This allows the truly "high" impact threats to be readily prioritized, where the cost analysis is more readily apparent and can truly be used to influence business decisions regarding selection of potentially costly mitigation strategies. An example of a threat tree showing impact ratings for each threat (represented by a leaf node on the tree) is included in Figure 7. It should be noted that threat trees are an aid to threat modeling and impact analysis for helping conduct cost/benefit analysis. Each node on the threat tree is mapped to one or more discreet threats, which for clarity are not included in the diagram.

Figure 7: Example Threat Profile with Impact Analysis



			Reputation	Life/Health	Productivity	Fines/Penalties	Financial	Likelihood	OVERALL
Insider	Accidental	Disclosure	M	L	L	L	L	L	M
		Loss/Destruction	M	H	H	M	L	H	H
		Modification	L	L	M	L	L	L	M
		Interruption	L	L	M	L	L	L	M
	Deliberate	Disclosure	H	L	L	H	L	L	H
		Loss/Destruction	M	H	H	H	L	H	H
		Modification	L	L	M	L	L	L	M
		Interruption	L	L	M	L	L	L	M
Outsider	Accidental	Disclosure							
		Loss/Destruction							
		Modification							
		Interruption							
	Deliberate	Disclosure	M	L	L	H	L	L	H
		Loss/Destruction	M	H	H	L	L	H	H
		Modification	L	L	M	L	L	L	M
		Interruption	L	L	M	L	L	L	M

xv. A clearly defined scope of what system(s) are being assessed.

Prior to any assessment, SRS clearly establishes rules of the road and confirms expectations for what is in scope of the assessment, and what is out of scope. For example, clients may wish to scope out of the assessment those systems which are exempt from HIPAA (e.g. Workers Compensation systems interfacing with occupational health systems) or may wish to include additional systems not having a direct bearing on ePHI, but important to the overall security posture of the organization (e.g. payment card data for credit card processing systems). Scope statements and system boundaries are discussed in the project kick-off meeting. Additionally, immediately prior to any technical security testing on the network, SRS facilitates a deep-dive review of the network architecture with the systems administrators/architects to ensure SRS is cognizant of any additional considerations which should be addressed prior to testing. Examples include legacy systems or clinical systems on the network which may no longer be supported by the vendor, but for cost reasons have not yet been upgraded or replaced by the covered entity. Extra precautions are always taken prior to assessing legacy systems or systems which may have a bearing on health/safety (e.g. fetal monitoring systems in a maternity ward).

xvi. Policy and Procedure Review of all parties that have access to protected and/or critical information.

In addition to a 100% review of policies and procedures in place for the Covered Entity being assessed, SRS will support the collection of assertions from Business Associates and individual employees, consultants, and other third parties who may have access to sensitive information. SRS will catalogue and inventory all such third parties.

xvii. Active Social Engineering.

SRS will confirm during the kick-off meeting whether active social engineering is a permitted attack vector during the testing phase. If it is, SRS will employ a variety of methods to demonstrate typical social engineering techniques and at the same time test the resiliency of staff members to those techniques. Good practices will be documented, as well as areas for improvement and any associated specific recommendations (such as updates to security training materials or a social-engineer awareness campaign). In the past, SRS has even used social engineering techniques to gain physical access to server room locations and other restricted areas within a facility.

xviii. Third Party Oversight Review - contractors, Business Associates, vendors, etc.

An important part of the Gap Analysis and risk assessment is documenting who has access to protected information, and how they in turn protect it. SRS will include these areas in the third party interviews of Business Associates and Subcontractors.

xix. System Inventory and Documentation Collection.

As previously described, our technical approach includes a detailed network discovery phase. As part of the documentation resulting from that activity, SRS will work with the CE staff to determine exactly which systems do (or may) contain protected health information. This then becomes in effect an inventory of systems containing ePHI, which is useful in determining where additional security and privacy controls may have the greatest impact.

xx. Physical/Environmental Security Review including physical access/egress points, access permission(s) process(s), etc.

Our response to item (ix) in this question describes some of the aspects of the physical security review SRS conducts during on-site risk assessments. A summary of past performance projects Covered Entities is also shown in Table 2. All aspects of the physical security requirements of the HIPAA Security Rule will be addressed, including a review of the Facility Security Plan and any administrative or operational safeguards (such as visitor control or employee training) which may have an impact on security. As previously described, security enhancements above and beyond those required in the security rule will be included and noted as enhancements. Sources for enhancements include NIST SP800-53r4, physical security controls for systems categorized at the FIPS 99 level of moderate (typically considered the baseline for healthcare systems).

xxi. Agency Personnel and IT Staff Training and Awareness Review.

Completeness, relevance, and validity of all security awareness and training policies, procedures and training materials will be evaluated. As described earlier in this proposal, SRS staff are proud to have an impressive cadre of recognized HIPAA security professionals who are also highly experienced educators in HIPAA Security. SRS staff have trained over 200 HIPAA security officials throughout the DoD healthcare System, close to 300 providers as part of the Alabama Meaningful Use Regional Extension Center program, and many more through regular course deliveries hosted by the SEI at CMU, but delivered by SRS personnel as part of the SEI Visiting Scientist program. SRS will spot check understanding and compliance with randomly selected employees, and will review the training records to assess the percentage of the workforce who have completed HIPAA Security Training within the preceding 12 months.

xxii. Internal Vulnerability Assessment.

Full details of the internal vulnerability assessment have been addressed throughout the previous section of this proposal. Rest assured, the assessment will include a full analysis of the entities' compliance with the HIPAA Security Rule, with best practices for Information Security (per NIST guidelines), and will include a fully comprehensive internal vulnerability assessment. The assessment will include the previously described steps for discovery and host enumeration, credentialed scans using NESSUS and Retina tools, manual checks using system administrator support tools such as Hyena, as well as manual methods performed by our certified consultants. Examples of technical findings are included in the Appendix H . Results will be verified, categorized according to vulnerability severity, and grouped by host type if applicable. Additional manual tests will be conducted to review firewall rules, router configurations, and defense in depth considerations (such as correct placement of components in DMZ, effective use of VLANs, appropriate wireless security, etc).

xxiii. Assessment of telephone system and recorded call security.
SRS has conducted active security testing on various phone systems and conference bridge systems, such as Cisco Unified Meeting Place. SRS will leverage their experience in testing these systems to help with the overall security posture of the network, as well as its potential means for facilitating phishing attempts (e.g. directory listings and voice playback features to anonymous callers) and the potential for phone fraud through techniques such as trunk-to-trunk bridging by outside callers.

xxiv. Host/Server/Network Analysis.
Included in the internal vulnerability assessment is a thorough host/server/network analysis. For servers, 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 often found in clinical systems on networks in treatment facilities (e.g. radiology systems). SRS will also conduct a comprehensive search for unlicensed software, and for home-grown data repositories which may contain unsecured PHI.

xxv. Network and website penetration and intrusion testing.
Detailed methods for conducting internet facing system testing, or "external" penetration tests are included in our response to section #14. Please refer to that response for details on the methodology and expected outcomes.

xxvi. Access Control Review for employee's contractors and business associates.
In addition to the logical access control review described in subsection VI to this question, SRS will review policies and procedures in place for authorizing individual access to the protected information. This review will not only address authorization procedures, but also revocation procedures for individuals upon termination or transfer, period audit/review of access privileges, and verification of "need to know" and completion of appropriate training prior to access being granted.

19. Please provide a specific description of the Vendor's Products and Services. The response should address the following:

i. Detailed description of proposed solution/services.
Details regarding the products and services offered by SRS are included in response to question #4 in this proposal, and is explained in detail throughout the individual responses to questions in this proposal. Conducting HIPAA Security Risk Assessments is among our core business offerings. SRS is a Security Risk Management firm with a specific focus in healthcare regulatory compliance. We have substantial experience and credibility in performing these services. SRS uses a tailored methodology to conduct the assessment, as described earlier in this proposal. The assessment methodology is based on NIST Special Publication 800-30, mapped to the eight step risk assessment process described by ONC

and CMS, and leverage threat modeling techniques from additional methods such as OCTAVE from the SEI/CERT at CMU. The technical approach includes a full HIPAA Security Gap Analysis (all policies, procedures, HIPAA documentation requirements, and analysis of technical, physical, and administrative controls). It incorporates an internal network vulnerability assessment, which incorporates a full network discovery, network mapping activity, 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 leverages techniques from penetration testing to identify 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 any HIPAA compliance gaps in the "compliance roadmap" final report and presentation. Additionally, SRS will conduct threat identification and mitigation planning as part of the HIPAA Risk Management process. Resulting threats will be prioritized according to impact, and mitigation strategies prioritized along with a cost/benefit determination. All aspects of the engagement will address interfaces with third parties, and will encompass all aspects of the WV PEIA Offices and systems, WV CHIP Offices and systems, and WV Office of Technology Offices.

ii. Known vulnerabilities and solutions.

Known vulnerabilities are discovered during the internal technical assessment. Non–technical vulnerabilities are discovered during the detailed review of the Physical, Administrative and Documentation requirements. Solutions to identified known vulnerabilities are categorized according to impact, and mitigation strategies are suggested in terms of cost/benefit analysis. Mitigation approaches and technical solutions are recommended based on Industry best practices from NIST and ISO, and technical resources from MITRE (CVE database), and of course the real world experience our team brings to the table.

iii. Tools that the vendor will be using.

Our staff are trained and experienced in the use of a variety of tools used to support security testing and evaluation activities, although it should be noted that our services rely more on the tenure and expertise of the consulting staff rather than the tools employed. However, assessment tools can provide an effective perspective, albeit an incomplete one. SRS uses a combination of commercial and open-source freeware assessment tools to support these activities, some of which are included in Table 11 below:

Table 11: Examples of Scanning Tools Used by SRS

General Assessment Tools	Password Cracking Tools	General Web Application Assessment Tools
Retina	Crack	WebInspect
Nessus Professional Feed	Rainbow Crack	ISS SQL Injection Testing Suite
NMAP	L0phtcrack	SpikeProxy
Whisker	Brutus	Metasploit

iv. Methodology of non-software based vulnerability assessments, e.g., site inspections, intrusion testing, social engineering, etc.

Our response to this question has been addressed in detail throughout the proposal. The non-software based methodology includes knowledge elicitation interviews, physical walk-though inspections, manual reviews of technical items (such as network topology review for defense in depth), manual review of policies and procedures (including those required by HIPAA), manual spot-checks to assess compliance and understanding, and other techniques to ensure a fully comprehensive, repeatable and defendable process is utilized and well documented.

v. Minimum information that vendor will need to get started.

The minimum information needed to get started is discussed in the response to Question #11: "Please describe your approach to initial engagement with the customer and what expectations you have of the customer in order to begin work on the project". A document request list will be provided to the customer detailing specific items. Examples include any existing HIPAA Security Policies and Procedures, designated Points of Contact from each participating department/agency, and support in the scheduling of a project kick-off meeting.

vi. Description of your Quality Control process.

SRS believes that quality should be built in and managed continuously. It is the responsibility of the SRS Program Manager to ensure that adequate quality control processes are institutionalized in each subtask throughout the project. SRS applies a clearly defined quality control methodology, which has been refined as the result of years of experience, to ensure the following:

- Compliance with applicable regulatory requirements.
- Factual and typographical accuracy.
- Delivery in a timely fashion to meet both internal and external deadlines, and to allow adequate cycles for review and revision.
- Reflection of government or other stakeholder input and/or approval prior to release or dissemination.
- Development and adherence to all Quality Assurance Surveillance Plans (QASPs).

As described in our response to Question #21, SRS will create a Contract Deliverable Requirements List, which will specify each of the deliverables and the timeline, format, and any other constraints regarding delivery (e.g. verbal briefings, written reports etc). SRS will develop and use a Quality Assurance Surveillance Plan (QASP) to specify the acceptable and expected standard for each one of the deliverables. SRS will include the CDRL and QASP as integral components of the project plan and management process. Sufficient time for customer review of draft deliverables will be included, and customer input to the iterative development of deliverables will be apparent throughout the engagement.

vii. Project plan including timelines.

Our response to question 11 includes a detailed description of how the project plan will be developed. Unless otherwise requested by the customer, MS Word and MS Project will be used to document the detailed work plan, WBS structure, and resource allocation. The detailed plan will be delivered within ten (10) working days of the post-award meeting. The work plan will explicitly identify any critical dependencies between tasks, on external parties, or on the Government.

A high level timeline is shown in Table 12 below, however this is not based on discussions with the customer and should be considered a notional draft. Customer input is required to confirm expectations, timelines and resources. Timelines may need to be adjusted, depending on the customers' desires and expectations (e.g. execution of completely separate assessments for the WV Office of Technology, WV PEIA and WV CHI, or combining certain aspects of the assessments in order to realize potential efficiencies).

Furthermore, certain steps included in the timeline below may need to be repeated to address different facilities and technical infrastructure for the different State Agency departments in scope for the assessment. Wherever possible, efficiencies will be implemented to minimize duplication of effort, but in some cases (e.g. physical inspections) this may not be possible.

Table 12: DRAFT Project Timeline

Timeline (weeks)	Contract Milestone	HIGH-LEVEL ACTIVITY (DRAFT – subject to changed based on discussions with customer)
0-4		PLANNING PHASE
0	◆	**Contract Award**
		Validate compliance with WV licensing/business registrations all complete.
		Fully execute subcontracts and other legal documents.
		Conduct internal team planning meeting with subcontractor team members.
		Prepare customer kick-off meeting materials and schedule meeting.
		Confirm staffing plan, assign team resources.
2	◆	**Submit document request to customer**
3	◆	**Customer Kick-off Meeting**
		Includes scheduling on-site activities and verification of appropriate test windows.
4	◆	**Deliver Project Work Plan**
5-13		DISCOVERY PHASE – NON TECHNICAL
		Review of HIPAA Security policies and procedure to determine if they are complete and appropriately implemented. Initiate development of Gap Analysis based on documentation provided to SRS.
10	◆	**Complete Initial Document Review**
		Provide comments/ additional information requests to customer
11	◆	**Initiate Risk Analysis and Part of Risk Management Process**
		Confirm scope of risk analysis activity within the overall HIPAA Risk Assessment Engagement
		Data gathering: knowledge elicitation interviews, discovery, critical asset determination, network topology discussion, etc. Include input from all departments/agencies in scope for the assessment.
		Identify and document potential threats and organizational vulnerabilities – based on organizational security posture, policies and procedures required under the HIPAA Security Rule and other relevant regulatory requirements.
13-24		TECHNICAL ASSESSMENT
13	◆	**Technical Assessment Kick-off Meeting**
		Facilitate a deep dive discussion with representatives to address technology scope, testing windows, review test procedures etc prior to conducting any testing

13	◆	**Internal Technical Assessment**
		Identify and document potential threats and vulnerabilities from inside: Includes scanning, network discovery, topology diagram development and validation, vulnerability identification, spot checks, manual audits, defense in depth topology review, configuration checks, wireless assessment, ePHI inventory etc.
18	◆	**External Technical Assessment**
		Identify and document potential threats and vulnerabilities from outside: Includes identification of external interfaces, all ports/protocols/services providing potential entry points, traffic analysis/sniffing of data crossing interfaces to assess for potential data leakage or exposure, intrusion attempts etc.
24	◆	**Present interim/draft findings to customer**
24-26	PHYSICAL ASSESSMENT	
24	◆	**Physical Assessment Walk-throughs**
		Assess current security physical security measures. Techniques Include social engineering, server room review, compliance with HIPAA Security Policies and procedures, spot checks for physical security, gate access, visitor processes etc.
		Prepare documentation to consolidate initial findings.
26	◆	**Present interim/draft findings to customer**
27-42	DOCUMENTATION PREPARATION AND ANALYSIS	
		Validate findings, consolidate documentation, remove false positives etc.
		Assess adequacy of current security measures and develop risk evaluation criteria.
		Conduct iterative meetings, updates and validation sessions with customer representatives and stakeholders throughout.
		Determine the likelihood of threat occurrence for identified concerns.
		Conduct threat tree analysis to determine the potential impact of threat occurrence, and document findings.
		Determine the level of risk and document.
39	◆	**Present interim/draft findings to customers.**
	MITIGATION PLANNING	
		Develop prioritized list of recommendations – constituting a "compliance roadmap".
		Prepare resource estimates for each mitigation strategy.
42	◆	**Present findings to customers and stakeholders.**
43-52	FINAL REPORT AND PRESENTATION	
		Prepare documentation.
		Provide drafts to customer for review and validation.
		Conduct quality review, using CDRL and QASP to ensure acceptance.
		Update document based on customer feedback.
50	◆	**Present final report and out-brief presentation.**
52	◆	**Contract close-out and return of data to customer.**
1-52	ONGOING PROGRAM MANAGEMENT ACTIVITIES	
Weekly		Weekly status reports and coordination meetings with subcontractors.
Monthly	◆	**Monthly progress reports to customer.**
Monthly		**Monthly financial reports to customer.**

Ongoing	◆	**Program risk management activities, including development of risk and issues register to manage risks associated with delivery of services described in RFP.**
Ongoing		Quality assurance surveillance activities
Ongoing		Implementation of strong fiscal controls and maintenance for full financial responsibilities.
Quarterly	◆	**Periodic formal in-progress reviews with customer**

20. Please describe and differentiate how your product(s) and/or services differ from those of your competitors. Please include any and/or all information about cost effectiveness of service(s); willingness to indemnify the State of West Virginia from subsequent compliance action(s); benefits brought to previous customers, etc. Be as specific as possible.

SRS services differ from those of our competitors in terms of:

- Subject matter expertise (we have Internationally and Federally recognized security and privacy experts).
- Over 10 years of working together (even prior to the formation of SRS) in conducting HIPAA Security Risk Assessments, which gives us unparalleled experience in threat analysis and development of mitigation strategies.
- Real-world experience with first-hand understanding of what it really takes to "get this done right". While we have fine-tuned assessment approaches and leverage a variety of tools and techniques to achieve efficiencies, we never short-cut the process which ultimately provides the organization with an improved security posture along with documented and defendable due-diligence.

Please see our earlier response to Question 17 for additional examples of our differentiators and benefits.

21. The vendor must demonstrate how their security analysis product(s) or service(s) will address all of the deliverables listed in item 18 of this Attachment. Please describe how you, as a vendor, will assess the aforementioned.

SRS will create a Contract Deliverable Requirements List, which will specify each of the deliverables and the timeline, format, and any other constraints regarding delivery (e.g. verbal briefings, written reports etc). Additionally, SRS will develop and use a Quality Assurance Surveillance Plan (QASP) to specify the acceptable and expected standard for each one of the deliverables. SRS will include the CDRL and QASP as integral components of the project plan and management process.

22. The vendor must work with / coordinate work with The State of West Virginia Office of Technology (WVOT) and agency staff that will provide Oversight Review to include collaboration with Information Services leadership of the WVOT, and key representatives at participating agencies to assess the risk of each vulnerability, and prioritize, as appropriate. Please describe how you, as a vendor, will facilitate and accomplish this collaboration.

SRS is well versed in collaborative techniques for consensus building and cross-coordination among multiple stakeholders in a non-confrontational manner. We facilitate collaborative outreach communication calls with potential stakeholders to keep them apprised of activities and to solicit their input and engagement as appropriate. Examples of coordination activities we use in a variety of cross-stakeholder environments include:

- Informational webinars on the project.
- Leadership/Executive outreach briefings.
- Monthly progress reports.
- Regular steering committee/board level updates.
- Coordinated communication and collaborative decision making, where appropriate.
- Identification of ways for potential stakeholders to participate.

As examples of our professionalism and expertise in facilitating cross-collaboration meetings, SRS facilitated the Healthcare IT Standards Panel (HITSP) Security, Privacy and Infrastructure Technical Committee for over three years. In another example, SRS has facilitated the ONC Data Segmentation for Privacy initiative for the last 18 months. During the course of the project, SRS facilitated collaborative discussions with over 300 individuals from approximately 100 committed organizations.

23. Please provide a detailed timeline for completion of this project from beginning to end.
Please refer to Table 12, DRAFT Project Timeline, included as our response to question 19 subpart vii ("Project plan including timelines")

24. Based on the vendor's knowledge, training, and experience, what can be foreseen as potential obstacles in preventing the successful completion of this project?
SRS feels very comfortable that given the opportunity, we will be entirely successful in all aspects of this project. Potential obstacles include the possibility of a lack of consensus on the current state of practice between WV PEIA departments and partners, and also potentially resistance from third parties to cooperate in the process. SRS believes that strong communication, knowledge transfer, and stakeholder buy-in to the process can mitigate any concerns in this area.

25. Based on the vendor's knowledge, training, and experience, are there any parts of a HIPAA/HITECH Security Risk and Vulnerability Assessment that have been overlooked and/or omitted from this solicitation that you would view as important in maintaining the privacy and security of the personally identifiable information and/or protected health information collected, used, stored, and/or maintained by the State of West Virginia and/or its respective Covered Entities?
SRS suggests including a "Covered Transactions" analysis to help determine and validate precisely which workflows and interfaces are considered subject to the security and privacy protections of the HIPAA Security and Privacy rules. For example, in the case of Workers Compensation related health data, even though professional ethics require that only the minimum amount of healthcare data relating to the claim be shared, it is possible for a patient's entire medical record to be shared under this exclusion from the HIPAA rules. The information could readily end up in the hands of the employee, and the patient may have none of the legal protections required by HIPAA.

Additionally, certain types of healthcare information are considered by regulations to be more sensitive than others and are therefore afforded enhanced privacy protections beyond those availed through the HIPAA Privacy rule. Examples include 42 CFR Part 2 data (where certain uses of substance abuse and mental health data require explicit patient consent for sharing, even beyond HIPAA Treatment, Payment and Operations purposes). Other examples include cases of intimate partner violence, certain information pertaining to Veterans and VA facilities protected by Title 38, Section 7332, USC (such as sickle cell anemia and HIV data), and information concerning minors. In all of these cases, HIPAA protections may be insufficient, and additional privacy and security considerations should be identified and addressed accordingly. More recently, the "self-pay" rule [45 CFR Part 164.522(a)(1)(iv)] which became effective in March 2013 and has a compliance deadline of September 2013 institutes requirements for providers to be able to withhold information from health plans for services a patient has received and paid for in full, out of pocket.

Another consideration resulting from recent changes brought about by HIPAA/HITECH extensions and promulgated through the Omnibus Rule are the breach notification requirements. SRS recommends that WV addresses means to ensure that Business Associates -and also certain subcontractors – apply the same degree of rigor to protecting their systems and reporting breaches as is required of the Covered Entity. SRS can help the WV PEIA and associated departments develop ways to ensure the breach notification requirements are promulgated downstream appropriately, and are contractually and legally enforceable.

Attachment B: Mandatory Specifications Checklist

Section 4, Subsection 5.1: Prospective vendors agree and understand that, by submitting a bid on this RFP, they agree to and will abide by all of the General Terms and Conditions as outlined in Section 3 of this RFP document.

Vendor Response: SRS agrees and understands that , by submitting a bid on this RFP, they agree to and will abide by all of the General Terms and Conditions as outlined in Section 3 of this RFP document.

Section 4, Subsection 5.2 The vendor must submit a plan of assessment of the physical site(s) security for strengths, weaknesses, vulnerabilities, and/or risk(s).

Vendor Response: Yes. The plan of assessment of physical security is an integral part of our overall assessment methodology and plan. Please see Table 10, in section ix of response to question 18 for details of the types of activities the assessment will include. Please refer to the methodology, and timeline described in Table 12 for more details on how the physical security portion of the assessment is included within the overall HIPAA Security Assessment plan.

Section 4, Subsection 5.3 The vendor must provide a plan of assessment of the virtual environments of the Covered Entity(ies) for strengths, weaknesses, vulnerabilities, and/or risks.

Vendor Response: Yes. Please refer to the methodology, and timeline described in Table 12 for more details on how the virtual environments will be assessed as part of the overall HIPAA Security Assessment plan. Details of the specific approach for internal and external assessments, including pre-kickoff meetings and testing expectations are included throughout the proposal.

Section 4, Subsection 5.4 The vendor shall provide a plan for obtaining comprehensive documentation of the IT environment of the Covered Entity(ies) including, but not limited to: network(s), firewalls, interfaces, telephony, websites/portals, and related equipment.

Vendor Response: Yes. Plans for network discovery, testing and documentation are included in the various sections of the proposal, including the project timeline. Specifics for addressing the security of various components are included.

Section 4, Subsection 5.5 The vendor must Identify and assess access and distribution points and interfaces for security risks and/or vulnerabilities.

Vendor Response: Yes. Procedures for identifying and documenting access and interfaces are described in the external assessment portion of the assessment methodology, and throughout the proposal (e.g. interviews, spot checks, technical scans, threat identification activities during risk analysis etc).

Section 4, Subsection 5.6 The vendor shall identify internal and external security vulnerabilities (both real and potential).

Vendor Response: Yes. The Risk Analysis portion of the Risk Management Activity under the HIPAA Security Rule shall be addressed in detail, which includes identification of potential and actual threats and vulnerabilities. The entire proposal documents our approach and methods for identifying these concerns, and utilizes multiple techniques (scanning tools, interviews, spot checks, discovery etc).

Section 4, Subsection 5.7 The vendor shall identify organizational strengths that help provide security.

Vendor Response: Yes. Our proposal specifies that throughout the assessment process, strengths and areas of excellence will be documented. Where appropriate, they will be held as examples to support other suggestions for best practice and mitigation planning.

Section 4, Subsection 5.8 The vendor must conduct a comprehensive assessment of the physical and virtual environments of the covered entities.

Vendor Response: Yes. As described throughout our proposal , SRS will conduct a thorough assessment of all relevant aspects of the physical and virtual environments of the covered entities. Our proposal contains an excerpt of the physical security checklist and describes processes for internal and external testing and documentation of the virtual environments.

Section 4, Subsection 5.9 The vendor shall conduct a review of staff training, policies, procedures, practices, etc. as they relate to the human aspect of information security.

Vendor Response: Yes. Our proposal and assessment methodology includes a full review of these items. Please refer to our response to Question 18(x).

Section 4, Subsection 5.10 The vendor must prepare and provide a presentation with supporting documentation to the management of the Covered Entity(ies) about findings of the assessment(s).

Vendor Response: Yes. This is included as one of the deliverables, and incorporated in the project plan and timeline in Table 12.

Section 4, Subsection 5.11 The vendor shall provide a plan for the development of an action plan, including a cost analysis, to prioritize identified security risks and/or vulnerabilities.

Vendor Response: Yes. The proposal incorporates activities, in the project plan and timeline, for the development of a corrective action plan, or "get well" plan. Note that the risk analysis activity will result in a specific risk assessment report, which includes prioritized risks and mitigation strategies. The assessment will also include technical reports from the technical assessments, and reports regarding the completeness and effectiveness of policies and procedures required by regulation. The overall corrective action plan will include items identified in the risk analysis, and all assessment activities throughout the engagement. The plan will prioritize recommended actions according to impact, compliance, urgency, and cost/benefit analysis. This is described throughout the proposal.

Section 4, Subsection 5.12 The vendor must draft a recommended schedule for audits, system testing, and/or re-assessment.

Vendor Response: Yes. The plan of action and milestones is included in Table 12. The proposal also describes how a more detailed plan will be developed as an early deliverable, based on information learned and expectations communicated through the kick-off meeting.

Section 4, *Subsection 5.13 Prospective vendors must be able to fulfill the full scope and intent of this project. The State of West Virginia, PEIA, and WV CHIP are looking to partner with one (1) vendor who can provide the comprehensive array of services necessary for a thorough HIPAA/HITECH Security Risk and Vulnerability Assessment. The use of subcontractors to provide work on this project is permitted but there must be only one (1) primary vendor.*

Vendor Response: Yes. SRS is fully capable, experienced and qualified to conduct all aspects of this project. SRS is proposed as the primary vendor for this effort. SRS will lead, manage and be fully responsible for all aspects of project performance. The two subcontractors are included to provide additional (surge) resources in support of the technical assessment, and to engage a local (Charleston WV) presence with first-hand knowledge and long-term familiarity with the State Agencies.

Section 4, Subsection 5.14 Prospective vendors must have previous experience providing HIPAA/HITECH Security Risk and Vulnerability Assessments for at least three (3) entities of a similar size and scope as this proposed project.

Vendor Response: Yes. SRS has conducted assessments of similar size and scope, many times over. These assessments are our core business and we have been described by clients as "setting the standard" for HIPAA Security Risk Assessments.

Section 4, Subsection 5.15 Prospective vendors must sign the State of West Virginia Business Associate Agreement referenced in Section 3, #38 of this RFP. Further, vendors must ensure that the provisions of that Business Associate Agreement are clearly conveyed to any and/or all subcontractors who may work on any portion of this project.

Vendor Response: Yes. SRS has signed the BAA and included it as Appendix E to the proposal. SRS understands the importance of ensuring all information is adequately protected. All requirements of the HIPAA Security Rule that apply to Business Associates and Subcontractors will be included in the subcontract agreements with the subcontractors. Subcontractors will also be required to sign the WV Business Associate Agreement. A copy of each will be provided to WV upon request.

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

Security Risk Solutions, Inc.
(Company)

(Authorized Signature)

Johnathan Coleman, Principal
(Representative Name, Title)

(P)843.647.1556 (F)843 416 4881
(Phone Number) (Fax Number)

8th July, 2013
(Date)

Attachment D: State of West Virginia Vendor Preference Certificate

The State of West Virginia Vendor Preference Certificate is included on the next page.

Attachment D

State of West Virginia
VENDOR PREFERENCE CERTIFICATE

(See form attached)

Rev. 07/12

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 Resident Vendor Preference, if applicable.

1. **Application is made for 2.5% resident 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% resident 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% resident 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% resident 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% resident 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% resident 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:**

Date: July 8th, 2013 **Title:** Principal

Appendix A: Limited Data Use Agreement

The Limited Data Use Agreement is included on the next two pages.

APPENDIX A: LIMITED DATA USE AGREEMENT

A limited data set is a set of records containing personally identifiable information (PII and/or protected health information (PHI), from which direct identifiers may have been removed, but in which certain potentially identifying information remains. The use or disclosure of a limited data set is limited to research, public health, and health care operations purposes only.

Name of data recipient: SECURITY RISK SOLUTIONS, INC.

Description of data: **Agency** data that may be disclosed in the course of conducting the security risk/vulnerability assessment.

Purpose of use: An agency may disclose a limited data set to a vendor contractor during the course of providing a security risk/vulnerability assessment as an administrative function under provisions of the Security Rule(s) of HIPAA and/or HITECH. Said vendor will also have signed a State of West Virginia Business Associate Agreement.

By signing this agreement the recipient agrees:

- Not to further use or disclose any of the information, outside the purpose listed above, without prior written permission from the agency or as otherwise required by law;
- That any further information requested by Recipient, or its Affiliates, regarding the data and/or any reports must be made in writing to the agency.
- Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
- To notify the agency if any third party will be allowed access to the information provided as part of the performance of work under the scope of this RFP prior to that third party being granted access;
- Report to the agency use or disclosure of the information not provided for by its data use agreement, of which it becomes aware;
- Ensure that any agent, including any affiliates, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
- Not to identify the information or to contact the individuals to whom the information pertains, if applicable.
- Properly and completely dispose of any and/or all data provided by the State of West Virginia and/or its Agency(ies) upon RFP process completion.

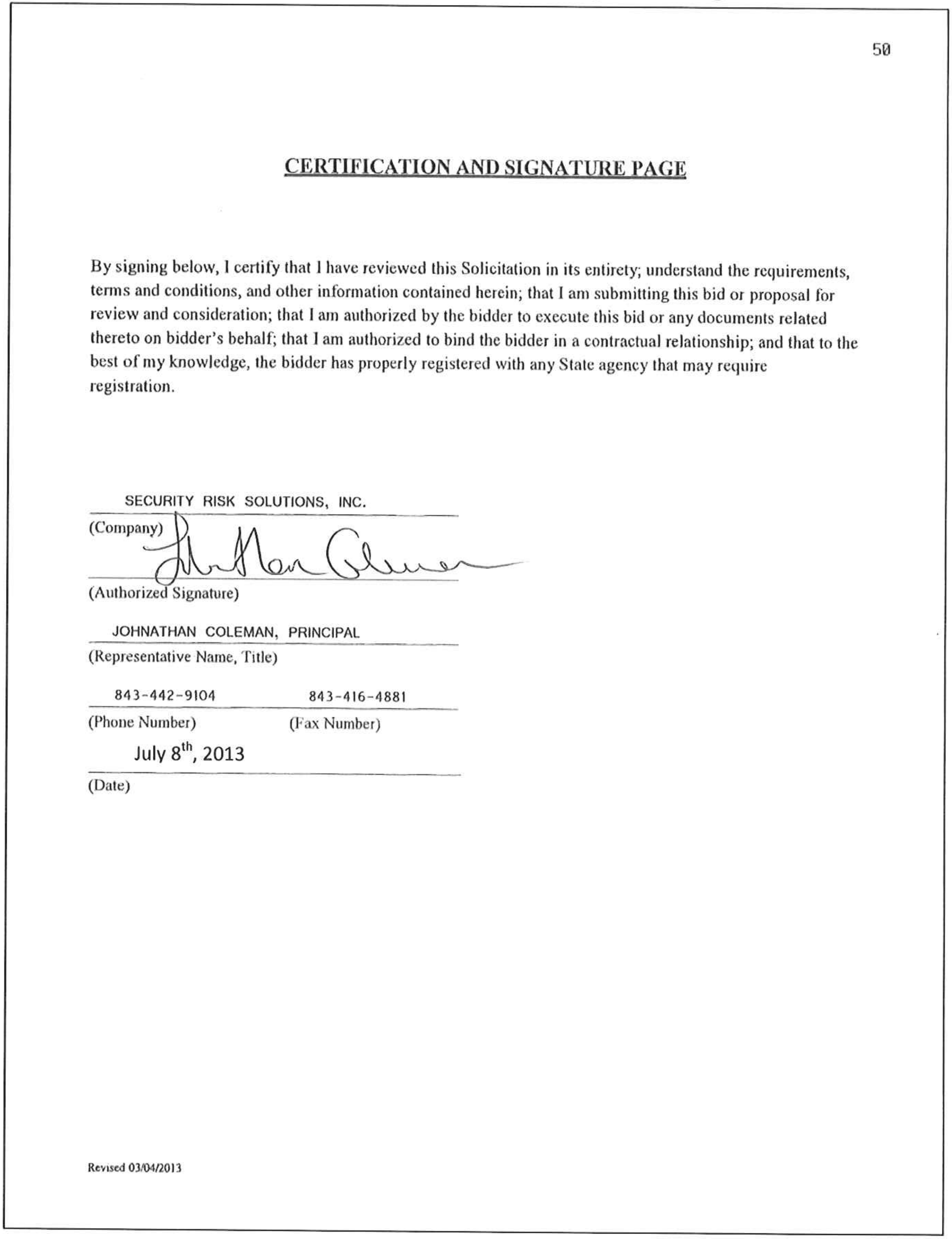
An agency may terminate the agreement if it notifies the recipient of a pattern of activity or practice that constitutes a material breach or violation of the data use agreement, or law, unless the recipient cures the breach or ends the violation within a reasonable time, as determined by an agency will take reasonable steps to cure the breach or end the violation and if such steps are unsuccessful the agency will discontinue disclosure and report the violation to the appropriate authorities.

July 8th, 2013

Signature of Vendor Representative — Date

Signature of PEIA/WV CHIP Representative — Date

Appendix B: Certification and Signature Page



CERTIFICATION AND SIGNATURE PAGE

By signing below, 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 or proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

SECURITY RISK SOLUTIONS, INC.

(Company)

(Authorized Signature)

JOHNATHAN COLEMAN, PRINCIPAL

(Representative Name, Title)

843-442-9104 843-416-4881

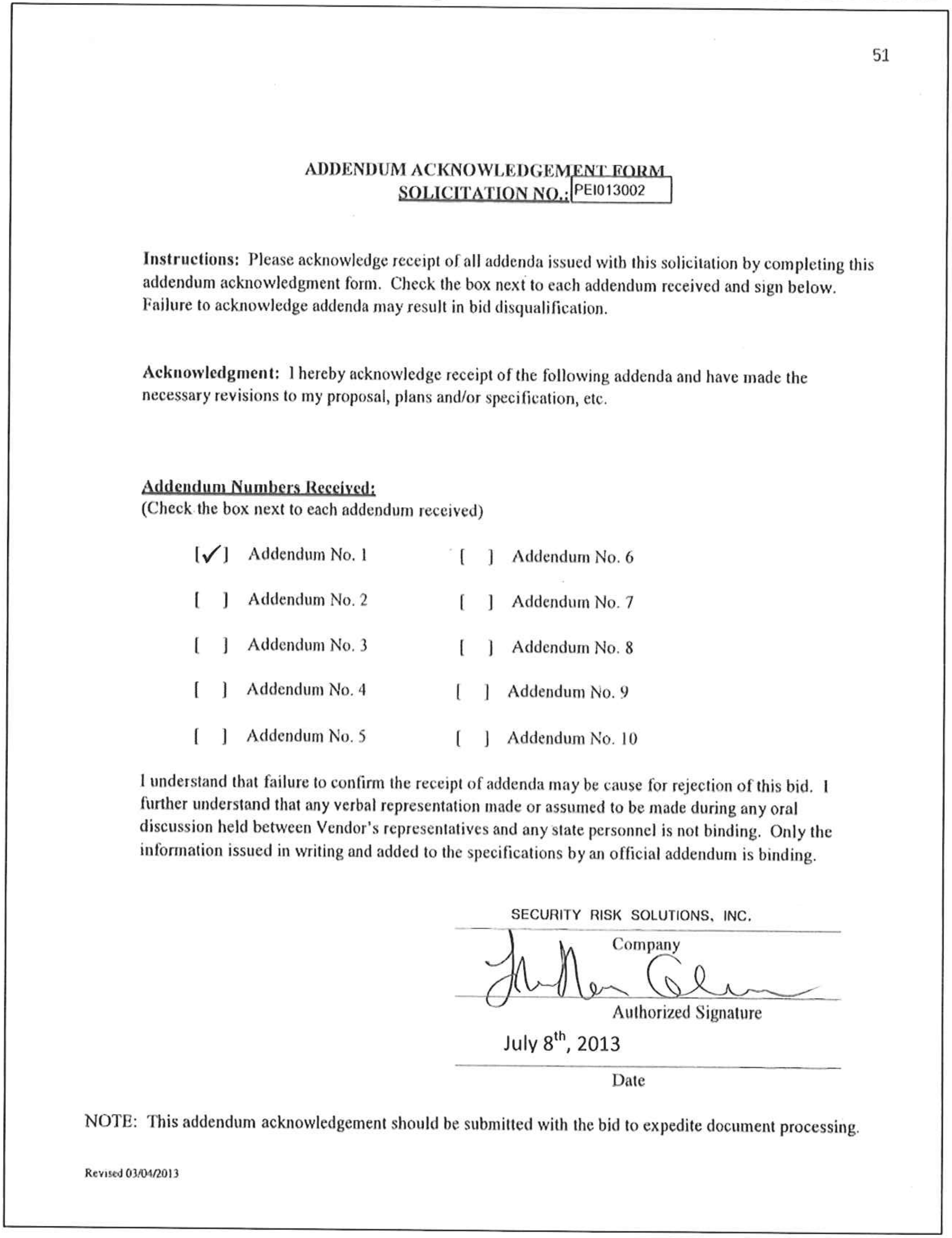
(Phone Number) (Fax Number)

July 8th, 2013

(Date)

Revised 03/04/2013

Appendix C: Addendum Acknowledgement Form - Solicitation No. PEI 013002



51

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: PEI013002

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

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

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

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

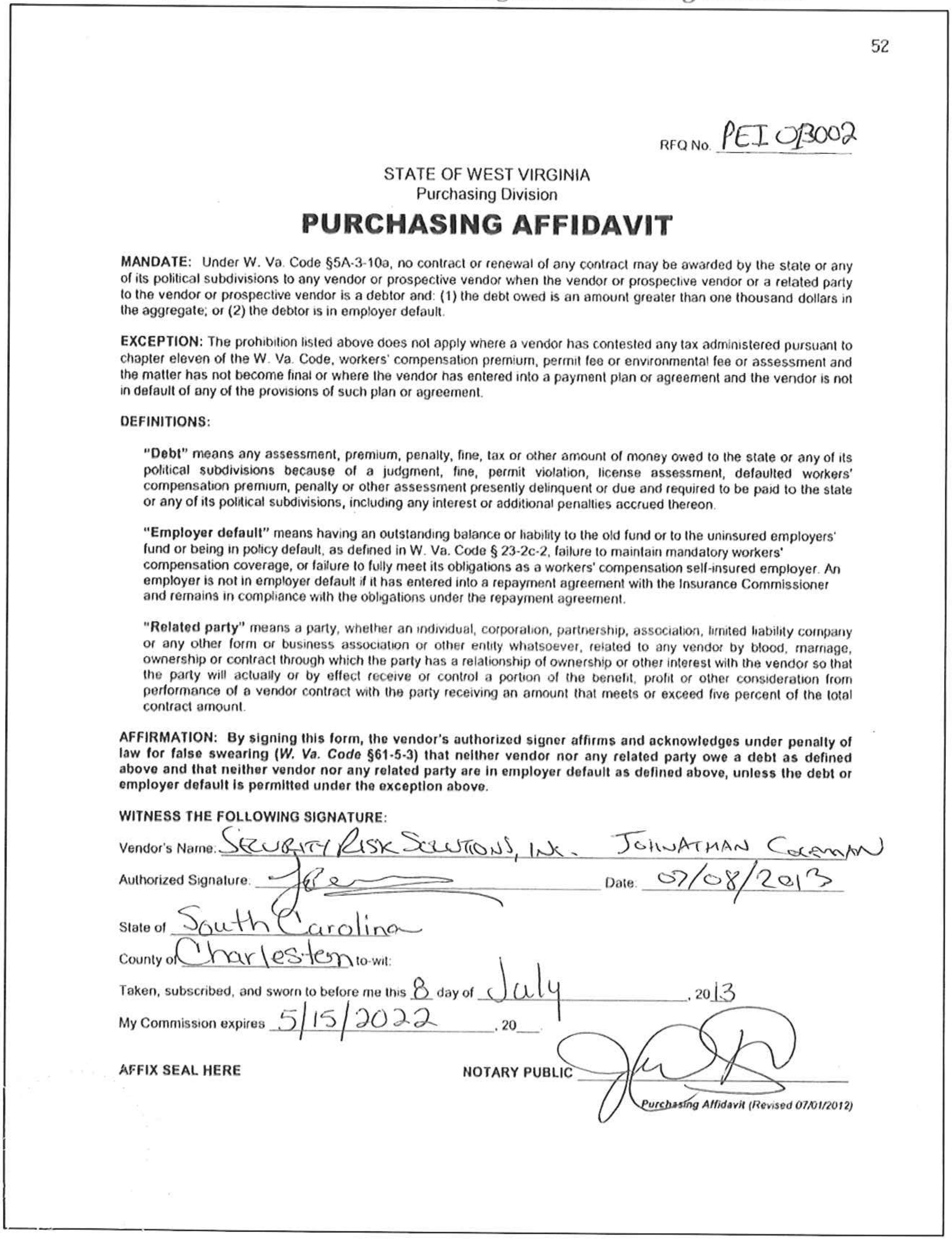
Authorized Signature

July 8th, 2013
Date

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

Revised 03/04/2013

Appendix D: State of West Virginia Purchasing Affidavit



RFQ No. PEI 013002

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. JONATHAN COLEMAN

Authorized Signature: Date: 07/08/2013

State of South Carolina

County of Charleston to-wit:

Taken, subscribed, and sworn to before me this 8 day of July, 2013

My Commission expires 5/15/2022, 20__.

AFFIX SEAL HERE **NOTARY PUBLIC**

Purchasing Affidavit (Revised 07/01/2012)

Appendix E: HIPAA Business Associate Addendum

SRS acknowledges and understands that is must sign and adhere to the WV HIPAA Business Associate Agreement, and also the Addendum as cited in the RFP.

Security Risk Solutions, Inc.
(Company)

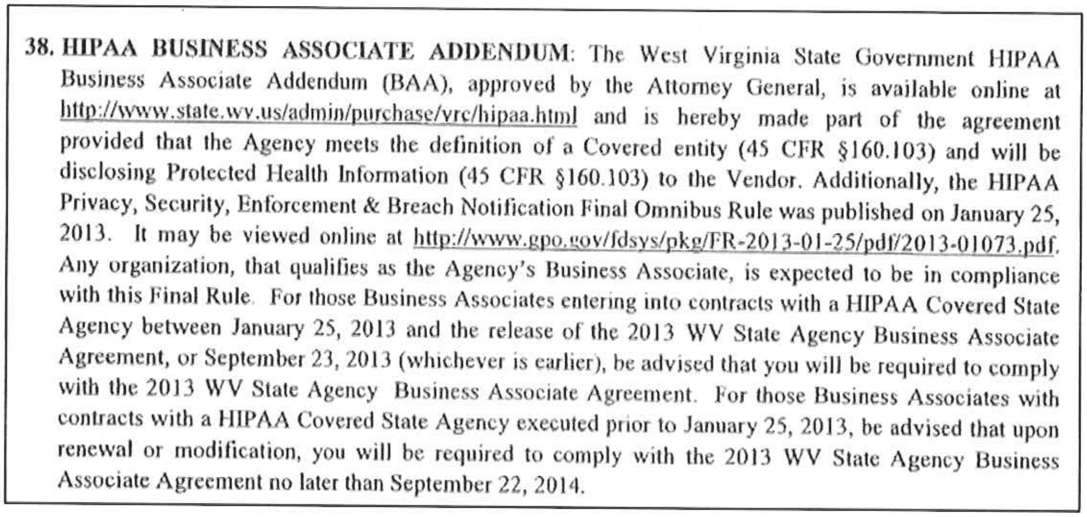
(Authorized Signature)

Johnathan Coleman, Principal
(Representative Name, Title)

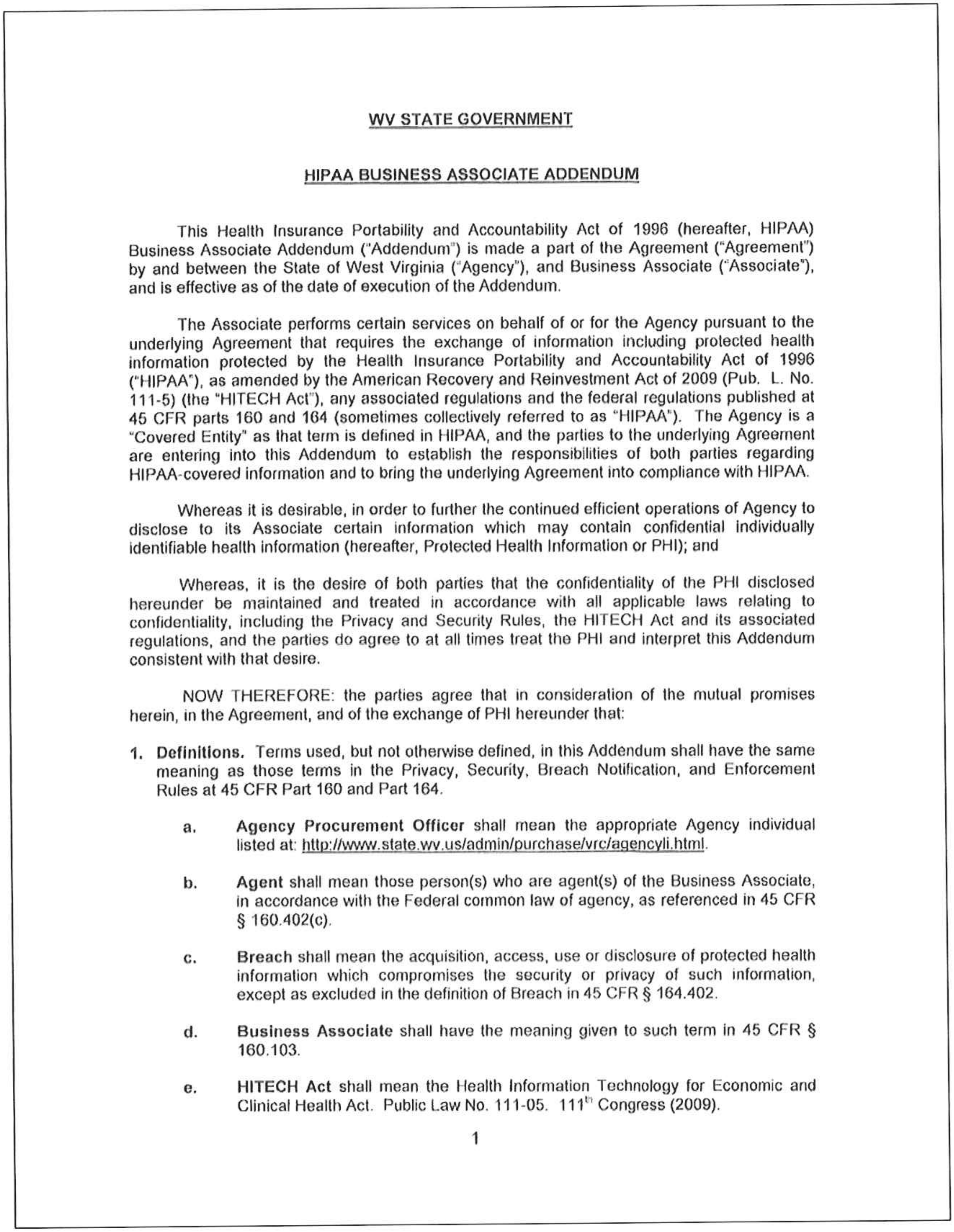
(P)843.647.1556 (F)843 416 4881
(Phone Number) (Fax Number)

8th July, 2013
(Date)

Figure 8: BAA Excerpt from RFP



38. **HIPAA BUSINESS ASSOCIATE ADDENDUM**: The West Virginia State Government HIPAA Business Associate Addendum (BAA), approved by the Attorney General, is available online at http://www.state.wv.us/admin/purchase/vrc/hipaa.html and is hereby made part of the agreement provided that the Agency meets the definition of a Covered entity (45 CFR §160.103) and will be disclosing Protected Health Information (45 CFR §160.103) to the Vendor. Additionally, the HIPAA Privacy, Security, Enforcement & Breach Notification Final Omnibus Rule was published on January 25, 2013. It may be viewed online at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Any organization, that qualifies as the Agency's Business Associate, is expected to be in compliance with this Final Rule. For those Business Associates entering into contracts with a HIPAA Covered State Agency between January 25, 2013 and the release of the 2013 WV State Agency Business Associate Agreement, or September 23, 2013 (whichever is earlier), be advised that you will be required to comply with the 2013 WV State Agency Business Associate Agreement. For those Business Associates with contracts with a HIPAA Covered State Agency executed prior to January 25, 2013, be advised that upon renewal or modification, you will be required to comply with the 2013 WV State Agency Business Associate Agreement no later than September 22, 2014.



WV STATE GOVERNMENT

HIPAA BUSINESS ASSOCIATE ADDENDUM

This Health Insurance Portability and Accountability Act of 1996 (hereafter, HIPAA) Business Associate Addendum ("Addendum") is made a part of the Agreement ("Agreement") by and between the State of West Virginia ("Agency"), and Business Associate ("Associate"), and is effective as of the date of execution of the Addendum.

The Associate performs certain services on behalf of or for the Agency pursuant to the underlying Agreement that requires the exchange of information including protected health information protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act"), any associated regulations and the federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA"). The Agency is a "Covered Entity" as that term is defined in HIPAA, and the parties to the underlying Agreement are entering into this Addendum to establish the responsibilities of both parties regarding HIPAA-covered information and to bring the underlying Agreement into compliance with HIPAA.

Whereas it is desirable, in order to further the continued efficient operations of Agency to disclose to its Associate certain information which may contain confidential individually identifiable health information (hereafter, Protected Health Information or PHI); and

Whereas, it is the desire of both parties that the confidentiality of the PHI disclosed hereunder be maintained and treated in accordance with all applicable laws relating to confidentiality, including the Privacy and Security Rules, the HITECH Act and its associated regulations, and the parties do agree to at all times treat the PHI and interpret this Addendum consistent with that desire.

NOW THEREFORE: the parties agree that in consideration of the mutual promises herein, in the Agreement, and of the exchange of PHI hereunder that:

1. **Definitions.** Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

   a. **Agency Procurement Officer** shall mean the appropriate Agency individual listed at: http://www.state.wv.us/admin/purchase/vrc/agencyli.html.

   b. **Agent** shall mean those person(s) who are agent(s) of the Business Associate, in accordance with the Federal common law of agency, as referenced in 45 CFR § 160.402(c).

   c. **Breach** shall mean the acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except as excluded in the definition of Breach in 45 CFR § 164.402.

   d. **Business Associate** shall have the meaning given to such term in 45 CFR § 160.103.

   e. **HITECH Act** shall mean the Health Information Technology for Economic and Clinical Health Act. Public Law No. 111-05. 111th Congress (2009).

f. **Privacy Rule** means the Standards for Privacy of Individually Identifiable Health Information found at 45 CFR Parts 160 and 164.

g. **Protected Health Information or PHI** shall have the meaning given to such term in 45 CFR § 160.103, limited to the information created or received by Associate from or on behalf of Agency.

h. **Security Incident** means any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy any information or interference with system operations in an information system.

i. **Security Rule** means the Security Standards for the Protection of Electronic Protected Health Information found at 45 CFR Parts 160 and 164.

j. **Subcontractor** means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

2. **Permitted Uses and Disclosures.**

a. **PHI Described.** This means PHI created, received, maintained or transmitted on behalf of the Agency by the Associate. This PHI is governed by this Addendum and is limited to the minimum necessary, to complete the tasks or to provide the services associated with the terms of the original Agreement, and is described in Appendix A.

b. **Purposes.** Except as otherwise limited in this Addendum, Associate may use or disclose the PHI on behalf of, or to provide services to, Agency for the purposes necessary to complete the tasks, or provide the services, associated with, and required by the terms of the original Agreement, or as required by law, if such use or disclosure of the PHI would not violate the Privacy or Security Rules or applicable state law if done by Agency or Associate, or violate the minimum necessary and related Privacy and Security policies and procedures of the Agency. The Associate is directly liable under HIPAA for impermissible uses and disclosures of the PHI it handles on behalf of Agency.

c. **Further Uses and Disclosures.** Except as otherwise limited in this Addendum, the Associate may disclose PHI to third parties for the purpose of its own proper management and administration, or as required by law, provided that (i) the disclosure is required by law, or (ii) the Associate has obtained from the third party reasonable assurances that the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the third party by the Associate; and, (iii) an agreement to notify the Associate and Agency of any instances of which it (the third party) is aware in which the confidentiality of the information has been breached. To the extent practical, the information should be in a limited data set or the minimum necessary information pursuant to 45 CFR § 164.502, or take other measures as necessary to satisfy the Agency's obligations under 45 CFR § 164.502.

3. **Obligations of Associate.**

a. **Stated Purposes Only.** The PHI may not be used by the Associate for any purpose other than as stated in this Addendum or as required or permitted by law.

b. **Limited Disclosure.** The PHI is confidential and will not be disclosed by the Associate other than as stated in this Addendum or as required or permitted by law. Associate is prohibited from directly or indirectly receiving any remuneration in exchange for an individual's PHI unless Agency gives written approval and the individual provides a valid authorization. Associate will refrain from marketing activities that would violate HIPAA, including specifically Section 13406 of the HITECH Act. Associate will report to Agency any use or disclosure of the PHI, including any Security Incident not provided for by this Agreement of which it becomes aware.

c. **Safeguards.** The Associate will use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of the PHI, except as provided for in this Addendum. This shall include, but not be limited to:

i. Limitation of the groups of its workforce and agents, to whom the PHI is disclosed to those reasonably required to accomplish the purposes stated in this Addendum, and the use and disclosure of the minimum PHI necessary or a Limited Data Set;

ii. Appropriate notification and training of its workforce and agents in order to protect the PHI from unauthorized use and disclosure;

iii. Maintenance of a comprehensive, reasonable and appropriate written PHI privacy and security program that includes administrative, technical and physical safeguards appropriate to the size, nature, scope and complexity of the Associate's operations, in compliance with the Security Rule;

iv. In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information.

d. **Compliance With Law.** The Associate will not use or disclose the PHI in a manner in violation of existing law and specifically not in violation of laws relating to confidentiality of PHI, including but not limited to, the Privacy and Security Rules.

e. **Mitigation.** Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Associate of a use or disclosure of the PHI by Associate in violation of the requirements of this Addendum, and report its mitigation activity back to the Agency.

f. **Support of Individual Rights.**

i. **Access to PHI.** Associate shall make the PHI maintained by Associate or its agents or subcontractors in Designated Record Sets available to Agency for inspection and copying, and in electronic format, if requested, within ten (10) days of a request by Agency to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.524 and consistent with Section 13405 of the HITECH Act.

ii. **Amendment of PHI.** Within ten (10) days of receipt of a request from Agency for an amendment of the PHI or a record about an individual contained in a Designated Record Set, Associate or its agents or subcontractors shall make such PHI available to Agency for amendment and incorporate any such amendment to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.526.

iii. **Accounting Rights.** Within ten (10) days of notice of a request for an accounting of disclosures of the PHI, Associate and its agents or subcontractors shall make available to Agency the documentation required to provide an accounting of disclosures to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR §164.528 and consistent with Section 13405 of the HITECH Act. Associate agrees to document disclosures of the PHI and information related to such disclosures as would be required for Agency to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. This should include a process that allows for an accounting to be collected and maintained by Associate and its agents or subcontractors for at least six (6) years from the date of disclosure, or longer if required by state law. At a minimum, such documentation shall include:

- the date of disclosure;
- the name of the entity or person who received the PHI, and if known, the address of the entity or person;
- a brief description of the PHI disclosed; and
- a brief statement of purposes of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure.

iv. **Request for Restriction**. Under the direction of the Agency, abide by any individual's request to restrict the disclosure of PHI, consistent with the requirements of Section 13405 of the HITECH Act and 45 CFR § 164.522, when the Agency determines to do so (except as required by law) and if the disclosure is to a health plan for payment or health care operations and it pertains to a health care item or service for which the health care provider was paid in full "out-of-pocket."

v. **Immediate Discontinuance of Use or Disclosure.** The Associate will immediately discontinue use or disclosure of Agency PHI pertaining to any individual when so requested by Agency. This includes, but is not limited to, cases in which an individual has withdrawn or modified an authorization to use or disclose PHI.

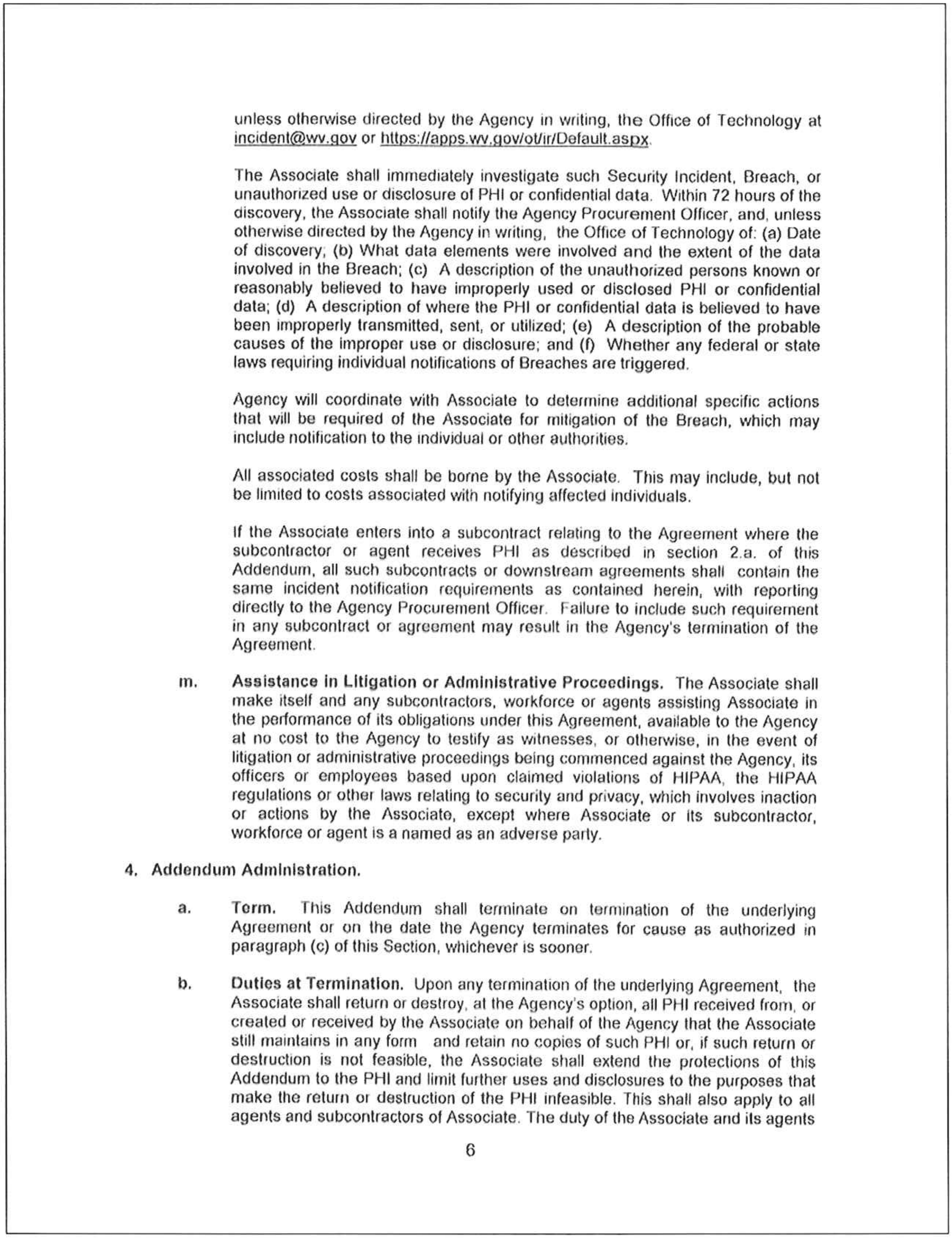
g. **Retention of PHI.** Notwithstanding section 4.a. of this Addendum, Associate and its subcontractors or agents shall retain all PHI pursuant to state and federal law and shall continue to maintain the PHI required under Section 3.f. of this Addendum for a period of six (6) years after termination of the Agreement, or longer if required under state law.

h. **Agent's, Subcontractor's Compliance.** The Associate shall notify the Agency of all subcontracts and agreements relating to the Agreement, where the subcontractor or agent receives PHI as described in section 2.a. of this Addendum. Such notification shall occur within 30 (thirty) calendar days of the execution of the subcontract and shall be delivered to the Agency Procurement Officer. The Associate will ensure that any of its subcontractors, to whom it provides any of the PHI it receives hereunder, or to whom it provides any PHI which the Associate creates or receives on behalf of the Agency, agree to the restrictions and conditions which apply to the Associate hereunder. The Agency may request copies of downstream subcontracts and agreements to determine whether all restrictions, terms and conditions have been flowed down. Failure to ensure that downstream contracts, subcontracts and agreements contain the required restrictions, terms and conditions may result in termination of the Agreement.

j. **Federal and Agency Access.** The Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI, as well as the PHI, received from, or created or received by the Associate on behalf of the Agency available to the U.S. Secretary of Health and Human Services consistent with 45 CFR § 164.504. The Associate shall also make these records available to Agency, or Agency's contractor, for periodic audit of Associate's compliance with the Privacy and Security Rules. Upon Agency's request, the Associate shall provide proof of compliance with HIPAA and HITECH data privacy/protection guidelines, certification of a secure network and other assurance relative to compliance with the Privacy and Security Rules. This section shall also apply to Associate's subcontractors, if any.

k. **Security.** The Associate shall take all steps necessary to ensure the continuous security of all PHI and data systems containing PHI. In addition, compliance with 74 FR 19006 Guidance Specifying the Technologies and Methodologies That Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII is required, to the extent practicable. If Associate chooses not to adopt such methodologies as defined in 74 FR 19006 to secure the PHI governed by this Addendum, it must submit such written rationale, including its Security Risk Analysis, to the Agency Procurement Officer for review prior to the execution of the Addendum. This review may take up to ten (10) days.

l. **Notification of Breach.** During the term of this Addendum, the Associate shall notify the Agency and, unless otherwise directed by the Agency in writing, the WV Office of Technology immediately by e-mail or web form upon the discovery of any Breach of unsecured PHI; or within 24 hours by e-mail or web form of any suspected Security Incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the Agency Procurement Officer at www.state.wv.us/admin/purchase/vrc/agencyli.htm and,



unless otherwise directed by the Agency in writing, the Office of Technology at incident@wv.gov or https://apps.wv.gov/ot/ir/Default.aspx.

The Associate shall immediately investigate such Security Incident, Breach, or unauthorized use or disclosure of PHI or confidential data. Within 72 hours of the discovery, the Associate shall notify the Agency Procurement Officer, and, unless otherwise directed by the Agency in writing, the Office of Technology of: (a) Date of discovery; (b) What data elements were involved and the extent of the data involved in the Breach; (c) A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data; (d) A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized; (e) A description of the probable causes of the improper use or disclosure; and (f) Whether any federal or state laws requiring individual notifications of Breaches are triggered.

Agency will coordinate with Associate to determine additional specific actions that will be required of the Associate for mitigation of the Breach, which may include notification to the individual or other authorities.

All associated costs shall be borne by the Associate. This may include, but not be limited to costs associated with notifying affected individuals.

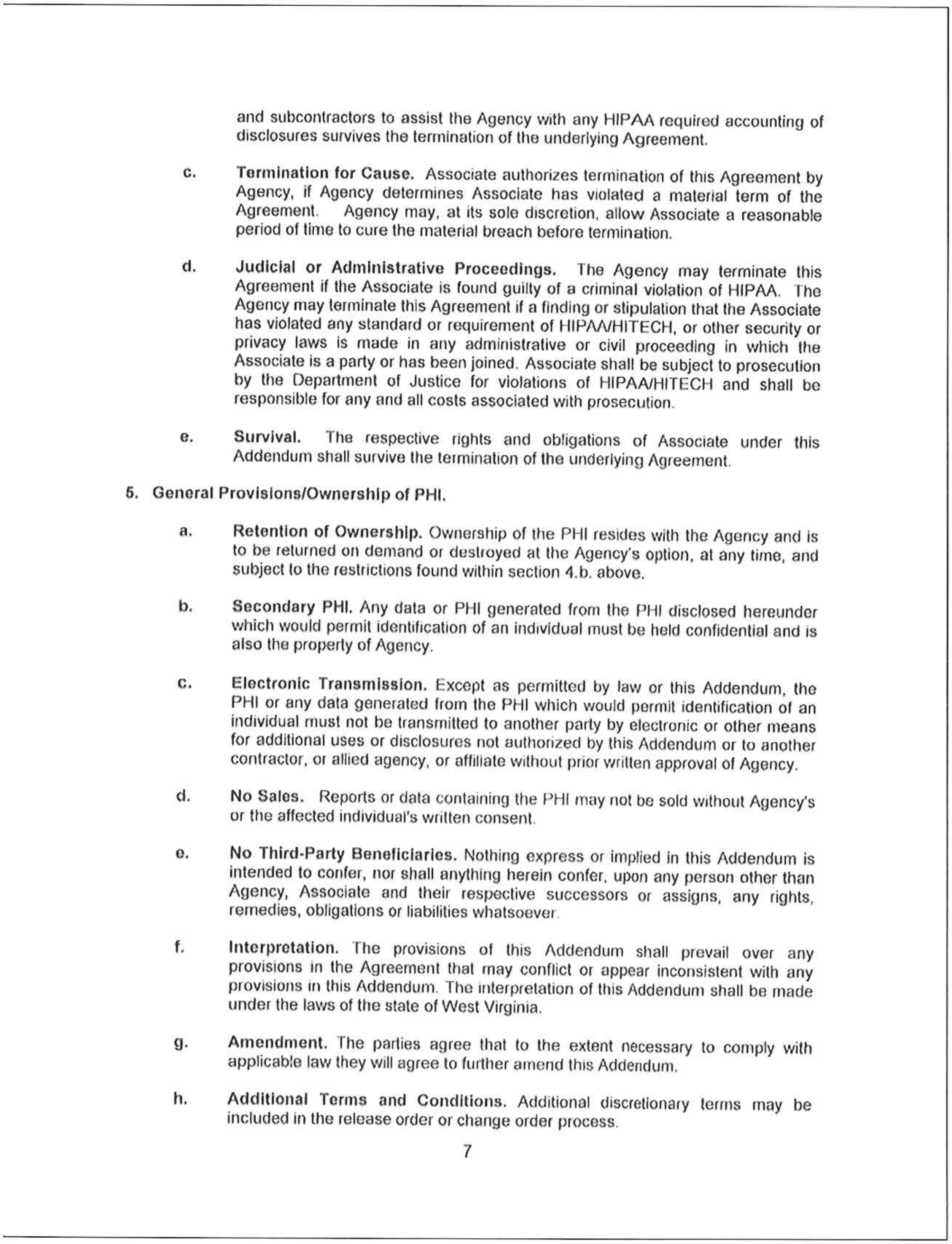
If the Associate enters into a subcontract relating to the Agreement where the subcontractor or agent receives PHI as described in section 2.a. of this Addendum, all such subcontracts or downstream agreements shall contain the same incident notification requirements as contained herein, with reporting directly to the Agency Procurement Officer. Failure to include such requirement in any subcontract or agreement may result in the Agency's termination of the Agreement.

m. **Assistance in Litigation or Administrative Proceedings.** The Associate shall make itself and any subcontractors, workforce or agents assisting Associate in the performance of its obligations under this Agreement, available to the Agency at no cost to the Agency to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Agency, its officers or employees based upon claimed violations of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inaction or actions by the Associate, except where Associate or its subcontractor, workforce or agent is a named as an adverse party.

4. Addendum Administration.

a. **Term.** This Addendum shall terminate on termination of the underlying Agreement or on the date the Agency terminates for cause as authorized in paragraph (c) of this Section, whichever is sooner.

b. **Duties at Termination.** Upon any termination of the underlying Agreement, the Associate shall return or destroy, at the Agency's option, all PHI received from, or created or received by the Associate on behalf of the Agency that the Associate still maintains in any form and retain no copies of such PHI or, if such return or destruction is not feasible, the Associate shall extend the protections of this Addendum to the PHI and limit further uses and disclosures to the purposes that make the return or destruction of the PHI infeasible. This shall also apply to all agents and subcontractors of Associate. The duty of the Associate and its agents



and subcontractors to assist the Agency with any HIPAA required accounting of disclosures survives the termination of the underlying Agreement.

c. **Termination for Cause.** Associate authorizes termination of this Agreement by Agency, if Agency determines Associate has violated a material term of the Agreement. Agency may, at its sole discretion, allow Associate a reasonable period of time to cure the material breach before termination.

d. **Judicial or Administrative Proceedings.** The Agency may terminate this Agreement if the Associate is found guilty of a criminal violation of HIPAA. The Agency may terminate this Agreement if a finding or stipulation that the Associate has violated any standard or requirement of HIPAA/HITECH, or other security or privacy laws is made in any administrative or civil proceeding in which the Associate is a party or has been joined. Associate shall be subject to prosecution by the Department of Justice for violations of HIPAA/HITECH and shall be responsible for any and all costs associated with prosecution.

e. **Survival.** The respective rights and obligations of Associate under this Addendum shall survive the termination of the underlying Agreement.

5. **General Provisions/Ownership of PHI.**

a. **Retention of Ownership.** Ownership of the PHI resides with the Agency and is to be returned on demand or destroyed at the Agency's option, at any time, and subject to the restrictions found within section 4.b. above.

b. **Secondary PHI.** Any data or PHI generated from the PHI disclosed hereunder which would permit identification of an individual must be held confidential and is also the property of Agency.

c. **Electronic Transmission.** Except as permitted by law or this Addendum, the PHI or any data generated from the PHI which would permit identification of an individual must not be transmitted to another party by electronic or other means for additional uses or disclosures not authorized by this Addendum or to another contractor, or allied agency, or affiliate without prior written approval of Agency.

d. **No Sales.** Reports or data containing the PHI may not be sold without Agency's or the affected individual's written consent.

e. **No Third-Party Beneficiaries.** Nothing express or implied in this Addendum is intended to confer, nor shall anything herein confer, upon any person other than Agency, Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

f. **Interpretation.** The provisions of this Addendum shall prevail over any provisions in the Agreement that may conflict or appear inconsistent with any provisions in this Addendum. The interpretation of this Addendum shall be made under the laws of the state of West Virginia.

g. **Amendment.** The parties agree that to the extent necessary to comply with applicable law they will agree to further amend this Addendum.

h. **Additional Terms and Conditions.** Additional discretionary terms may be included in the release order or change order process.

AGREED:

Name of Agency:________________

Signature:________________

Title:________________

Date:________________

Name of Associate: Johnathan Coleman, Security Risk Solutions, Inc.

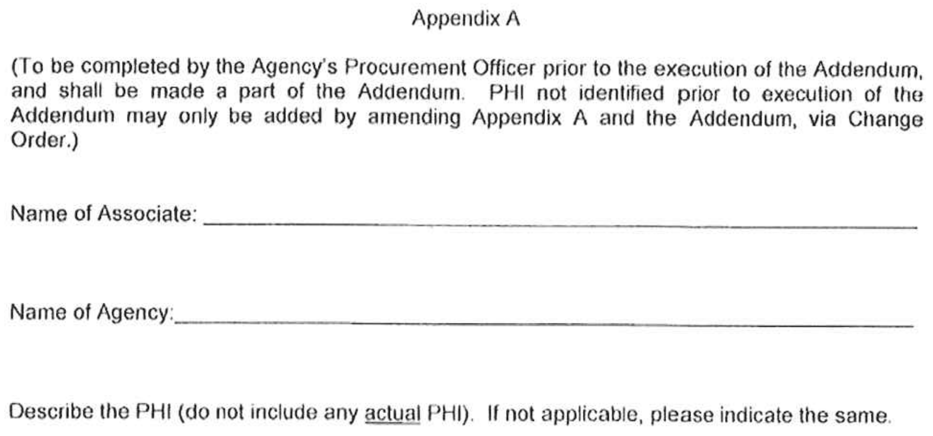
Signature:________________

Title: Principal

Date: 8th July, 2013

Form - WVBAA-012004
Amended 06.26.2013

APPROVED AS TO FORM THIS 26th
DAY OF Jun 20 13
Patrick Morrisey
Attorney General
BY ________________



Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. PHI not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

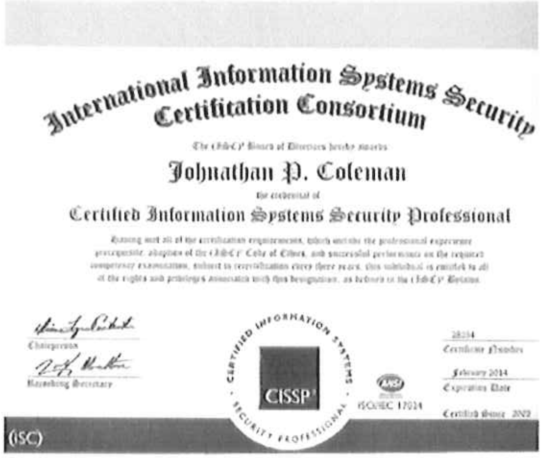
Name of Associate: ____

Name of Agency: ____

Describe the PHI (do not include any actual PHI). If not applicable, please indicate the same.

Appendix F: Copies of Staff Certifications and Degrees

NOTE: Due to the extensive number of certifications and degrees held by our team, only a sample has 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

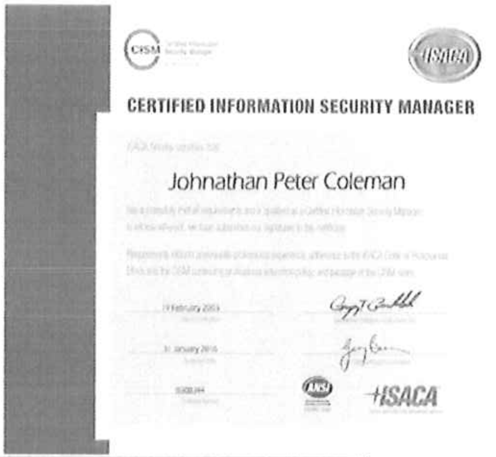
Secretary

28234
Certificate Number

February 2014
Expiration Date

Certified Since 2002

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP
ISO/IEC 17024
(ISC)



CERTIFIED INFORMATION SECURITY MANAGER

[illegible]

Johnathan Peter Coleman

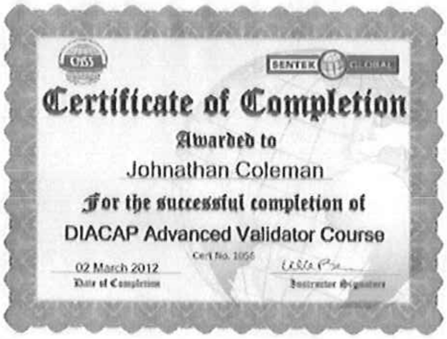
[illegible]

19 February 2003

31 January 2016

0308244

CISM
ISACA
ANSI



Certificate of Completion

Awarded to

Johnathan Coleman

For the successful completion of

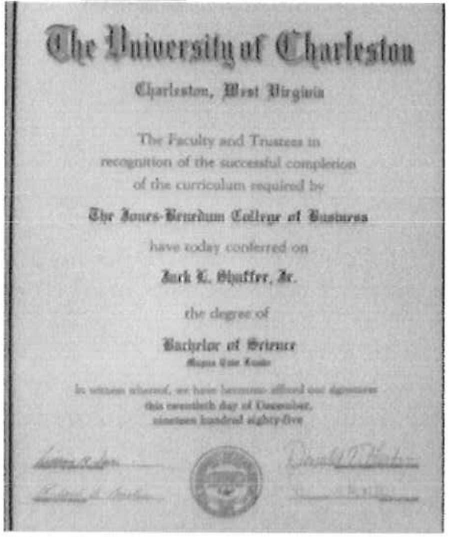
DIACAP Advanced Validator Course

02 March 2012
Date of Completion

Cert No. 1056

Instructor Signature

CISS
SENTEK GLOBAL



The University of Charleston

Charleston, West Virginia

The Faculty and Trustees in recognition of the successful completion of the curriculum required by

The Jones-Benedum College of Business

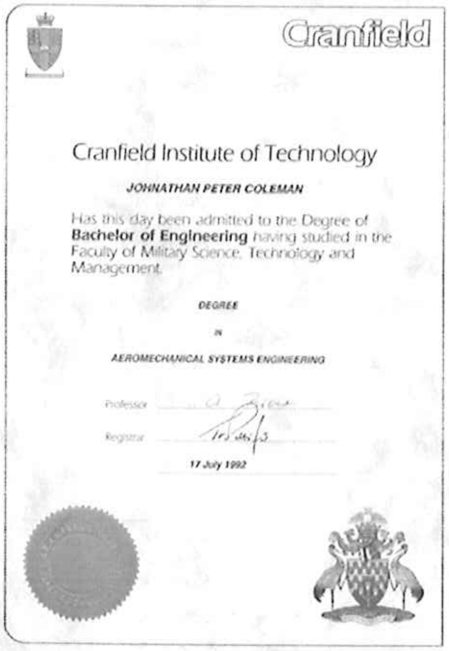
have today conferred on

Jack L. Shaffer, Jr.

the degree of

Bachelor of Science
Magna Cum Laude

In witness whereof, we have hereunto affixed our signatures this twentieth day of December, nineteen hundred eighty-five



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

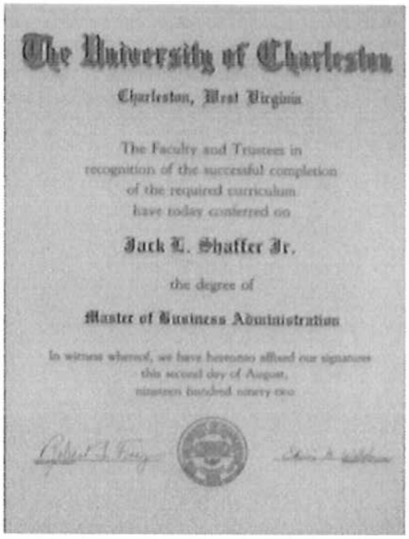
IN

AEROMECHANICAL SYSTEMS ENGINEERING

Professor

Registrar

17 July 1992



The University of Charleston

Charleston, West Virginia

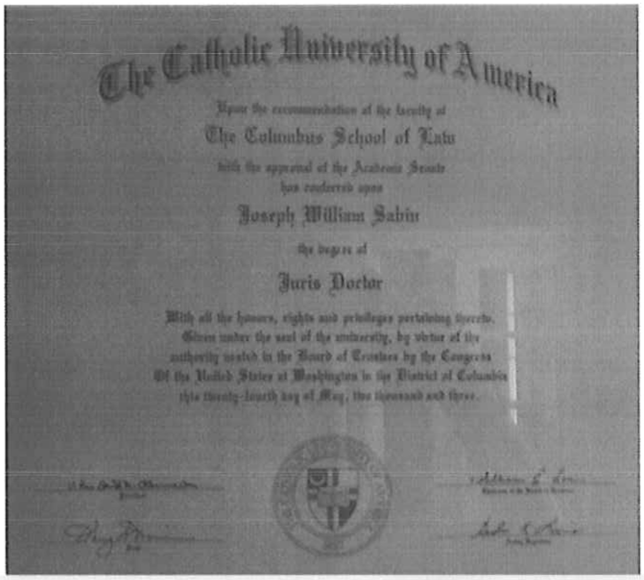
The Faculty and Trustees in recognition of the successful completion of the required curriculum have today conferred on

Jack L. Shaffer Jr.

the degree of

Master of Business Administration

In witness whereof, we have hereunto affixed our signatures this second day of August, nineteen hundred ninety one



The Catholic University of America

Upon the recommendation of the faculty of

The Columbus School of Law

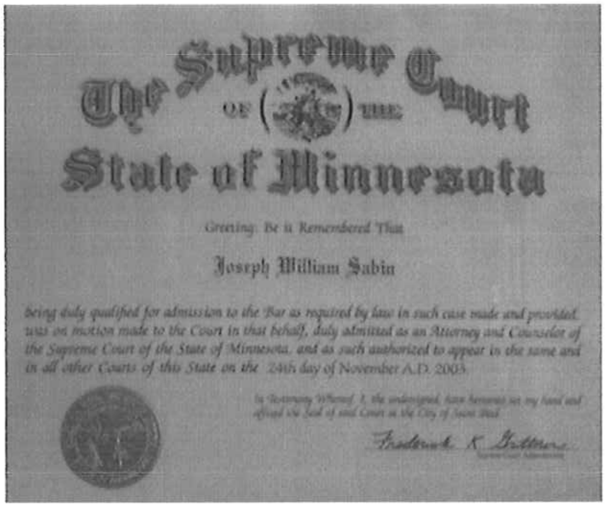
with the approval of the Academic Senate
has conferred upon

Joseph William Sabin

the degree of

Juris Doctor

With all the honors, rights and privileges pertaining thereto.
Given under the seal of the university, by virtue of the
authority vested in the Board of Trustees by the Congress
Of the United States at Washington in the District of Columbia
this twenty-fourth day of May, two thousand and three.



The Supreme Court of the State of Minnesota

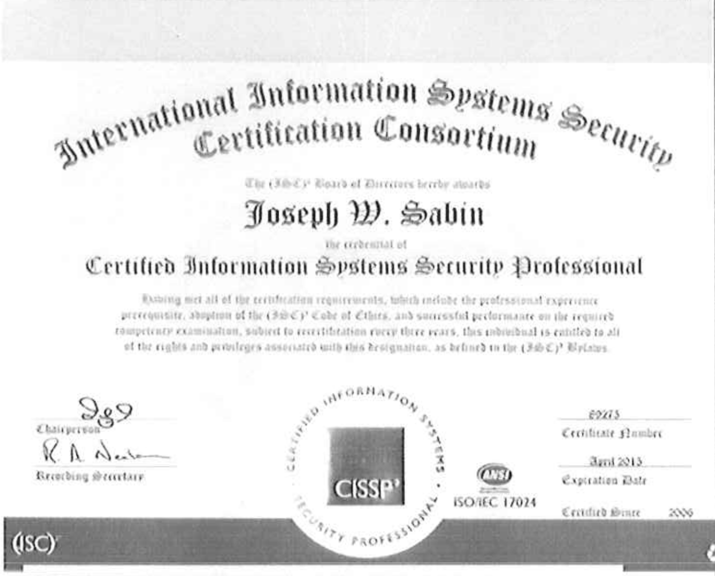
Greeting: Be it Remembered That

Joseph William Sabin

being duly qualified for admission to the Bar as required by law in such case made and provided, was on motion made to the Court in that behalf, duly admitted as an Attorney and Counselor of the Supreme Court of the State of Minnesota, and as such authorized to appear in the same and in all other Courts of this State on the 24th day of November A.D. 2003.

In Testimony Whereof, I, the undersigned, have hereunto set my hand and affixed the Seal of said Court in the City of Saint Paul

Frederick K. Grittner
Supreme Court Administrator



International Information Systems Security Certification Consortium

The (ISC)² Board of Directors hereby awards

Joseph W. Sabin

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

R. A. Newton
Recording Secretary

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®

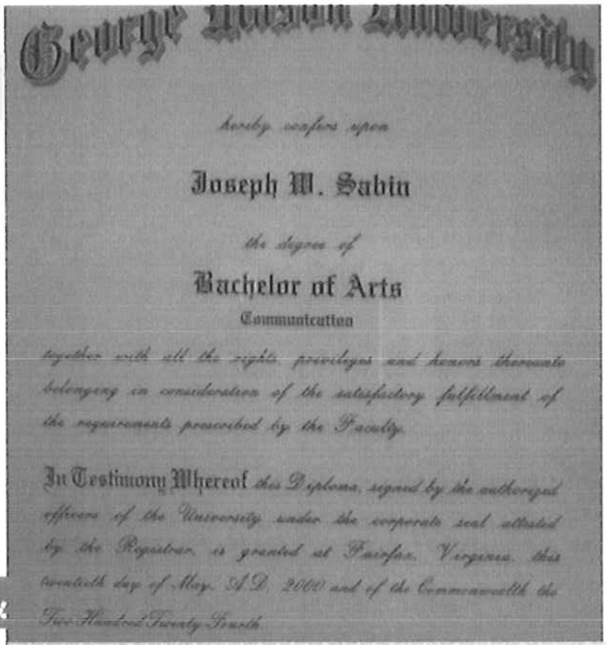
ANSI
ISO/IEC 17024

69273
Certificate Number

April 2013
Expiration Date

Certified Since 2006

(ISC)²



George Mason University

hereby confers upon

Joseph W. Sabin

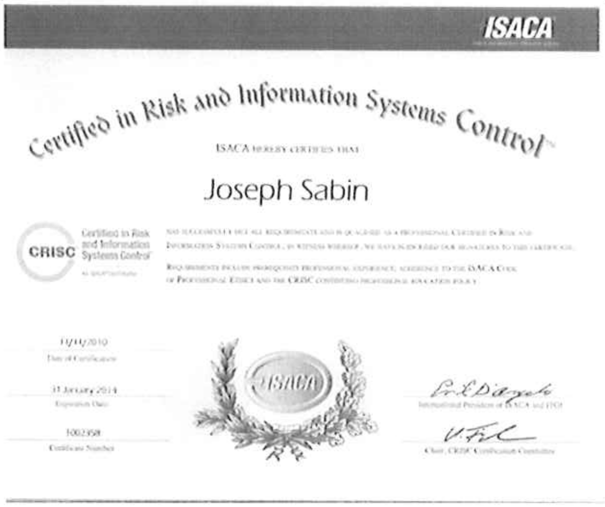
the degree of

Bachelor of Arts

Communication

together with all the rights, privileges and honors thereunto belonging in consideration of the satisfactory fulfillment of the requirements prescribed by the Faculty.

In Testimony Whereof this Diploma, signed by the authorized officers of the University under the corporate seal attested by the Registrar, is granted at Fairfax, Virginia, this twentieth day of May, A.D. 2000 and of the Commonwealth the Two Hundred Twenty-Fourth.



ISACA

Certified in Risk and Information Systems Control™

ISACA HEREBY CERTIFIES THAT

Joseph Sabin

CRISC Certified in Risk and Information Systems Control™

HAS SUCCESSFULLY MET ALL REQUIREMENTS AND IS QUALIFIED AS A PROFESSIONAL CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL. IN WITNESS WHEREOF, WE HAVE HEREUNTO PLACED OUR SIGNATURES TO THIS CERTIFICATE.

REQUIREMENTS INCLUDE PREREQUISITE PROFESSIONAL EXPERIENCE; ADHERENCE TO THE ISACA CODE OF PROFESSIONAL ETHICS AND THE CRISC CONTINUING PROFESSIONAL EDUCATION POLICY.

11/11/2010
Date of Certification

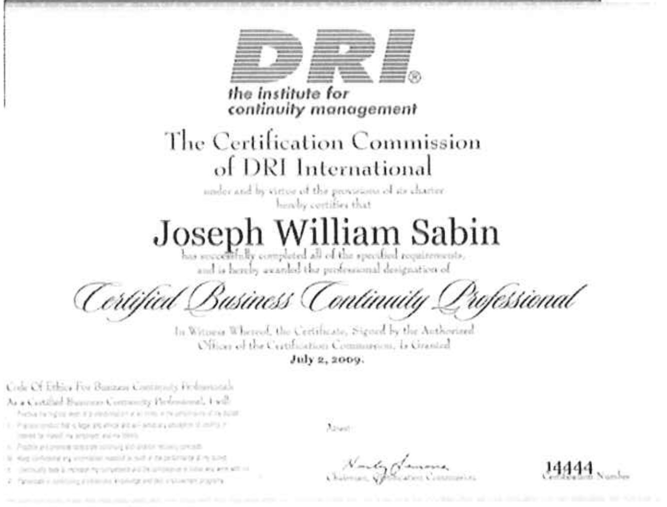
31 January 2014
Expiration Date

1002358
Certificate Number

ISACA

Rob E. D'Angelo
International President of ISACA and ITGI

V. Fd
Chair, CRISC Certification Committee



DRI®
the institute for
continuity management

The Certification Commission
of DRI International

under and by virtue of the provisions of its charter
hereby certifies that

Joseph William Sabin

has successfully completed all of the specified requirements,
and is hereby awarded the professional designation of

Certified Business Continuity Professional

In Witness Whereof, the Certificate, Signed by the Authorized
Officer of the Certification Commission, Is Granted
July 2, 2009.

Code Of Ethics For Business Continuity Professionals
As a Certified Business Continuity Professional, I will:
[illegible]

Attest:

Chairman, Certification Commission

14444
Certification Number

Appendix G: Resumes for Personnel Proposed

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

Education

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

Qualifications Summary

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. Mr. Coleman assists organizations with the development and implementation of information security programs including information security needs analysis, HIPAA/HITECH regulatory compliance, organizational resiliency planning, institutionalization of Risk Assessment and Business Impact Analysis methodologies, and facilitation of security compliance reviews. He leads client engagements for non-technical and technical services, including vulnerability assessments, penetration testing, system security testing, Certification and Accreditation (C&A), and IT contingency planning. He has participated as a lead auditor in numerous HIPAA security reviews, providing compliance gap analyses and recommendations which have been used in the development of Corporate Integrity Agreements and post-breach remediation plans.

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. He leads client engagements for non-technical and technical services, including vulnerability assessments, penetration testing, system security testing, certification and accreditation (C&A), and IT contingency planning. He participated as a lead auditor in numerous HIPAA Security reviews, providing compliance gap analyses and recommendations which have been used in the development of Corporate Integrity Agreements and post-breach remediation plans. Examples of HIPAA/HITECH Risk Assessment and Compliance Reviews include: Memorial Sloan Kettering Cancer Center (MSKCC), Community Healthcare Network of Connecticut (CHNCT), Princeton Health Care System (PHCS), and Rapid City Regional Healthcare (RCRH). He has provided HIPAA/HITECH security and privacy and Meaningful Use training to hundreds of providers through the ONC Regional Extension Center program, where SRS is under contract to the state of Alabama for providing HIPAA/HITECH Security and Privacy expertise.

He is a Navy Certification Authority (CA) Fully Qualified Navy Validator (FQNV), authorized to make certification determination recommendations to the Designated Approving Authority on whether or not Navy Information Systems and Enclave Networks should be granted an Accreditation for Authority to Operate (ATO). He is 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).

Experience Summary

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

Mr. Coleman provides security and privacy subject matter expertise to a variety of Federal and commercial healthcare clients. Building on his military background where he specialized in security communications, he has focused specifically on healthcare security and privacy for the last 13 years. For the Navy Medicine Information Systems Support Activity, tasking included providing SME support for Continuous Risk Management activities for over 20 medical treatment facilities in the Navy Medicine enterprise. As another example of his deep familiarity with DoD healthcare, he worked with Carnegie Mellon University's Software Engineering Institute as the Program Manager for the Defense Healthcare Information Assurance Program (DHIAP), a program funded through TATRC to identify security capabilities and train DoD personnel from over 200 Medical Treatment Facilities in the OCTAVE Information Security Risk Assessment methodology. He has further experience supporting TATRC in conjunction with Georgetown University Medical Center, where he participated in Project Argus - a Biosurveillance and early warning system which operates as a primer for U.S. countermeasure response plans in the context of a potentially catastrophic bioevent. The following projects highlight specific experience with relevance to Healthcare HIPAA Security and Privacy experience:

Department of Health and Human Services
Data Segmentation for Privacy Initiative Coordinator *(Sep 2011 – present)*
Healthcare IT Standards Panel (HITSP) Facilitator, Security and Privacy Technical Committee *(Oct 2005 – Apr 2010)*

As a nationally recognized subject matter expert in security and privacy interoperability standards, he was recently appointed the Data Segmentation for Privacy Initiative Coordinator by the Chief Privacy Officer at the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology (ONC). Under this program, Mr. Coleman leads and directs all activities associated with the development of a standards-based approach to applying privacy metadata to granular elements of an Electronic Health Record in order to appropriately sequester certain information which requires enhanced protection under the law (e.g. Veterans' Health Data protected under 38 USC Section 7332, "Title 38") while allowing other data to flow more freely. In this capacity he provides oversight on behalf of ONC to the VA/SAMHSA pilot which is proving the capability to apply entry-level tagging of privacy metadata to documents in the VA's EHR system and enforcing policy such as a prohibition on redisclosure. This pilot is directly testing the standards recommended by the Federal Health IT Standards Committee and the results are being used to inform not only the requirements for the DoD/VA iEHR, but also are informing meaningful use legislation, making the requirements mandatory for all certified EHR systems.

Building on his experience with the American National Standards Institute (ANSI) team tasked with harmonizing standards for seamless and secure electronic exchange of patient data, Mr. Coleman was selected to co-chair the HITSP Security, Privacy and Infrastructure ARRA tiger team which was chartered by HHS and supported by the VA and DOD to develop Interoperability Specifications to meet the requirements of the AHIC Use Cases and new provisions under HITECH. In this capacity he was responsibility for the harmonization of 249 security and privacy standards into the development of 30 specifications, including TP 20 (Access Control) and TP 30 (Management of Consent Directives). Mr. Coleman provided testimony on this work and the functional security requirements of the National Health Information Network (NHIN) to 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. In recognition of these achievements, the implementation specifications were recognized by the Secretary of the Department of Health and Human Services and published in the Federal Register.

Advanced Technology Institute
Deputy Director, Information Protection Technology *(2001 – 2005)*

As Deputy Director, Information Protection Technology at the Advanced Technology Institute (ATI), Mr. Coleman led the effort in training over 200 Department of Defense Information Security Readiness Teams in the OCTAVE methodology and authored instructor and train-the-trainer manuals for use by the DoD. This was part of the

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

multi-year, $12M research program named Defense Health Information Assurance Program (DHIAP) funded through TATRC. Mr Coleman served as Program Manager for the DHIAP and also led the Risk Assessment development and training tasks. While at ATI he conducted regulatory compliance gap analyses, technical vulnerability assessments and Business Impact Analyses for healthcare stakeholders, including the Department of Veterans Affairs. For example, he assisted the Ralph Johnson VA hospital with an on-site security assessment of their biomedical systems. Other engagements included on-site risk assessments with Memorial Sloan Kettering Cancer Center (MSKCC) in NY City, The University Medical Center at Princeton, the Cancer Treatment Centers of America, a regional group of 44 medical facilities in South Dakota, Georgetown University Medical Center, and the US Naval Base in Rota, Spain.

Regional Manager *(1998 – 2001)*

Mr. Coleman worked at Federal Risk Management Solutions (FRMS) and then at WareOnEarth Communications Inc, where he was responsible for program management of a $30 million Information Security Contract with the DoD's High Performance Computing and Modernization Office through SPAWAR, the Space and Naval Warfare Center. He was also appointed as the ISSO responsible for managing the C&A process of a newly developed security system for the US Postal Service and the Social Security Administration.

British Army *(1989 – 1998)*

Mr. Coleman is a graduate of the Royal Military College of Science in the United Kingdom and the Royal Military Academy, Sandhurst. As a commissioned officer in the British Army he held various NATO and UK Ministry of Defense (Army) positions engaged in the engineering, installation, and operation of deployable secure communication facilities. He received post graduate training with configuration and installation of secure WANs for voice and data in a wide range of communications systems and was awarded the prestigious "Top Student" honor in his class. Experience includes the redesign and operational management of the Multi-National Division Communications Headquarters for operations in Bosnia Herzegovina, multinational amphibious force tasking in Sardinia, United Nations attachment at the Greek-Turkish border in Cyprus, and anti-terrorist training for duties overseas.

Certifications, and Affiliations

Certifications

- Navy Certification Authority Fully Qualified Navy Validator (FQNV)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)

Publications and Noteworthy Presentations

- *Extra-Sensitive PHI: Appropriate Sharing using Data Segmentation for Privacy*, HIMSS 2013 Conference and Exhibition, March 2013, New Orleans, LA.
- *Segmenting Data Privacy;* Journal of AHIMA featured article, February 2013
- *Response to the HITSC Recommendations on Patient Privacy, Provenance and Identity Metadata*, Testimony to the Health IT Standards Committee (HITSC) Privacy and Security WG, 6/29/2012
- *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

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

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, Virginia
- 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

JACK L. SHAFFER, JR.
Chief Operating Officer, KRM Associates, Inc.

Education

INSTITUTION AND LOCATION	DEGREE	YEARS	FIELD OF STUDY
University of Charleston, Charleston, WV	MBA	1992	Business Administration
University of Charleston, Charleston, WV	BS (Magna Cum Laude)	1986	Computer Information Systems

Qualifications Summary

Mr. Shaffer has deep technical expertise spanning broad range of bleeding-edge technologies in the areas of telecommunications, m-Health, network solutions, hardware, software, operating systems, and programming languages. A summary of qualifications and characteristics follows:

- *Industry Vision & Leadership*
- *Business & Technology Strategy Plans*
- *Large-Scale Technology Operations*
- *Project Lifecycle Management*
- *Technology Infrastructure Development*
- *Best-Practice Process Engineering*
- *P&L / Financial Management*
- *Staff Hiring, Training & Retention*
- *Organizational Change Management*
- *Systems Design & Deployment*
- *M&A Corporate Integrations*

Unusual depth in both technology and business. Strong resource in all aspects of IT with 25+-year record of practical business application in both start-up and Fortune 500 companies. MBA and BS in Information Systems.

Big-picture, future focus, leveraging technology innovation and industry best-practices to drive change, capitalize on strategic market opportunities, capture operational efficiencies, and resolve complex business problems.

Accomplished presenter and communicator; achieve organizational excellence by creating an environment of collaboration and trust across all stakeholders. Unmatched work ethic, dedication, persistence, and adaptability.

Recognized healthcare technology leader tapped for management and Board roles in leading state-level organizations. Served as the "voice of change" for healthcare delivery and management through next-generation IT solutions.

Experience Summary

Mr. Shaffer's career has spanned multiple industries, primarily those in energy delivery and healthcare information technology. In all positions, he has exhibited strong leadership and consistent attention to detail in designing, implementing, managing, securing, and maintaining information systems, resulting in greater reliability, improved business processes, lower costs, and better customer service. He is bringing his wealth of technical and management skills, as detailed below, to KRM Associates, Inc. in July 2013.

Northeast Natural Energy, Charleston, WV
Vice-President Information Management (2010 – 2013)
Partner responsible for all aspects of the organization's information technology and systems as well as providing vision and leadership in the development and implementation of IT initiatives.

JACK L. SHAFFER, JR.
Chief Operating Officer, KRM Associates, Inc.

- Architected and implemented a highly scalable virtualized IT infrastructure using VMWare / VSphere with Dell Equillogic SANs to meet the demands of a rapidly growing business. Brought project in on-time and 30% under budget and increased system reliability to 99.5%.
- Replaced costly and inefficient business process outsource arrangement for accounting and land administration with an integrated software package. Led search and selection committee which recommended the acquisition of a unified General Ledger, Joint-Interest Billing, and Land Accounting package with integrated document imaging and indexing system. The system achieved a 17 month ROI over the business process outsource arrangement and allowed for increased integration between land, accounting and geographic information systems.
- Commissioned, designed, and provided project management for a custom competitive intelligence application providing vital information for key decision makers. System aggregated, cataloged and presented data from a variety of public and private data sources to provide greater levels of industry competitor activity while simultaneously removing 160 man hours per month in manual effort spent by the organization in gathering and organizing competitive information.
- Commissioned, designed, and provided project management for custom accounts payable routing and approval application. The custom web-based application fully integrated with the existing accounting software package and document imaging system, allowed for the elimination of the physical routing of invoices, which saved cycle-time and logistics costs, and reduced account classification errors by over 50% by use of an advanced logic engine. Accounting package software vendor has approached NNE to license the product.

Community Health Network of West Virginia (CHNWV), Scott Depot, WV
Chief Information Officer (2006 - 2010)

Provided strategy and driving action to develop and implement enterprise IT solutions in support of business operations. Top management authority for entire IT organization, staff of 17 direct/indirect reports, organizational structure and policies, network security, and service desk.

- Implemented, operated and enhanced the Indian Health Services Resource Patient and Management System (RPMS) EHR – a derivative of the Veterans Administration's VistA EHR - for member rural health clinics. The open source RPMS-EHR system is a fully integrated system - with CPOE for laboratory, radiology, medications; clinical decision support with order checks and clinical reminders; and progress notes – that was designed for use in hospital systems, which the organization adapted for use in a primary care environment.
    - In four years, the centrally hosted RPMS-EHR system was deployed in nearly 50 clinical locations and contained more than 190,000 unique patients – over 10% of West Virginia's total population - making it one of the largest EHR's deployed in the State of West Virginia at that time.
    - Developed an actionable and repeatable 31-week project implementation and training plan - that consisted of over 800 total hours of training - which was used at every health center adopting the EHR.
        - Commissioned and assisted in the development of custom medication management enhancements to the IHS RPMS-EHR which further adapted the system for use within West Virginia and the FQHC environment:
        - Added functionality to auto-finish medication orders within the system as necessitated by the fact that ambulatory providers do not have internal pharmacists to dispense and

JACK L. SHAFFER, JR.
Chief Operating Officer, KRM Associates, Inc.

finish the medication orders as required by the system.

- Created a custom prescription printing and faxing module which allowed for compliance of West Virginia law regarding Nurse Practitioners and Physician Assistants by creating a process to record, store, and print on the prescription the specific drug classes allowed to be prescribed for each PA or NP.
- Commissioned and assisted in the development of a custom open source iPhone application connected to the RPMS-EHR system. The application allowed for the creation, signing, printing, and faxing of new or existing medication orders – with full medication order checks and electronic signatures.

- Spearheaded the creation of a robust clinical data warehouse / business intelligence platform for health information - in cooperation with the clinical committee - which allowed member health centers to easily report on standardized clinical quality outcomes and measures. The system allowed member health centers to report on 24 clinical outcome measures and compare those measures to National Committee for Quality Assurance (NCQA) standard benchmarks in an effort to improve clinical outcomes for the patients of member health centers.
- Reengineered IT infrastructure to meet industry best practices and led turnaround of service desk strategy.
  - Managed plan to migrate entire datacenter to new facility and upgraded legacy network technology.
  - Realigned service organization with corporate goals, created program management office (PMO), and established ITIL best practices, change management processes, problem management system, and network monitoring system. Increased network reliability to 99.5%, improved network performance over 200%, and cut TCO $40,000 annually.
  - Delivered highly responsive service organization that handled average of 600 calls per month with 1:65 support desk to client ratio (less than half the industry standard), achieved 90% customer satisfaction rating, and was highly mobile.
- Created a Central Business Office and internal Medical Manager support desk. Created job descriptions, staffed positions, trained new hires, and terminated contract with outsourced vendor. Migrated all calls to internal support desk with no service interruptions, cut support costs $78,000 annually (23% of total support budget), and improved customer responsiveness, effectiveness, and satisfaction.
- Served as HIPAA Compliance Executive/Security Officer for the organization.

Chesapeake Energy, Charleston, WV
Manager, Technology Services & Development, Eastern Division, 2005-2006
Directed IT infrastructure for new Eastern Division including application servers, client support, database management systems, telecommunications, LAN/WAN, and helpdesk operations. Led staff of 5 direct and 10 indirect reports.

- Developed and staffed newly created Eastern Division following Chesapeake's acquisition of Columbia Natural Resources (CNR) from Triana Energy.
- On-boarded all CNR IT staff, resulting in full personnel merger with 0% attrition rate due to high caliber of professionals (Fortune 100-level qualifications) previously recruited and managed at CNR.
- Architected integration plan and migration of all systems from separate Active Directory/MS Exchange domains and Citrix farms into single, unified domain within 1 month of acquisition of

JACK L. SHAFFER, JR.
Chief Operating Officer, KRM Associates, Inc.

CNR.

- Achieved full migration of 50 servers, 300+ users, and associated client machines to new domain with minimal downtime, enabling employees of both organizations to share resources seamlessly.

Triana Energy / Columbia Natural Resources, LLC, Charleston, WV
Manager, Technology Services & Development (2003 – 2005)

Held high-level scope of authority that included $2.5 million annual O&M budget, annual capital budgets as large as $1 million, 300-person user base, 10 direct reports, and entire IT infrastructure (hardware, operating systems, database management, telecommunications, Internet/intranet, LAN/WAN, security, client support, and helpdesk operations.

- Led numerous initiatives to cut costs and improve operating efficiencies. Examples include:
  - Led 3-month project to restructure telecommunications to eliminate duplicate vendors and transition to lower-cost/higher-speed broadband connections. Saved $205,000+ annually and increased access speeds 2-3 fold.
  - Commissioned 9-month, $350,000 project to scan, index, and archive 2.5 million mission-vital land lease documents in fully searchable, digital format. Cut operating costs nearly $800,000 per year and boosted staff productivity.
- Partnered with outside consultants to prepare organization for successful Sarbanes-Oxley (SOX 404) audit. Led IT general controls component; designed and implemented change management, security, business continuity, disaster recovery, and audit-related controls to achieve IT compliance with COBIT best practices.
- Piloted implementation of intrusion detection/prevention tools and policies to monitor network activity, which allowed the organization to pass independent intrusion penetration test by world-class organizations. Security policies and capabilities recognized by security expert as being stronger and more effective than many Fortune 500 companies.

Triana Energy, LLC, Charleston, WV
Manager, Technology (2001 – 2003)

Partner in newly formed Triana Energy challenged with design and implementation of company's entire IT infrastructure.

- Built all aspects of enterprise IT architecture and operations from scratch in less than 2 months.
- Leveraged next-generation solutions to provide this small, startup organization with more capabilities than much larger organizations and create highly mobile workforce with 24/7 access from virtually anywhere worldwide.
- Directed team in separation and subsequent integration efforts surrounding purchase of Columbia Natural Resources (CNR) from Nisource.
- Renegotiated technology-related contracts with major software/hardware vendors. Drove migration plan to seamlessly move 340 employees to all-new enterprise systems with zero downtime or service interruptions. Led Triana in assuming full operations of CNR month earlier than anticipated (2 months after purchase date).
- Promoted to Manager of Technology Services & Development after purchase of CNR from Nisource.

Nisource Business Services, Columbus, OH

JACK L. SHAFFER, JR.
Chief Operating Officer, KRM Associates, Inc.

Manager, Application Architecture (2000 – 2001)

Guided strategic corporate direction for application architecture. Managed team of 5 direct reports in all aspects of data warehousing, Enterprise Application Integration (EAI), middleware, load testing, and quality assurance.

- Key member of IT team formed to integrate IT departments in acquisition of Columbia Energy/Columbia Gas System by Nisource.
- Developed organizational structure, policies, and staffing to support newly formed security group, centralized IT helpdesk, distributed client support, network operations center (NOC), and application architecture department.
- Team successfully reevaluated and placed 800+ IT professionals among 10 different operating companies within 4 months. Project also reduced operating costs $300+ million to aid in financing purchase.

Columbia Natural Resources, Inc., Charleston, WV
Manager, Network Services (1997 - 2000)

Managed all aspects of corporate network including hardware, operating systems, database management, helpdesk, and telecommunications. Scope of authority included $1.5 million annual O&M budget, $500,000 annual capital budget, base of 300+ users, and 10 staff. Member of Columbia Energy Group IT Management Council and Security Council.

- Led multi-year effort to modernize and expand corporate IT environment and capabilities.
- Led design, development, and installation of custom PDA data collection system in $800,000 project that spanned 16 field locations in 6 states and involved 100+ field staff, telecommuting developers, and union representatives. Achieved on-time, on-budget completion and unparalleled 100% adoption rate among unionized workforce in this politically charged project. Decreased data collection cycle time from 3 weeks to 1 and reduced data errors 70%.
- Chief architect for developing roadmap and replacing outdated 3-tier middleware program that was key component for every mission-critical application. Resulted in stable, vendor-neutral platform that remained in service 8 years.
- Engineered business continuity and disaster recovery plan to support mid-range client/server environment. Negotiated contracts with leading hot-site provider, developed recovery plans, and introduced disaster recovery tests at hot-site. Created capabilities to restore all mission-critical applications and data in less than 24 hours.
- Developed standard M&A due diligence templates and custom data conversion/cleansing programs. Served as the foundation for 3 successful acquisitions (Alamco, Wiser Oil, Meridian) delivered on-time and budget

Affiliations

- Board member of the West Virginia Telehealth Alliance
- Member of West Virginia Chapter of HIMSS
- Featured thought leader and speaker for numerous industry-leading healthcare and technology conferences, board meetings, continuing education seminars, and state legislative committees
- Co-authored a whitepaper on using an EHR as a health improvement tool.

Mr. Joseph Sabin, Esq., CISSP, FQNV, CBCP, CRISC
***Director, Federal IA Programs*, Security Risk Solutions, Inc.**

Education

INSTITUTION AND LOCATION	DEGREE	YEARS	FIELD OF STUDY
George Mason University, Fairfax, Virginia	BA (Bachelor of Arts)	2000	Communications
The Catholic University of America, Columbus School of Law, Washington D.C.	JD (Juris Doctor)	2003	Law
	Post Graduate Certificate	2003	Communications Law and Policy

Qualifications Summary

Mr. Sabin has over twenty years of demonstrable experience leading Enterprise-level Information Assurance (IA) and Risk Assessment initiatives, particularly within Federal and DoD healthcare technology environments. Representative experience includes establishing and executing organization-wide efforts in areas of IA Vulnerability Management (IAVM), Continuity of Operations (COOP), Certification and Accreditation (C&A), organizational resiliency, and risk management. Mr. Sabin further leverages his legal education, training and experience in areas of policy assessment and compliance to ensure Federal law, Agency policy, and Service-level directives, processes, and instructions are factored into overarching defense-in-depth activities. Mr. Sabin leads teams as well as participates within broader IA, IT, and functional organizational units. For example, Mr. Sabin has initiated and led two functional IA teams within an Enterprise Information Assurance department for Navy Medicine activities for more than four years, institutionalizing compliance measures for more than fifty Commands and 30 Programs of Record (PORs). He has introduced and guided to successful fruition C&A execution to new technology stakeholders (both Federal and commercial) and requirements such as were necessary to support Army-deployment of non-tactical Land Mobile Radio across all CONUS-based installations. He has also led several comprehensive Federal risk assessment efforts to include an effort for the Department of Health and Human Services (HHS) Centers for Disease Control and Prevention (CDC). Mr. Sabin has experience leading a team with efforts focused on assessing, training, and integrating emerging technologies via assessments, forums, and broad multi-media platforms.

Mr. Sabin holds several relevant professional credentials to include licensure to practice law by the State of Minnesota, Certified Information Systems Security Professional (CISSP), Fully Qualified Navy Validator (FQNV), Certified Business Continuity Professional (CBCP), Certified in Risk and Information Systems Control (CRISC), and Information Technology Infrastructure Library (ITIL) v.2 foundations.

Experience Summary

Mr. Sabin currently serves as the Director for Federal IA Programs at SRS. Within this capacity, he provides guidance and measured oversight to various IA projects and activities within the SRS portfolio. In the Federal Health IT domain, Mr. Sabin continues to provide task leadership and subject matter expertise to Federal clients including the Space and Naval Warfare (SPAWAR) Systems Center Atlantic. More specifically, Mr. Sabin is currently leading the Navy Medicine (NAVMED) IAVM Compliance Team, which includes successfully coordinating and executing more than 12 Communication Tasking Orders (CTOs), 300 IA Vulnerability Alerts/Bulletins (IAVA/Bs), etc. a year to Commands and Programs of Record (PORs). Within this capacity, Mr. Sabin and his team advance Enterprise-level IAVM by identifying requirements, developing intellectual capital and processes, training stakeholders, and coordinating execution activities necessary to achieve overarching compliance. In addition to his NAVMED Compliance Team lead role, Mr. Sabin supports various NAVMED IA functional activities to include Continuity of Operations (COOP), Certification and Accreditation (C&A), Organizational Resiliency, and institutionalization of tailored risk assessment and business impact analysis methodologies (consistent with industry best practices, NIST guidelines, regulations and emerging techniques from academia and industry). As pertains to COOP support, Mr. Sabin led the design, communication, training, proliferation, and assessment for an Enterprise-wide initiative focused on institutionalizing IT Contingency Planning (ITCP) and Disaster Recovery. Mr. Sabin has specific domain experience in information assurance and resiliency, risk management techniques, program and project management, budget management, communications law and policy, information technology,

Mr. Joseph Sabin, Esq., CISSP, FQNV, CBCP, CRISC
***Director, Federal IA Programs*, Security Risk Solutions, Inc.**

business operations and development, team leadership, and personnel management.

Booz Allen Hamilton
Associate *(2003 – 2008)*
As an Associate with Booz Allen Hamilton, Mr. Sabin managed numerous IA and Risk Analysis support projects (e.g., policy development awareness, training, key management, business continuity, incident response, IT policy, configuration management) for several Federal departments, agencies, and services such as Health and Human Services (HHS) Centers for Disease Control and Prevention's (CDC), Air Force Space Command (AFSPC), Missile Defense Agency (MDA), and U.S. Army. More specifically, Mr. Sabin led and conducted risk assessment support to HHS CDC. Mr. Sabin also provided policy and process development support to the MDA in numerous disciplines to include Contingency Planning, NetOps, and Privileged Account Management. For AFSPC, Mr. Sabin led a 14 person team in support to all areas of IA management (e.g., C&A, COMSEC, EMSEC, FISMA reporting, guidance and process development). Mr. Sabin also supported the U.S. Army as it upgraded Non-Tactical Land Mobile Radio at all CONUS installations in response to narrowband mandates, and by correlation to technology advances, compliance with pertinent DoD security requirements (e.g., DITSCAP, DIACAP, DoDI 8500.2).

Various Law and Policy Associate and Internships *(2001 – 2003)*
Mr. Sabin next completed his Juris Doctor while also working as an intern and/or associate with six policy and law organizations to include Booz Allen Hamilton; the Media Access Project; the National Association of Broadcasters; Mintz, Levin, Cohn, Ferris, Glovsky, and Popeo; the Federal Communications Commission, and the U.S. House of Representatives Subcommittee on Telecom and the Internet. Within these semester and summer-long opportunities, Mr. Sabin supported myriad legal research, drafting, and advocacy roles and responsibilities.

Booz Allen Hamilton
Senior Consultant *(1996 – 2001)*
Mr. Sabin led a technology awareness function that included coordinating staff and a suite of seven programs focused on promoting staff and client familiarity with emerging technology development across 17 categories. These programs ranged from showcase lab space to audio news magazines to seminar series. Mr. Sabin was also responsible for channeling information to 7,000+ staff via communication tools such as an intranet web presence, email publications, internal advertisements, tours and presentations, and 33 information media libraries.

U.S. Army *(1990 – 1996)*
Mr. Sabin served in the U.S. Army for six years to include duty assignments at the American Forces Korea Network (AFKN) and the White House Communications Agency (WHCA). While serving with AFKN, Mr. Sabin rose to the level of Newscast Director, coordinating personnel, equipment, and events for daily newscasts viewed by an average audience of more than 750,000. In 1992, Mr. Sabin earned an assignment with WHCA where he achieved the position of Audio-Visual Director for Presidential and Vice Presidential Events. Related duties included directing WHCA personnel and coordinating vendor support to produce sound, lighting and press distribution systems for Presidential events ranging from press briefings to 50,000 person international events. Mr. Sabin further traveled with and provided direct communications support to two U.S. Presidents and one Vice President.

Certifications, and Affiliations

Certifications and Credentials

- Navy Certification Authority Fully Qualified Navy Validator (FQNV)
- Certified Information Systems Security Professional (CISSP)
- Certified Business Continuity Professional (CBCP)
- Certified in Risk and Information Systems Control (CRISC)
- Foundations Certificate in IT Service Management (ITIL v.2)

Ronald L. Krutz, Ph.D., P.E., CISSP, ISSEP
Chief Scientist, Security Risk Solutions

EDUCATION

INSTITUTION AND LOCATION	DEGREE	YEAR(S)	FIELD OF STUDY
University of Pittsburgh	BSEE	1961	Electrical Engineering
University of Pittsburgh	MSEE	1967	Electrical Engineering
University of Pittsburgh	Ph.D. EE/Computer Engineering	1972	Electrical and Computer Engineering

QUALIFICATIONS SUMMARY

Dr. Krutz has over 30 years experience in government and industrial research and development, academia, and the commercial electrical engineering and computer engineering fields. He has capabilities in information assurance, certification and accreditation,, CISSP and ISSEP course development and teaching, computer architectures, real-time systems, SCADA systems security, security awareness training, information security standards, HIPAA, the HITECH Act, SSE-CMM (Systems Security Engineering Capability Maturity Model), and assessment methodologies. He also developed the HIPAA-CMM, adapting the HIPAA Privacy, Security, and Code Sets Rules to the Capability Maturity Model paradigm. While at BAE Systems, he conducted a HIPAA assessment using the Model for Medstar Health. He also recently developed course material detailing the critical elements of the HITECH Act.

He held senior research positions at the Gulf R&D Laboratories, Singer R&D Laboratories, Lockheed Martin Corporation, BAE Systems, and Threatscape Solutions. Dr. Krutz was a professor in the Carnegie Mellon University Department of Electrical and Computer Engineering and Associate Director of the Carnegie Mellon Research Institute. He also served as an Officer in the U.S. Army Ordnance Corp.

Dr. Krutz has authored or co-authored 16 texts in the area of information system security. He also developed the patent-pending Computer Forensics CMM for Lockheed Martin. Dr. Krutz was a lead instructor for ISC2 CISSP certification review seminars. He was a Distinguished Visiting Lecturer in the University of New Haven Henry C. Lee College of Criminal Justice and Forensic Sciences (delivered CISSP courses at Sandia Labs and Lawrence Livermore) and a Senior Lecturer at the California Sciences Institute. He is also a Senior Fellow of the International Cyber Center of George Mason University.

Dr. Krutz is a Life Senior Member of IEEE, a Registered Professional Engineer, holds the CISSP and ISSEP Certifications, and has been awarded 7 patents in the area of digital systems.

EXPERIENCE SUMMARY

Security Risk Solutions, Inc.
Chief Scientist *(2010 to present)*
As part of the SPAWAR NAVMISSA Continuous Risk Management team, Dr. Krutz has worked on modifying and enhancing the SRS proprietary risk management framework (RMF), providing expertise in the incorporation of NIST SP 800-53, DoDI 8500.2, HIPAA, and other standards and guidelines. Other efforts include review and evaluation of STIGS, SSA's, and other relevant DoD and Navy publications. He has contributed material to revisions of assurance documents such as the Medical Devices STIG, developed training materials related to HIPAA and the HITECH Act, and

Ronald L. Krutz, Ph.D., P.E., CISSP, ISSEP
Chief Scientist, Security Risk Solutions

authored white papers on a variety of information assurance-related topics.

ThreatScape Solutions, Inc. (formerly Cybrinth, LLC)
Chief Technical Officer and Infosec Consultant - *(2007-2010)*

Dr. Krutz provided research, analytic, and strategic support to the corporation in the field of information systems security, privacy, SCADA and industrial control system security, risk analysis, cryptography, capability maturity model (CMM) development, and assessment methodologies. In this position, he investigated and evaluated new technologies, developed proposals and white papers, and provided recommendations for future technological investment. He also worked on special information security projects for financial institution customer and evaluated strengths of various cryptographic systems.

Lockheed Martin/The Sytex Group, Advanced Technology Research Center
Senior Infosec Consultant *(2003-2007)*

Dr. Krutz worked on privacy issues, information security research, security assessment methodologies, SCADA system security, computer forensics, wireless security, Infosec course development, developing white papers, digital rights management, and strategic planning. He developed the Computer Forensics CMM.

BAE Enterprise Systems/Corbett Technologies
Senior Technical Staff *(2000-2003)*

Dr. Krutz had responsibilities for CISSP Infosec course development, proposal development, privacy, information security, HIPAA Privacy and Security assessment methodologies (including HIPAA-CMM, which he developed), SSE-CMM, BS7799, Common Criteria, authoring white papers, strategic planning, proposal development, and marketing support.

Carnegie Mellon University
Faculty and Associate Director, Carnegie Mellon Research Institute *(1975-2000)*

Dr. Krutz was a professor in the ECE Department of Carnegie Mellon University. In this capacity, he developed and taught courses and conducted funded research in the areas of digital design, real-time systems, control theory, distributed computing architectures, hardware descriptive languages, and information systems security. He supervised research programs of graduate students working toward their Masters and Ph.D. degrees and published a variety of technical papers. He then established the Computer Engineering Center of the Carnegie Mellon Research Institute (CMRI) and conducted and supervised research is areas such as AI, modeling and simulation, real-time systems, SCADA systems, information security, software process improvement and control systems. Dr. Krutz also founded the CMRI Cybersecurity Center and was Associate Director of CMRI.

Certifications, and Affiliations

Certifications

- Registered Professional Engineer in Pennsylvania
- CISSP
- ISSEP
- Life Senior Member, IEEE

Publications

Dr. Krutz has published over 40 technical papers and co-authored the following information systems security books from 2000 to 2011 for John Wiley and Sons:

- *The CISSP Prep Guide*
- *The CISSP Prep Guide, Advanced Q&A*

Ronald L. Krutz, Ph.D., P.E., CISSP, ISSEP
Chief Scientist, Security Risk Solutions

- *The CISSP Prep Guide, Gold Edition*
- *The Security+ Prep Guide*
- *The CISM Prep Guide*
- *The CISSP Prep Guide, 2nd Edition: Mastering CISSP and ISSEP*
- *The Network Security Bible 8. The CISSP and CAP Prep Guide, Platinum Edition: Mastering CISSP and CAP*
- *Securing SCADA Systems*
- *Certified Ethical Hacking (CEH) Prep Guide*
- *Network Security Fundamentals*
- *Project Manual--Network Security Fundamentals*
- *The CSSLP Prep Guide.*
- *Cloud Computing Security*
- *Web Commerce Security.*

He also authored two university texts on microprocessors and logic design and digital interfacing techniques for John Wiley & Sons, and recently authored *Industrial Automation and Control System Security Principles* for the International Society of Automation (ISA) (2013.)

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

Mr. Bret Peresich, FQNV, CISSP, CISA, OSCP
Project Lead for IA Controls Verification and Validation Team, Athena Consulting Group, LLC

Education

INSTITUTION AND LOCATION	DEGREE	YEARS	FIELD OF STUDY
Strayer University, Charleston, SC	BS	2009	Computer Information Systems/Computer Security

Qualifications Summary

Mr. Peresich has demonstrated experience with military and government agencies with hands-on technical work and project management, as well as working directly with customers in a consulting capacity. He has coordinated and directed teams involved in security test and evaluation (ST&E) for system Certification and Accreditation (C&A) package development, risk assessments, HIPAA/HITECH regulatory compliance, server and workstation migration for Navy and Marine Corps Intranet (NMCI), and server deployments, with an emphasis on learning solutions and end-user support. Mr. Peresich has excellent technical, communication, presentation, and customer service skills. He is a resourceful problem solver with proven ability to bring quick resolution to challenging situations. His management background includes leading teams, developing and managing budgets, devising timelines, monitoring project standards for all deliverables, creating strategies, overseeing technical design and development of all learning solutions, new business development, documentation, development of training curriculum, conducting training, and maintaining quality assurance.

Mr. Peresich is an experienced network vulnerability and penetration tester, and compliance consultant. He provides technical security expertise and C&A program management and program leadership to multiple, concurrent healthcare programs, including:

- Navy Medicine Enterprise Information Assurance Security Test and Evaluation
- Navy Medicine Enterprise Information Assurance Independent Verification and Validation Testing

He is a Navy Certification Authority (CA) Fully Qualified Navy Validator (FQNV), authorized to make certification determination recommendations to the Designated Approving Authority on whether Navy Information Systems and Enclave Networks should be granted an Accreditation for Authority to Operate (ATO). He is a Certified Information Systems Security Professional (CISSP), accredited by the International Information Systems Security Certification Consortium and is a Certified Information Security Auditor (CISA) as accredited by the Information Systems Audit and Control Association (ISACA). He is a certified penetration tester with the Offensive Security Certified Professional as accredited by Offensive Security.

Experience Summary

Athena Consulting Group, LLC (2005 – Present)
RL Phillips, LLC (2002 – 2006)
Project Lead
Navy Medicine Information Systems Support Activity (NAVMISSA) (Contractor)

Mr. Peresich provides senior level advice and guidance on technical problems, solutions and challenges as they relate to the Navy Medicine Information Assurance environment. He conducts risk assessments and delivers findings and reports to senior level management. He also prepares and submits whitepapers, position papers and briefs explaining technical issues to senior leadership.

Mr. Peresich is currently the project lead for the Navy Medicine Enterprise Information Assurance Independent Verification and Validation (IV&V) and Security Test and Evaluation (ST&E) Team; ensuring compliance with DoD, DoN, and HIPAA/HITECH regulations. He developed the Test Team Standard Operating Procedures as well as the custom vulnerability reporting tools.

He serves as the project lead for the Secure Compliance Tool Suite Deployment Team. Mr. Peresich developed the Navy Medicine Concept of Operations (CONOPS) and Standard Operating Procedures (SOP) for SCCVI-SCRI implementation. He developed the cost estimate to deploy the Secure Compliance Tools Suite throughout Navy Medicine sites and developed the Secure Configuration Compliance Validation Initiative-Secure Configuration

Mr. Bret Peresich, FQNV, CISSP, CISA, OSCP
Project Lead for IA Controls Verification and Validation Team, Athena Consulting Group, LLC

Remediation Initiative (SCCVI-SCRI) deployment strategy for Navy Medicine.

Space and Naval Warfare Systems Center Atlantic (Civilian)
Network Technician DT-0856-2 (2000-2002)

Mr. Peresich chaired the Security Working Groups for NMCI Legacy Application migration efforts. He developed processes and procedures for the Legacy Applications Quarantine Reduction Team and developed processes and procedures for the Information Management Team. He served as Technical Lead for Legacy Applications Quarantine Reduction and conducted Legacy Systems Security Improvement Pilot at NAVAIR Orlando. Mr. Peresich installed Securify SecurVantage for network traffic monitoring and analysis and 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. He was also the quick Look Assessment Lead Technical Advisor. Mr. Peresich developed processes and procedures for Information Assurance Tiger Team (IATT) Quick Look Assessment Teams. He conducted port and protocol analysis for network communication of legacy applications within the Department of the Navy and worked with sites to develop accurate server lists based on network mapping. He also 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, and advised of the Legacy Systems Transition Guide and the System Transition Engineering Review Questionnaire for the NMCI Legacy Systems Security Improvement pilot.

United States Navy, Petty Officer First Class Fire Controlman (1988-1998)

Mr. Peresich served on board the USS Nicholas (FFG-47) from 1990-1995. During that time he maintained and troubleshot the MK92 Mod 2 Fire Control Weapons System (FCS) and the AN/SWG Harpoon Weapon System Console. He was a watch stander on MK92 FCS and Harpoon Console in Combat Information Center (CIC). He was a member of the Damage Control Training Team and the Combat Systems Training Team. He participated in Operation Desert Shield and Desert Storm; earning a Combat Action Ribbon. From 1995 to 1998 he was stationed at the Bureau of Naval Personnel (BUPERS) in Washington, DC. His responsibility was the Fire Controlman Schools Detailer. He was 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. He developed a Branch checkbook application to automate personnel and budget accounting for $25M+ budget, saving hundreds of man hours of work.

Certifications, and Affiliations

Certifications

- Navy Certification Authority Fully Qualified Navy Validator (FQNV)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Offensive Security Certified Professional (OSCP)

Affiliations

- Armed Forces Communications and Electronics Association (AFCEA)
- International Information Systems Security Certification Consortium ((ISC)2)

Mr. Bret Peresich, FQNV, CISSP, CISA, OSCP
Project Lead for IA Controls Verification and Validation Team, Athena Consulting Group, LLC

Education

INSTITUTION AND LOCATION	DEGREE	YEARS	FIELD OF STUDY
Strayer University, Charleston, SC	BS	2009	Computer Information Systems/Computer Security

Qualifications Summary

Mr. Peresich has demonstrated experience with military and government agencies with hands-on technical work and project management, as well as working directly with customers in a consulting capacity. He has coordinated and directed teams involved in security test and evaluation (ST&E) for system Certification and Accreditation (C&A) package development, risk assessments, HIPAA/HITECH regulatory compliance, server and workstation migration for Navy and Marine Corps Intranet (NMCI), and server deployments, with an emphasis on learning solutions and end-user support. Mr. Peresich has excellent technical, communication, presentation, and customer service skills. He is a resourceful problem solver with proven ability to bring quick resolution to challenging situations. His management background includes leading teams, developing and managing budgets, devising timelines, monitoring project standards for all deliverables, creating strategies, overseeing technical design and development of all learning solutions, new business development, documentation, development of training curriculum, conducting training, and maintaining quality assurance.

Mr. Peresich is an experienced network vulnerability and penetration tester, and compliance consultant. He provides technical security expertise and C&A program management and program leadership to multiple, concurrent healthcare programs, including:

- Navy Medicine Enterprise Information Assurance Security Test and Evaluation
- Navy Medicine Enterprise Information Assurance Independent Verification and Validation Testing

He is a Navy Certification Authority (CA) Fully Qualified Navy Validator (FQNV), authorized to make certification determination recommendations to the Designated Approving Authority on whether Navy Information Systems and Enclave Networks should be granted an Accreditation for Authority to Operate (ATO). He is a Certified Information Systems Security Professional (CISSP), accredited by the International Information Systems Security Certification Consortium and is a Certified Information Security Auditor (CISA) as accredited by the Information Systems Audit and Control Association (ISACA). He is a certified penetration tester with the Offensive Security Certified Professional as accredited by Offensive Security.

Experience Summary

Athena Consulting Group, LLC (2005 – Present)
RL Phillips, LLC (2002 – 2006)
Project Lead
Navy Medicine Information Systems Support Activity (NAVMISSA) (Contractor)

Mr. Peresich provides senior level advice and guidance on technical problems, solutions and challenges as they relate to the Navy Medicine Information Assurance environment. He conducts risk assessments and delivers findings and reports to senior level management. He also prepares and submits whitepapers, position papers and briefs explaining technical issues to senior leadership.

Mr. Peresich is currently the project lead for the Navy Medicine Enterprise Information Assurance Independent Verification and Validation (IV&V) and Security Test and Evaluation (ST&E) Team; ensuring compliance with DoD, DoN, and HIPAA/HITECH regulations. He developed the Test Team Standard Operating Procedures as well as the custom vulnerability reporting tools.

He serves as the project lead for the Secure Compliance Tool Suite Deployment Team. Mr. Peresich developed the Navy Medicine Concept of Operations (CONOPS) and Standard Operating Procedures (SOP) for SCCVI-SCRI implementation. He developed the cost estimate to deploy the Secure Compliance Tools Suite throughout Navy Medicine sites and developed the Secure Configuration Compliance Validation Initiative-Secure Configuration

Mr. Bret Peresich, FQNV, CISSP, CISA, OSCP
Project Lead for IA Controls Verification and Validation Team, Athena Consulting Group, LLC

Remediation Initiative (SCCVI-SCRI) deployment strategy for Navy Medicine.

Space and Naval Warfare Systems Center Atlantic (Civilian)
Network Technician DT-0856-2 (2000-2002)

Mr. Peresich chaired the Security Working Groups for NMCI Legacy Application migration efforts. He developed processes and procedures for the Legacy Applications Quarantine Reduction Team and developed processes and procedures for the Information Management Team. He served as Technical Lead for Legacy Applications Quarantine Reduction and conducted Legacy Systems Security Improvement Pilot at NAVAIR Orlando. Mr. Peresich installed Securify SecurVantage for network traffic monitoring and analysis and 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. He was also the quick Look Assessment Lead Technical Advisor. Mr. Peresich developed processes and procedures for Information Assurance Tiger Team (IATT) Quick Look Assessment Teams. He conducted port and protocol analysis for network communication of legacy applications within the Department of the Navy and worked with sites to develop accurate server lists based on network mapping. He also 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, and advised of the Legacy Systems Transition Guide and the System Transition Engineering Review Questionnaire for the NMCI Legacy Systems Security Improvement pilot.

United States Navy, Petty Officer First Class Fire Controlman (1988-1998)

Mr. Peresich served on board the USS Nicholas (FFG-47) from 1990-1995. During that time he maintained and troubleshot the MK92 Mod 2 Fire Control Weapons System (FCS) and the AN/SWG Harpoon Weapon System Console. He was a watch stander on MK92 FCS and Harpoon Console in Combat Information Center (CIC). He was a member of the Damage Control Training Team and the Combat Systems Training Team. He participated in Operation Desert Shield and Desert Storm; earning a Combat Action Ribbon. From 1995 to 1998 he was stationed at the Bureau of Naval Personnel (BUPERS) in Washington, DC. His responsibility was the Fire Controlman Schools Detailer. He was 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. He developed a Branch checkbook application to automate personnel and budget accounting for $25M+ budget, saving hundreds of man hours of work.

Certifications, and Affiliations

Certifications

- Navy Certification Authority Fully Qualified Navy Validator (FQNV)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Offensive Security Certified Professional (OSCP)

Affiliations

- Armed Forces Communications and Electronics Association (AFCEA)
- International Information Systems Security Certification Consortium ((ISC)2)

Mr. Brandon Friesner, MS, CISSP, Security +, CCNA
Senior Information Assurance Professional, Security Risk Solutions, Inc.

Education

INSTITUTION AND LOCATION	DEGREE	YEARS	FIELD OF STUDY
Park University, Parkville, MO	B.S.	2008	Management/Computer Information Systems
Southern Methodist University, Dallas, TX	M.S.	2011	Systems Engineering

Qualifications Summary

Mr. Friesner is a technically proficient and decisive senior information assurance professional offering over 13 years of experience in Information security and risk management. He is well-versed in network security testing, certification and accreditation (C&A), risk analysis development, reporting, and security policy execution. Mr. Friesner is highly knowledgeable in the interpretation, evaluation, and implementation of Federal regulations and guidelines, including FISMA, HIPAA/HITECH, OMB Circular A-130, NIST SP-800 Series, FIPS, and DoD 8500 Series. He has a proven ability to build, lead, and mentor highly technical engineering and analytical teams to meet organizational goals and objectives. He is recognized for the ability to realize the "big picture" and work closely with senior management to develop Enterprise security strategy and management programs in highly dynamic and complicated environments. Mr. Friesner is regarded as an analytical, diplomatic, and detail oriented professional with the ability to effectively communicate technical and business perspectives, both orally and in writing.

Areas of expertise include business continuity, C&A, CMMI, configuration management, DIACAP, enterprise architecture, incident response, information assurance, HIPAA/HITECH, IT contingency planning, IT policy/governance, OCTAVE®, process improvement, project management, requirements management, risk management, security test and evaluation, strategic planning, systems security engineering, TCP/IP, technical leadership, telecommunications and network security, vulnerability management.

Experience Summary

Mr. Friesner received his Bachelor of Science, Management Information Systems, from Park University, Parkville, Missouri as well as a Master of Science, Systems Engineering, from Southern Methodist University, Dallas, Texas. Prior to his civilian career, Mr. Friesner served as a Tactical Network Specialist in the United States Marine Corps (USMC). Mr. Friesner currently holds the Certified Information Systems Security Professional (CISSP), Security +, and Cisco Certified Network Associate (CCNA) certifications and has completed the Navy Defense Information Assurance Certification and Accreditation Process (DIACAP) Validator Course and the Software Engineering Institute (SEI) Introduction to CMMI Version 1.2 training. As a Senior Information Assurance Professional, he assists organizations with the development and implementation of information security programs including information security needs analysis, HIPAA/HITECH regulatory compliance, organizational resiliency planning and institutionalization of Risk Assessment and Business Impact Analysis methodologies. He currently serves both the Navy Medicine Enterprise Information Assurance Continuous Risk Management and Information Technology Continuity Planning tasks as a subject matter expert focusing on the development and institution of an 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 also provides information security consulting services to the Centers for Medicare and Medicaid Services (CMS), Comparative Billing Reports (CBR) Producer system. In this capacity, he is responsible for the assessment and implementation of administrative, technical, and operational IA controls to ensure confidentiality, integrity, and availability of the CBR system and the sensitive information which it processes. Mr. Friesner currently serves as the Information System Security Officer (ISSO) for the Army National Guard (ARNG) Electronic Security System (ESS) Program. Responsibilities include oversight and execution of Certification and Accreditation activities, Configuration Management, Risk Management, security testing and evaluation and security architecture design. He has previously supported numerous programs with National Institutes of Health (NIH) and National Organization for Rare Disorders (NORD) providing subject matter expertise with an emphasis on the evaluation and successful implementation of organizational, NIST 800-53 and HIPAA/HITECH security requirements. Mr. Friesner assisted the Charleston County Aviation Authority (CCAA) with technical and non-technical information security services in an

Mr. Brandon Friesner, MS, CISSP, Security +, CCNA
Senior Information Assurance Professional, Security Risk Solutions, Inc.

effort to validate compliance with industry best practices for Information Security, including domain specific requirements such as those specified in the PCI DSS. He provided recommendations which enabled CCAA to implement an effective information security program, while at the same time close the gaps identified specifically the PCI review. As a Navy Civilian, he was designated as the Information Assurance Manager (IAM) and Submitting Trusted Agent (STA) for the Navy Medicine Enterprise Services Operations Center (ESOC). In this role, he was responsible for the execution and implementation of Certification and Accreditation, DoD 8500.2, Public Key Infrastructure (PKI), Configuration Management, Information Assurance Vulnerability Management (IAVM), Incident Response, and Risk Management activities. The following projects highlight specific experience with relevance to Healthcare HIPAA Security and Privacy experience:

Navy Medicine Enterprise Information Assurance Program
Information Technology Contingency Planning Subject Matter Expert *(February 2013-present)*
Continuous Risk Management Subject Matter Expert *(March 2012-present)*
Mr. Friesner ensures the continuity of Navy Medicine (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) develop and exercise IT Contingency Plans (ITCPs) to comply with Federal /departmental policies and guidelines (e.g., FISMA, DoDI 8500.2, NIST, HIPAA/HITECH). He identifies areas of improvement for selected Enclaves and PORs via after action reports (AARs) and plans of action and milestones (POA&Ms).
Mr. Friesner focuses on the development and institution of an 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 as part of an Enterprise-wide Continuous Risk Management Program.

National Guard Bureau (NGB) Electronic Security Systems (ESS) Program
Information Systems Security Officer *(March 2012-present)*
Mr. Friesner independently manages and executes the C&A process for version 2.0 of the type-accredited system, successfully achieving a three year ATO. 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. Mr. Friesner has developed, instituted, and currently oversees IS configuration management and DIACAP sustainment activities for ESS Version 2.0.

Charleston County Aviation Authority (CCAA)
Information Security Risk Management Consultant *(March 2012-February 2013)*
Mr. Friesner provides information security services to the CCAA. He has authored the CCAA Information Security Framework, which provides an overview and comparative analysis of three frameworks tailored to meet the needs of CCAA, demonstration of the recommended Information Security Framework, and an explanation of activities required to implement the Information Security Framework. 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. Mr. Friesner included a totality of controls applicable to remediation and improvement of the CCAA security posture in the form of an Information Security Framework matrix to support the mitigation process. 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.

National Organization of Rare Disorders (NORD)
Information Security Subject Matter Expert *(May 2012-November 2012)*
Mr. Friesner assists 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 outlines the baseline security controls based on the requirements

Mr. Brandon Friesner, MS, CISSP, Security +, CCNA
Senior Information Assurance Professional, Security Risk Solutions, Inc.

specified in the HIPAA Security Rule/HITECH and suggested security controls defined in NIST SP 800-53. He is also responsible for the development and institution of the NORD MAP System Security Plan.

National Institutes of Health (NIH)
Information Security Subject Matter Expert *(May 2012-November 2012)*
Mr. Friesner previously supported numerous programs with National Institutes of Health (NIH) providing subject matter expertise, specifically the Safety Reporting Portal (SRP) and the Genetic Modification Clinical Research Information System (GeMCRIS), with an emphasis on the evaluation and successful implementation of organizational, NIST 800-53 and HIPAA/HITECH security requirements.

Space and Naval Warfare (SPAWAR) Systems Center Atlantic
Information Technology Specialist *(2009-2012)*
Navy Medicine Information Assurance Manager (IAM) *(2010-2012)*
NAVMED Lead Project Engineer/Technical Risk Manager *(2009-2010)*
Mr. Friesner served as IAM for the NAVMED Enterprise Services Operations Center. His duties also included the management and execution of the NAVMED 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 C&A process for NAVMED networks and information systems located at SPAWAR Atlantic and Enterprise deployed PORs. His efforts resulted in NAVNED 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 assesses 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.
Mr. Friesner was 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. His responsibilities included the management of the Enterprise IA Technical Projects functional teams, assignment and prioritization of tasks, reviewing deliverables, supplying metrics to Senior Leadership, and identification, tracking, and escalation of functional risks. With support from his teams, he developed and maintained common risk impact criteria for centrally managed assets, to include the NAVMED Enterprise Services, NitroView System Information and Event Management (SIEM), Riverbed Steelhead WAN Network Optimization, and Network Protection Suite PORs, 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 NAVMED Cyber CERT functions.

Science Applications International Corporation (SAIC)
NAVMED Lead Project Engineer *(2007-2009)*
NAVMED Enterprise Engineering and Technical Services Team *(2005-2007)*
As the Technical and Engineering Lead for the Navy Medicine Enterprise Host Based Security System (HBSS) project, assisting the Project Manager in the 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

Mr. Brandon Friesner, MS, CISSP, Security +, CCNA
Senior Information Assurance Professional, Security Risk Solutions, Inc.

documentation, and management of personnel.

Mr. Friesner supported the NAVMED 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 IA consulting services to NAVMED. While supporting the Engineering and Technical Services Team, Mr. Friesner successfully executed project management duties, concepts, and demonstrated ability to lead a team for a technical program that is dynamic and complex.

Mr. Friesner was responsible for the implementation and migration of an Enterprise Active Directory solution across NAVMED. His individual responsibilities include leading a deployment team of up to three engineers in order to meet critical deadlines associated with an aggressive migration schedule. Mr. Friesner administered network security and access devices, DNS, access control lists (ACLs), 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.

WareOnEarth Communications, Inc.
Network Engineer, Military Health Systems *(2003-2005)*

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), VPNs, IDSs, 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.

Certifications, and Affiliations

Certifications

- CompTIA Security+, June 2009
- Cisco Certified Network Associate (CCNA), August 2010, #404124168967CRDN
- Certified Information Systems Security Professional (CISSP), March 2011, #390098
- Defense Acquisition Workforce Improvement Act (DAWIA), Information Technology Level I

LINDA G. JENSEN
Senior Technical Writer, KRM Associates, Inc.

Education

INSTITUTION AND LOCATION	DEGREE	YEARS	FIELD OF STUDY
Capella University, Minneapolis, MN	BS (Summa cum Laude)	2010	Information Technology
Community Health Network of West Virginia, Scott Depot, WV		2007	Clinical Application Coordinator Training
USAF Technical School, Chanute AFB, IL	Honor Graduate	1976	Digital Flight Simulator Maintenance

Qualifications Summary

Information Technology

Extensive experience in testing and documenting software under development including both functionality and user utility. Familiarity with database design and maintenance. Also experienced in video and sound editing for both web and cd/dvd publication Expert user of Microsoft Office applications, including Word, Excel, PowerPoint, Project, FrontPage, as well as a myriad of other word-processing, media manipulation, web-development and instruction authoring applications.

Healthcare Applications:

Supported the creation of OSEHRA, developing certification standards and procedures and engaging the healthcare community strategies for Stage 2 Meaningful Use certification. Assisted with in-depth research into the attitudes toward and interactions with healthcare applications by both care providers and patient users. Familiar with the processes for preparing users to implement electronic healthcare applications and the requirements for customizing and personalizing systems for effective deployment. Intimately acquainted with the process and pitfalls – functional, technical, legal, and attitudinal – of developing and deploying an electronic system for collecting and displaying personal identity and health data.

Technical Writing

Performs all phases of writing, editing and publishing technical manuals, including: analysis of procedures, reading and interpreting engineering drawings and schematics, determining step-by-step procedures and corrective actions, writing both quick reference lists and detailed narratives, editing for content, grammar and style, verifying procedures and performing routine updates and changes.

Instructional Systems Design

Uses a systematic approach of analysis, review, revision and post-implementation feedback to design, develop, implement, and manage highly effective computer- or web-based interactive instructional programs for a wide variety of topics. Has a facility for identifying and meeting critical training needs in any field of endeavor.

On-the-Job Training

Design and deliver OJT training to individuals and groups, coaching and mentoring use of computer applications, specialized tools (such as HIT applications) and 'Soft' skills (leadership, diversity awareness, sexual harassment, security).

LINDA G. JENSEN
Senior Technical Writer, KRM Associates, Inc.

Experience Summary

Ms. Jensen is an intuitive problem-solver who grasps the big picture and effectively communicates solutions. Her extensive experience in technical writing, instructional systems design and implementation, digital video editing, computer-based training development, quality assurance, and training program management across a variety of industries, from the military to healthcare, allows her to rapidly assess and identify potential problem areas along with probable remedial activity.

Building on a solid foundation of electronics and computer theory acquired as an active duty Non-Commissioned Officer in the US Air Force, she used her facility for written communication to become an accomplished technical writer, working alongside design engineers and interpreting system diagrams to write comprehensive troubleshooting and repair manuals, as well as user guides and system checklists for weapons systems, railroad braking and control systems, integrated metals refining and alloying processes, retail sales and inventory systems, and, most recently, healthcare applications.

Working in and around sensitive industries has honed Ms. Jensen's knowledge of, and attention to, security requirements and procedures, and she has developed and presented numerous training courses on the subject.

KRM, Inc., Shepherdstown, WV
Senior Technical Writer (2011 – Present)
Support of the Open Source Electronic Health Record Agency, taking custody of the VA's VistA software and devising methodologies to safeguard, update, modify, and certify software for use by the VA and any other entity desiring to deploy VistA. Support of Shepherd University's Nursing Informatics curriculum with classroom presentation of PHR system. Writing proposals. Supporting the NEBOSS contract at the VA National Security Operations Center, writing procedure and policy manuals. Obtained Public Trust Security Clearance.

Shepherd University Research Corporation, Shepherdstown, WV
ADPAC (2009 - 2010)
Contract position supporting a multiyear Medicaid Transformation Grant initiative to pilot both Electronic Medical Record and Personal Health Record systems for use by care providers in the state of West Virginia, including surveys; user training development and delivery, technical assistance, and project coordination.

- For the Student Health Center EHR pilot deployment:
    - Coordinated with university administration, IT department, and Health Center staff to minimize disruption
    - Performed pre-implementation assessments
    - Configured installed system with required notes templates, custom treatment orders, and scheduling schema
    - Developed and delivered training for staff in use of system and security requirement
    - Provided hands on training and assistance during implementation period
    - Transferred paper records for all (~400) returning students with a history of using health Center services

LINDA G. JENSEN
Senior Technical Writer, KRM Associates, Inc.

  - Gathered feedback and assisted in preparing a report on the success of the implementation
- General contract support, including monthly, quarterly, and final reports

KRM, Inc., Shepherdstown, WV
Independent Contractor, Technical Writer (2005 – 2009)
Working under a series of task orders, provided:

- Support of Medicaid Transformation Grant initiatives to pilot Electronic Medical Records, Personal Health Records and Health Information Exchange systems for use by care providers in the state of West Virginia, including:
  - surveys;
  - monthly and quarterly reporting,
  - website and application design,
  - training, and project coordination.
- Support a 6 month project to certify and accredit security for all (500+ systems in more than 200 locations) Veteran's Health Administration computer systems. All systems certified on schedule and $1.2M under budget.
  - Document the repeatable process for continuous monitoring of the systems.
  - Prepare presentations, checklists, tracking spreadsheets.
  - Package on cdrom and submit for approval final reports.
- Test, evaluate, and document a Web-enabled IT Security Assessment tool prior to roll-out implementation by the DOD.
- Design corporate marketing brochure.

Giant Eagle, Inc., Pittsburgh, PA
Training Specialist (2002 – 2004)
Design, develop and implement policy and procedures training for employees, using both traditional classroom and web-based training media.

- Write and publish company training manuals and training aids.
- Design web-based applications for financial reporting.
- Member of Corporate Shrink Committee, the body responsible to identify sources of loss within the company
  - Devise and implement policies and procedures to curtail losses
  - Savings of more than $2,000,000 realized in 2003

NCR, Rockville, MD
Contract Instructional Designer (2001 - 2001)
Design and implement computer-based training CDs for a contract with the US Postal Service, teaching operation and maintenance of the Point-Of-Service (POS) system. Project manager for a pilot web-based training program to reduce the cost of reproducing and distributing CDs and printed manuals for quarterly system updates.

Union Switch and Signal Inc., Pittsburgh, PA
Engineering Systems Specialist (1999 - 2000)
Manage training portion of contracts, with an average training value of .5 to 1.5 million dollars,

LINDA G. JENSEN
Senior Technical Writer, KRM Associates, Inc.

including:

- writing proposals,
- creating budget estimates,
- contracting for temporary workers,
- establishing schedules,
- managing personnel assignments and budgets,
- reviewing engineering proposals to ensure all training requirements are met,
- assisting in the design, writing, review, editing and publishing of all system manuals, training documents and instructional aids,
- arranging for translation services for foreign language contracts.

ASE Limited, Pittsburgh, PA
Instructional Design (1998 - 1999)
As training Team Lead, design and implement embedded training in the integrated production line at the INCO facility in West Virginia. Also provided computer skills introduction and upgrade training for INCO personnel. An additional project was to script, edit and publish a local cable commercial spot for Mt. Lebanon, PA's First Night 1999 celebration.

GEC Marconi Dynamics, Lancaster, PA
Instructional Systems Design (1995 to 1996
As training Team Lead, design, develop and implement training for the United Arab Emirates Air Force in the operation and maintenance of weapons systems bought under contract with the US Navy.

Required Secret security clearance.

Northrop Grumman, Inc., Bethpage, NY, Instructional Design Engineer (1985 - 1995)
Design, develop, debug and implement computer-based interactive training. Research, write, edit and publish technical manuals for users and maintainers of company products, including aircraft, weapons systems and simulators. All documentation created to U.S. military specification standards.

Required Secret – or above - security clearance.

U. S. Air Force
Non-commissioned Officer in Charge, F-4E Flight Simulator (1976 – 1985)
Honorable Discharge
Supervise up to 15 subordinate enlisted personnel, plan and implement operations and maintenance schedules, manage operations and maintenance budget, perform daily operations and maintenance, train subordinates in duty requirements, maintain technical library, specify and recommend engineering changes and upgrades to equipment, write annual performance reviews, write and submit daily, weekly and monthly status reports. Required Secret (NoForn) security clearance.

Certifications, and Affiliations

Affiliations

- Member of OSEHRA
- Member of WorldVistA

Mr. James McAlister, MSc, PMP, Sec+
Program Risk and Quality Manager, Security Risk Solutions, Inc.

Education

INSTITUTION AND LOCATION	DEGREE	YEARS	FIELD OF STUDY
Georgetown University, School of Foreign Service Washington, DC	BS (Bachelor of Science)	1993	International Relations
London School of Economics and Political Science London, England	MSc (Master of Science)	1998	International Relations

Qualifications Summary

Mr. McAlister possesses 20 years of experience working with both public and private sector organizations, demonstrating proven skills and expertise in the areas of information assurance and security, risk management, healthcare regulation, and project management. Functionally, he focuses primarily on process improvement, technology solutions, and change management.

Experience Summary

Space and Naval Warfare Systems Center Atlantic

Navy Medicine Enterprise Information Assurance Compliance Team *(June 2012 – present)*

Since June of 2012, Mr. McAlister has served as a Compliance Coordinator for the Department of Defense Navy Medicine Enterprise. As part of the overall Navy Medicine Information Assurance (IA) effort, he is responsible for tracking and reporting on compliance with IA Vulnerability Management for Navy Medicine Commands and Programs of Record (PORs). He ensures that the field is aware of IA compliance requirements, deadlines, and available mitigation solutions. He coordinates with Navy Medicine Leadership when clarification on vulnerability notices is needed and supports Commands and PORs to achieve compliance. He works closely with other IA teams such as Certification and Accreditation (C&A) and Continuity of Operations (COOP) to ensure the desired risk posture for the Navy Medicine Enterprise is achieved. More specifically, Mr. McAlister Facilitates the inventory of up-to-date IAVM Plans for Commands and PORs, coordinates regular IA sustainment meetings between POR Management and associated User Commands, and supports the creation of new compliance policy and directives for use by Navy Medicine Leadership. He also serves as liaison between the Compliance and C&A Teams for POR IA sustainment activity, trains stakeholders in compliance reporting, and updates and maintains the Compliance Team Portal.

Space and Naval Warfare Systems Center Atlantic

Program Risk Manager, Veterans Affairs Sub-Portfolio *(2010-2012)*

Mr. McAlister served as Risk Manager at the Space and Naval Warfare (SPAWAR) System Center Atlantic's VA Program Support Office (PSO). He provided leadership, oversight, and direction for risk management activities for four Integrated Project Teams spanning some 23 VA projects with funded contract ceilings totaling in excess of $500 million. Projects supporting application development, web portal development, and benefits delivery include the Post 9/11 Veterans Benefits Program (Chapter 33) and implementation of the Veterans Benefit Management System (VBMS).

McAlister Consulting Company

Principal *(2006-2010)*

Mr. McAlister provided program management services for Wyeth Consumer Healthcare's initiative to ensure compliance of all product labels and mitigate risk of infraction against government regulations and internal standards, including CFR Part 11 (AER). He managed the label review work stream, facilitated review team meetings, prepared the project dashboard, and documented the risk of progress against plan. He managed the

Mr. James McAlister, MSc, PMP, Sec+
Program Risk and Quality Manager, Security Risk Solutions, Inc.

review of regulatory documents and formulation information for all products within 13 brand families, and managed the effort to document, categorize, and remediate all label discrepancies to ensure quality and eliminate risk in the form of remediation plans for each product in the consumer healthcare family.

World Class International, Inc.

Senior Life Sciences Consultant *(2000-2006)*

Mr. McAlister was a Senior Life Sciences Consultant for World Class International in New York, NY. His primary responsibility was business process re-engineering activities including definition and documentation of "as-is" processes, documentation of risk, elimination of non-value-added steps, and establishment of "to-be" processes. He ensured continuous improvement and mitigation of risk by defining metrics and measures for management, prepared project deliverables including presentations to management and communications to staff, and participated in technology solutions by facilitating the definition of operational and systems requirements, testing, version control and documentation, and system user training. Clients included Pfizer, Bristol Meyers Squibb, Bayer, GlaxoSmithKline, Abbott Laboratories, and Schering-Plough.

PricewaterhouseCoopers, LLC

Management Consultant *(1998-2000)*

Mr. McAlister served as a management consultant for PricewaterhouseCoopers in Washington, DC after attending graduate school in the United Kingdom. He supported the re-engineering of the budget formulation and execution process for the US Forest Service by defining current and future states and managing a system requirement/ selection process. He also managed approximately 120 independent contractors as part of a performance measurement project for the US Postal Service.

US Department of Justice, Antitrust Division

Paralegal Coordinator *(1993-1997)*

After graduating from Georgetown University, Mr. McAlister entered Federal service and joined the U.S. Department of Justice as Assistant Chief of Antitrust Division's Paralegal Unit. He recruited, interviewed, trained and supervised 140 paralegals. Mr. McAlister liaised with the Office of Human Resources to shepherd applicants through the Federal hiring process and worked closely with the Office of the Assistant Attorney General and all 15 litigating sections to establish training programs, determine case assignments for all paralegal staff, and establish policies and procedures for the Unit. He was promoted to Chief of the Paralegal Unit (GS-12 Supervisory Paralegal Specialist) in 1997 prior to leaving for graduate school.

Certifications and Affiliations

Certifications

- Project Management Professional (PMP)
- CompTIA Security+ (Sec+)

Ms. Jeanne Burton, PMP
Business Manager, Security Risk Solutions, Inc.

Education

INSTITUTION AND LOCATION	YEARS	FIELD OF STUDY
Project Management Professional, PMI	2009	Health Care Compliance and Information Assurance
United States Navy Active Duty - Cryptology	1987-1999	Project Management and Oversight
United States Naval Reserves – Cryptology	1999-2005	Quality Assurance and Risk Management

Qualifications Summary

Ms. Burton has demonstrated experience with government agencies in the initialization and execution of multiple, large-scale programs and projects. Ms. Burton currently serves as the Business Manager at Security Risk Solutions, Inc. Ms. Burton also serves as the Initiative Coordinator for the Data Segmentation for Privacy Initiative supporting the Office of the National Coordinator (ONC). She also is providing program and risk management to the Space and Naval Warfare (SPAWAR) Systems Center Atlantic as the risk manager for the $22M Navy Medicine (NAVMED) Integrated Product Team (IPT) which oversees the IPT projects supporting the NAVMED Enterprise Information Technology services. Ms. Burton is a specialist in program oversight and management, project management, risk management, strategic planning and quality assurance. Specifically, she provides guidance, education and program monitoring of programmatic and operational related risks and issues which span throughout the Navy Medicine hospitals and treatment centers worldwide. She has an extensive background in information assurance specializing in HIPAA auditing, security and risk assessments.

Experience Summary

Department of Health and Human Services (Contractor)
Data Segmentation for Privacy Initiative Coordinator (2013 – Present)

Ms. Burton is currently serving as the Initiative Coordinator for the Data Segmentation for Privacy Initiative providing coordination, scheduling and oversight of the initiative activities including assisting the pilot projects as needed and facilitating the monthly community-led nationwide updates.

Space and Naval Warfare Systems Center Atlantic (Contractor)
James A. Lovell Federal Health Care Center (FHCC)
Quality Assurance Manager (September 2010 – September 2011)

Ms Burton served as the Quality Assurance Manager for SPAWAR supporting the James A. Lovell Federal Health Care Center (FHCC) ensuring proper controls and quality in work products for the project were met. In her capacity as direct support to the program manager, she evaluated and reviewed all project documentation to ensure that Federal standards were met. She also identified, defined, advised on, and responded to any existing and future communication and relationship management needs impacting the successful implementation of FHCC applications, processes, and procedures. She applied state-of-the-art communications, change management concepts, and principals when presenting to the FHCC Director on joint information interoperability project matters. Her duties included performing final review of all correspondence and documentation developed and prepared by SPAWAR personnel on the FHCC project to ensure VA standards were met. She was also responsible for program and project internal audits, performance improvement, metrics reporting and compliance for the FHCC project.

Ms. Jeanne Burton, PMP
Business Manager, Security Risk Solutions, Inc.

Space and Naval Warfare Systems Center Atlantic (Contractor)
Veterans Affairs (VA) Sub-Portfolio
Quality Pillar Lead *(2008 –2010)*

During this time Ms. Burton provided program management and project start-up support to SPAWAR through the establishment of the SPAWAR Veterans Affairs (VA) Program Support Office (PSO). The program was a $188 million effort consisting of over twenty projects formulating applicable VA-wide policies, guidelines, procedures and processes. She established procedures with the VA's Technology Acquisition Center (TAC) for creating performance work statements, statement of work development, and contracting strategies and cost estimating. Ms. Burton was also responsible for establishing and implementing goals, objectives and program policies to establish standardization within the projects that included initiation, planning, executing, monitoring, control, and implementation and close-out procedures. Additionally, Ms. Burton assisted senior leadership in implementing program structure and assuring estimates for proposals and statement of work estimates. She also developed strategic plans to meet customer expectations through implementation meetings and discussions with the customer, business development plans, performed compliance auditing of project schedules, spend plans, deliverables and financial data. Through this support she ensured VA and SPAWAR implementation processes and standards were met including the assurance of the development and execution of operating budgets and finances. Also during this period, Ms. Burton served as a recognized expert by senior VA and other government leaders in working with, educating, informing, and advising the highest levels of senior counterparts to plan reviews, draft reports, conduct analyses and provide mitigation recommendations.

Space and Naval Warfare Systems Center Atlantic (Contractor)
Navy Medicine Senior Program Manager *(2001-2208)*

As Senior Program Manager, Ms. Burton was assigned to support SPAWAR's establishment of the program office for the Navy Medicine Chief Information Officer (CIO) located in Washington, DC. She developed project scopes, staffing plans, and cost requirements and was responsible for the oversight and management of all staffing and requirements development which included acquiring experts in policy, certification and accreditation (C&A), compliance, system and security engineering, and medical systems for the CIO office. Ms. Burton ensured Department of Navy and SPAWAR implementation processes and standards were met including the assurance of the development and execution of operating budgets and finances. She served as a recognized expert by senior Navy Medicine and other government leaders in working with, educating, informing, and advising the highest levels of senior counterparts to plan reviews, draft reports, conduct analyses and provide mitigation recommendations on cost, schedule and performance.

Additionally, Ms. Burton established a five year $100M program strategy and served as Deputy Program Manager for the NAVMED IA program and served as management and oversight of the Program. She was instrumental in the establishment of the strategy to provide Navy Medicine a clear IA roadmap to ensure policy development, network C&A, firewall compliance, training and awareness and vulnerability assessment and mitigation for the Navy Medicine Enterprise. She conducted numerous HIPAA security audits and risk assessments for the program outlining gaps, deficiencies and recommendations needed for compliance. She formulated achievable goals, objectives, strategies and solutions for Navy Medicine projects. During this period she also served as Navy Anti-Terrorism Force Protection (ATFP) Strategic planner and Program Management Office (PMO) Manager. This program was a $140M program which spanned ten projects. Within the ATFP program, she provided PMO development, program oversight,

Ms. Jeanne Burton, PMP
Business Manager, Security Risk Solutions, Inc.

strategic planning, cost analysis and earned value management (EVM) solutions. Ms. Burton served as the Military Health Systems (MHS) Quality Assurance (QA) Manager which had a working capital budget of over $40 million dollars. Through direct interface with the customer and the project leads, she was able to quickly document existing organizational and functional processes to determine project gaps and deficiencies. Through this effort she assisted the MHS through the establishment of standardized processes in project management, communication, and quality assurance plans. Ms. Burton developed a quarterly quality assurance schedule for use within the program to monitor all projects with immediate readiness metrics dashboards for senior management review.

She served as the Deputy Program Manager for the Information Assurance Tiger Team (IATT) which had a program budget of $5.2 million responsible for the day to day management and final quality product review of 45 security engineers who were responsible for executing security assessments of Navy networks as they prepared for transition to the Navy Marine Corps Intranet (NMCI). Her direct responsibilities also included project financial forecasting, measurement and analysis, and quality assurance. She led the final report review board which outlined the network topologies, security testing, results and recommendations in ensuring site/network compliance in support of the Navy's certification and accreditation requirements.

Certifications

- Project Management Professional (PMP)

Mr. Michael Davino, BA, MS, CISSP
IA Professional - COOP Team Lead, Security Risk Solutions, Inc.

Education

INSTITUTION AND LOCATION	DEGREE	YEARS	FIELD OF STUDY
Loyola University of Chicago, Chicago, IL	MS (Master of Science)	1986	Computer Science
DePaul University, Chicago, IL	BA (Bachelor of Arts)	1971	English
George Washington University, Washington, DC	AD (Associate Certificate)	2007	Project Management

Qualifications Summary

Mr. Davino has 20+ years experience coordinasting IT Security, Risk Management, Disaster Recovery and Business Continuity Planning functions across healthcare, insurance, financial, manufacturing, and defense sectors; including managing IT Security and Risk Management at a major financial institution, and hands-on involvement in evaluating DR and Business Continuity programs for major hospital groups.

He has significant experience in IT training and education having served as an Adjunct Faculty member of Computer Science at McHenry County College, Harper College, Triton College, Mallinckrodt College, and Loyola University of Chicago; Advisory Board member at Mallinckrodt College, Loyola University of Chicago, and ITT Technical Institute; and independent technical consultant to Applied Learning, Deltak Training, and Career Education.

He has his Certified Information Systems Security Professional (CISSP) certification, recently completed Advanced DIACAP Validator Certification training, and is awaiting Fully Qualified Navy Validator (FQNV) certification from the Navy Validator Certification Authority.

Experience Summary

Space and Naval Warfare Systems Center Atlantic
Continuity of Operations (COOP) Team Lead (*2010 – present*)

Mr. Davino is responsible for planning, supporting, and sustaining Enterprise Information Assurance (EIA) Information Technology Contingency Planning (ITCP) services for the Navy Medicine (NAVMED) Enterprise including: project management and administrative support, site-level ITCP Support, Enterprise-level ITCP support, COOP training Subject Matter Expertise (SME) and support, Disaster Recovery Planning (DRP) Baseline Development, and Information Assurance (IA) training SME and support. He assists NAVMED Enclaves and Programs of Record (PORs) develop, review, implement, and exercise their contingency plans to assure compliance with representative Federal and departmental policies and guidelines (e.g., FISMA, DoDI, etc.).

SunGard Availability Solutions
Lead Consultant and Project Manager (*2008 – 2010*)

Mr. Davino provided subject matter expertise in the identification, prioritization, and sustainment of Mission Essential Functions (MEFs) for myriad commercial enterprises. Mr. Davino's efforts included identifying and balancing operational imperatives and corresponding system requirements (e.g., mainframe, server-based applications) via comprehensive Business Impact Analysis (BIA), and defining and promulgating responsive COOP strategies and execution-level plans. Mr. Davino led Enterprise-wide risk assessment and mitigation programs. He supported compliance testing, evaluation, and training (e.g., against National Institute of Standards and Technology [NIST] guidance and security controls, and Information Technology Infrastructure Library [ITIL] best practices) to ensure consistent application among Enterprise leadership and tactical personnel.

HSBC Technology Services
Manager of IT Security *(2003 – 2008)*

Mr. Davino managed teams of security analysts responsible for Access Management, Identity Management, Access Revalidations, Remote Access, Threat & Incident Management, Patch Management, Encryption, Workflow Automation, Application Security Reviews, Third Party Assessments, Log Reviews, and Security Awareness. He directed internal assessments of IT policies, standards, procedures and controls to ensure compliance with

Mr. Michael Davino, BA, MS, CISSP
IA Professional - COOP Team Lead, Security Risk Solutions, Inc.

applicable industry regulations and guidelines. He also coordinated development and implementation of Web/Intranet landing pages to document and publish Threat & Incident Management, Security Awareness, Access Management, Regulatory policies, standards and procedures. Mr. Davino also implemented Incident Management standards and procedures within the ITIL framework to streamline IT Security crisis support activities, and improve problem response time.

HSBC Technology Services
Data Center Consolidation Project Manager *(2001 – 2003)*
Mr. Davino coordinated the construction of a $26 million, Tier-1 recovery data center comprised of 6 IBM zOS mainframe parallel processors, 20 IBM iSeries and Sun midrange processors, and 100+ Windows and Unix servers. He also coordinated the development of Data Center Systems Requirements, Operational Requirements, Testing, and Evaluation standards with internal IT infrastructure teams including Data Center Operations, Scheduling, Systems Programming, Network Operations, Capacity Planning, Telecommunications, Distributed Systems, Data base Administration, Middleware, Applications Support, Help Desk, and external configuration engineers from IBM, EMC, Hitachi, and HP.

HSBC Technology Services
Senior Manager of Disaster Recovery and Business Continuity *(1998 – 2001)*
Mr. Davino managed Enterprise-wide DR and Business Continuity programs including BIA, risk assessment, Data Center Recovery Plans (DCRPs), Business Continuity Plans (BCPs) and DR Plans (DRPs) for 2 major data centers, supporting 30,000 employees across 10 regional offices and 1,500 branch offices in the U.S. and Canada. He advised C-level corporate and IT management regarding DR/BCP goals, objectives, best practices, success criteria and performance; provided recommendations for continuous improvement; and maintained productive relationships with sponsors, stakeholders and clients across a broad array of business sectors. In this role Mr. Davino also directed internal risk assessments to ensure compliance with applicable regulations and guidelines (e.g., NIST); directly interfaced with regulators and teams of internal and external auditors to review IT and business policies, procedures, and applications; successfully identified, prioritized and coordinated the remediation of all potential compliance issues; and developed quality and performance measurements to ensure critical IT functions continually aligned with enterprise requirements.

Kemper Insurance
IT Area Manager of Claim and Loss Systems *(1995 – 1998)*
Mr. Davino was responsible for monitoring the ongoing performance, productivity, and quality of three managers, 30+ developers, and multiple third party contractors responsible for developing and supporting mainframe, midrange and client-server based Risk Management, Claims & Loss, and Policy Management systems. In this role, Mr. Davino also managed the entire System Development Lifecycle (SDLC) of enterprise-wide mainframe and client-server based applications including the development and coordination of Business Requirements, Systems Requirements, Operational Requirements, Testing, and Performance Monitoring. He was also responsible for DR, Business Continuity, Change Management, Capability Maturity Modeling (CMM), and Quality Assurance & Metrics.

Trans Union Technology Services
IT Manager – Data Acquisition Reengineering *(1995 – 1995)*
Mr. Davino managed multiple application development teams responsible for migrating data acquisition services from mainframe to client-server platforms. In this role he also coordinated the activities of middleware teams developing 3-tiered client-server infrastructure using DCE, Encina, TCP/IP, and PVCS; supervised the development of API's and RPC's using C and C++; managed VB developers and Sybase DBA's migrating legacy CICS, COBOL and DB2 mainframe applications to RS6000 client server platform; and coordinated Business Requirements, Systems Requirements, Operational Requirements, Testing, & Performance Monitoring for application development teams.

Certifications: Certified Information Security Systems Professional (CISSP)

JAMIE DOYLE
Systems Architect, KRM Associates, Inc.

Education

INSTITUTION AND LOCATION	DEGREE	YEARS	FIELD OF STUDY
Hagerstown Community College, Hagerstown, Maryland	AA	2001	General Studies
Shepherd University, Shepherdstown, West Virginia	BS	2003	Computer Science

Qualifications Summary

Mr. Doyle has extensive experience and background in various areas of Information Technology ranging from health information security to software engineering & development.

With a strong focus on health information security, Mr. Doyle has worked directly with:

- Federal entities & agencies
  - Department of Veterans Affairs (VA)
  - Department of Defense (DoD)
  - Department and Health and Human Services (DHHS)
  - Indian Health Service (IHS)
- Academic institutions
  - Georgetown University
  - Carnegie Mellon University Software Engineering Institute (SEI)

As a member of the VA's Health Information Security Division (HISD), Mr. Doyle was directly responsible for developing testing criteria, methodology and policies to secure FDA-regulated medical devices. He also developed specialized software to evaluate test results and worked directly with vendors to mitigate threats and improve the security posture of their devices.

As part of the DoD Defense Health Information Assurance Program (DHIAP), Mr. Doyle was a software engineer on the Enterprise Information Security Assessment System (ENTISAS) team. This tool is used by DoD to analyze security risks, threats and vulnerabilities as well as mitigation plans and protections profiles and other information security elements across multiple organizations and organizational elements.

Experience Summary

KRM Associates Inc., Shepherdstown, West Virginia
Systems Architect (2003 – Present)

Open Source Electronic Health Record Agent (OSEHRA)

- Member of the OSEHRA team collaborating with the VA to release innovative best of breed 'open source' healthcare software & solutions.
  - Blue Button for America
  - Worked directly with 2012 Presidential Innovation Fellow and Team to provide every Veteran in

JAMIE DOYLE
Systems Architect, KRM Associates, Inc.

America with the ability to download their health record through MyHealtheVet. This project was a major open source initiative and won Innovation of the Year award for 2012.

- HealtheMe™
  - Prepared and released open source version of the HealtheMe™ Personal Health and Wellness Management System through OSEHRA. This release was a major milestone as it allows anyone to download, use, or modify the application and make contributions back to the project at will.

Health Information Security Division (HISD)

- Directly involved in all aspects of system development including initial HISD Lab installation and set-up; communication with vendors throughout the medical device configuration and vulnerability assessment process; establishing policies and procedures, including development of the VA Hardening Guidelines for Networked Medical Devices; conducting vulnerability assessments and the mitigation of identified risks through on-going vendor relations; and preparation of Vulnerability Assessment Reports and Mitigation Letters sent to vendors.
- Performed security assessments on FDA and non-FDA regulated medical devices for the Medical Security Device Assessment Center (MeDSAC) responsible for assessing security of medical systems for the Veterans Administration.
- Member of the Health Information Security Division (HISD) team that launched, operate, and maintain a comprehensive system for testing and remediating FDA regulated and non-regulated networked medical devices for the Department of Veterans Affairs
- Worked with vendors and VA personnel to ensure medical devices comply with HIPAA requirements and federal regulations.
- Collaborate with the VA team responsible for migrating new and legacy networked medical devices into the Medical Device Isolation Architecture (MDIA).
- Developed the automated tools and database technologies to support automated risk assessments.

Worked with medical device vendors to create a Security Configuration Guideline providing VA field personnel with access to antivirus requirements for each medical device as well as detailed guidance in preventing, detecting and removing viruses.

- Independently developed and implemented the Medical Device Vulnerability Assessment Information System (MeDVAIS), a tool that drastically increased the HISD Vulnerability Assessment Report accuracy while slashing eight to 12 days from the time needed to generate reports. The first version of the tool has been copyrighted and a second version, with improved features and capabilities, is in the developmental stage.
- Directly involved in the successful testing of 62 networked medical devices in various environments including in the HISD lab, at remote vendor operations, and on-site at VA medical centers.

Certification & Accreditation Center

- Worked closely with C&A Program Manager and key players to develop C&A documentation including the VistA System Level Control Appendices (SLCA) and Site Security Plan (SSP) following guidance provided by the National Institute of Standards and Technology (NIST) 800-series publications.
- Designed and developed a Cold Fusion/Microsoft SQL Server 2000 based solution that aggregated test results from the field for each of the 23 VISNs (Veterans Integrated Service Network) within the VA. Test result data for each VISN was gathered by the "SCAAT" Tool and was imported into the enterprise repository tool mentioned above. The implementation of this tool alone provided unprecedented enterprise-wide C&A reporting functionality which allowed program managers easily pin point trends and major areas of non-compliance in need of remediation.

JAMIE DOYLE
Systems Architect, KRM Associates, Inc.

Department of Health and Human Services (HHS)

- Health Resources and Services Administration (HRSA)
  - Public Health Courseware Development
  - Worked with team to develop a SCORM-based (healthcare provider) training course.

Centers for Medicare & Medicaid Services (CMS)

- Medicaid Transformation
  - Served as Technical Lead, Designer, and Project Manager for Healthe*Me*™ (Healthe*Mountaineer*) Personal Health Record pilot for West Virginia's DHHR/Medicaid. The system was developed as a "best of breed open source" solution deployed on a low cost platform using widely accepted standards both in the medical and IT sectors. The initial release allows clinicians to enroll patients, link health record "identifiers" found within their native EMR systems, and empowers the patients to manage various aspects of their health record. A small community clinic in rural West Virginia was chosen for the pilot and health records were successfully exchanged via ASTM CCR. This revolutionary technology enabled patients to have access to their real medical record (for the first time) in near real-time with the added ability to self-enter records. The system is being expanded to integrate a full CONNECT complaint Health Information Exchange (HIE) which will enable multiple organizations to share health information with the patient having full control over the flow of information.

KRM Associates Inc.

- ENTISAS™
  - Assisted in the design and development of the Enterprise Information Security Assessment (ENTISAS) system marketed by KRM for enterprise wide security assessments and evaluations.
  - Support TATRC and Georgetown University Hospital in the security evaluations and assessments of healthcare entities. Part of the team that performed the DITSCAP on ENTISAS.
- Datacenter
  - Responsible for complete remodel of leased datacenter. Managed all aspects of project including (but not limited to): floor plan illustrations, heat load calculations / CRAC specs, electrical specs, physical security (alarm & smart card access), fire suppression, backup power generation and distribution.
  - Assisted in all phases of build out including equipment specs, acquisition & installation. Worked with various VARs to bring assets online and responsible for ongoing maintenance including inventory management.

Certifications, and Affiliations

Affiliations

- Member of OSEHRA

SHANE McCLAUGHRY
KRM Associates, Inc.

Education

INSTITUTION AND LOCATION	DEGREE	YEARS	FIELD OF STUDY
Shepherd University, Shepherdstown, West Virginia	Bachelor of Science	2008	Network and Data Communications (NDA)

Qualifications Summary

Mr. McClaughry, with a background in networking and security, has worked on various contracts dealing with local and federal government, each imploring different aspects of technology. Focusing on the security aspects of technology, he has worked directly with the VA NSOC where his main product support contributions were to the McAfee HBSS applications. Through having worked directly with a federal organization, it has given him the ability to quickly learn and adapt to policies related to the task at hand.

Experience Summary

Mr. McClaughry has worked with many different technologies and aspects of technology during the course of his career. Having started as a basic ground technician performing basic computer and network repair, up to working onsite at a government installation providing national support for host based security systems. Supporting multiple government related contracts at a local and federal level has also provided in-depth experience with the inner workings of government related contracts and key expectations.

KRM Associates, Inc.
System Engineer (2009 – 2010, 2011 – present)
Security Engineer (2010 – 2011)
Internship (2008 – 2009)

Mr. McClaughry has worked on various contracts while employed at KRM Associates. Originally employed as an Intern, he obtained his start at KRM working on the West Virginia Health Transformation Portal Project. This project having been a joint operation of WV DHHR and none government organizations was aimed at improving healthcare for the West Virginia community. Tasks included different aspects of web design, including, scripting, development, and incorporating user feedback.

Mr. McClaughry upon becoming a full time employee became a System Engineer. As a System Engineer, he worked both on contracts as well as helping maintain the infrastructure which supported daily operations at KRM Associates. His contractual work while varied, typically included support for KRM's PHR HealtheMe. HealtheMe originally grew from the CMS PHR Pilot, where he took on the role of tester for various system related functionality. During the Shepherd University Nursing pilot, he setup, and maintained systems which housed HealtheMe.

In 2010, Mr. McClaughry became part of the Veterans Affairs NEBOSS contract and was located onsite at the VA NSOC. On the NEBOSS contract, he worked on different aspects of security. Windows patch testing, to confirm that the Microsoft updates would not break various functions of the systems they were being installed on. IBM Proventia Network Intrusion Protection Systems, which included setup, monitoring, and maintenance. Different aspects of the McAfee HBSS suite, including Linux/Unix/Windows versions of Anti-Virus, HIPs, ePO 3.5 and 4.0. McAfee work included Tier 3

SHANE McCLAUGHRY
KRM Associates, Inc.

support, virus submission to McAfee, installation of updated definitions to fix submitted viruses, updating ePO, AV, and HIPS Policies, writing and maintaining installation documentation and policies, and reporting to management based upon HIPS information collected during that week. Other systems worked with but on a minor role during this time include: Splunk, BigFix, Solaris Solarwinds, and ISS HIPS.

After the conclusion of the NEBOSS contract, Mr. McClaughry became part of the OSEHRA contract as well as his active role of KRM infrastructure support. Infrastructure support included VM management, domain management, active directory support, network monitoring, backup management, and anti-virus products. His OSEHRA related activities have been varied, but have included, FOIA VistA product testing, product support, VM construction and distribution, as well as document support related to the stated areas.

Clarke County Public School System
Internship (2004 – 2005)

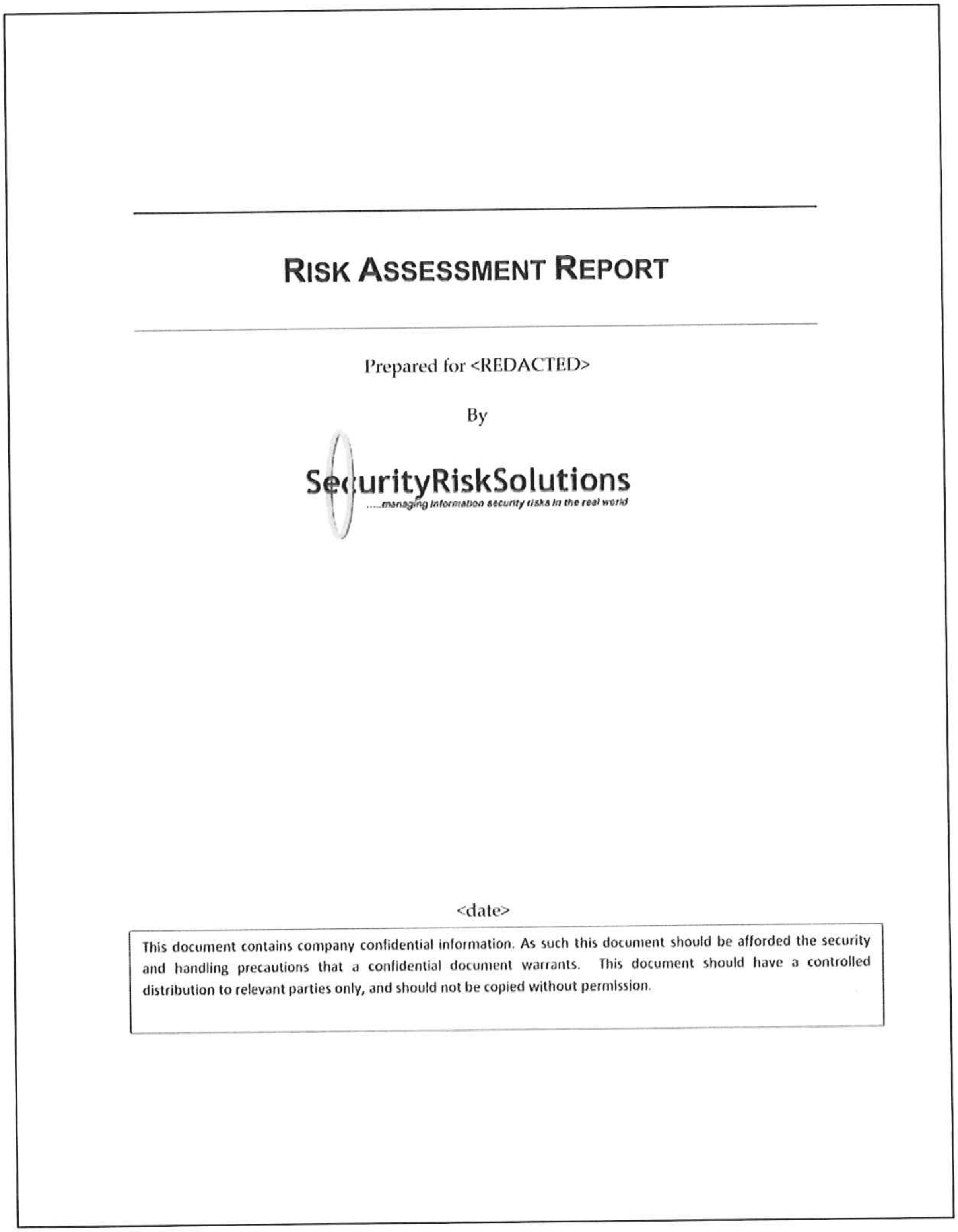
Mr. McClaughry worked for Clarke County Public Schools as an Intern of Technology. As an intern he functioned as a ground technician and helped with various troubleshooting and system repairs.

Certifications, and Affiliations

Certifications

- CompTIA Security +
- Cisco Certified Network Associate (CCNA)

Appendix H: Sample Executive Summary Report with Technical Information



RISK ASSESSMENT REPORT

Prepared for <REDACTED>

By

SecurityRiskSolutions

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

<date>

This document contains company confidential information. As such this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only, and should not be copied without permission.

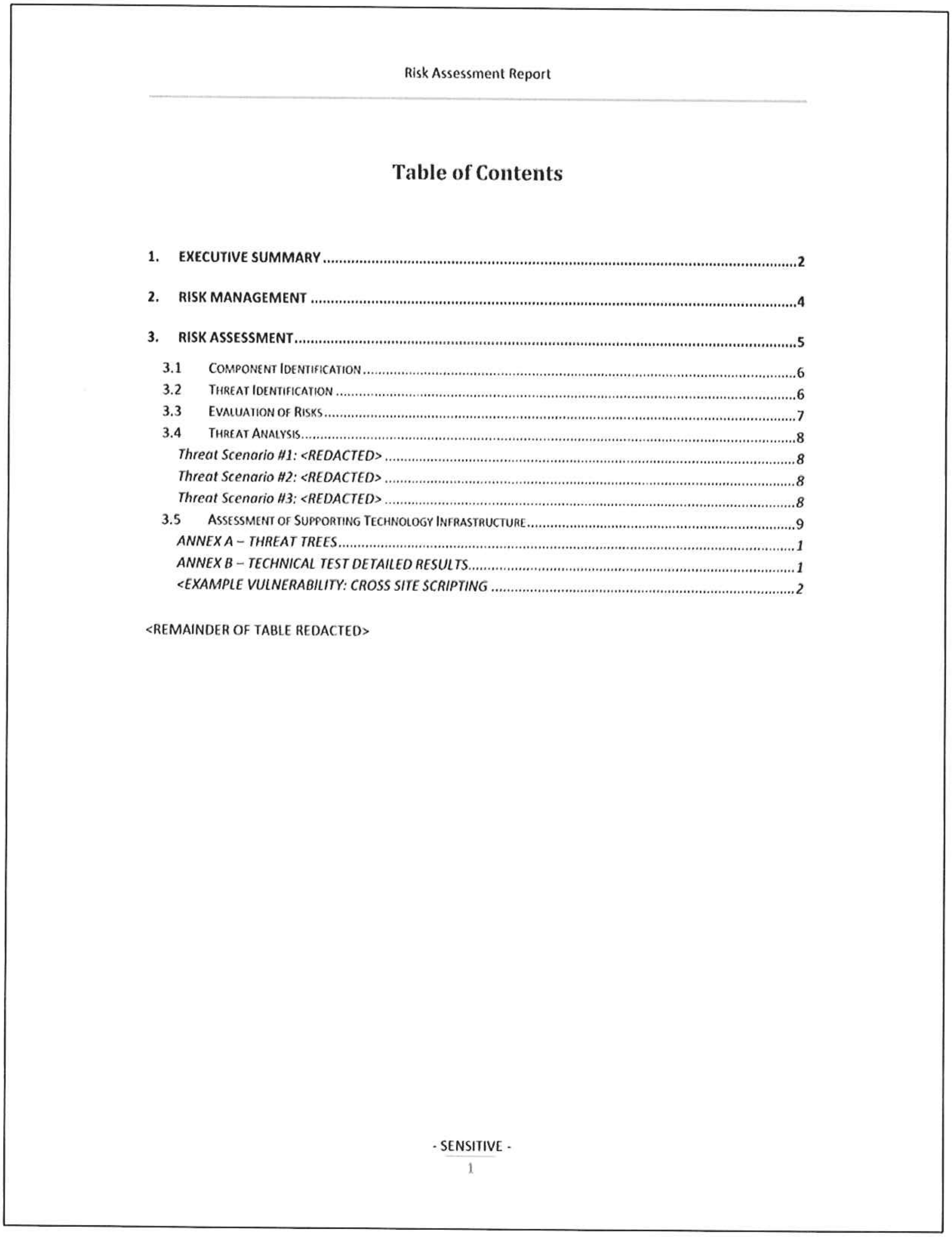
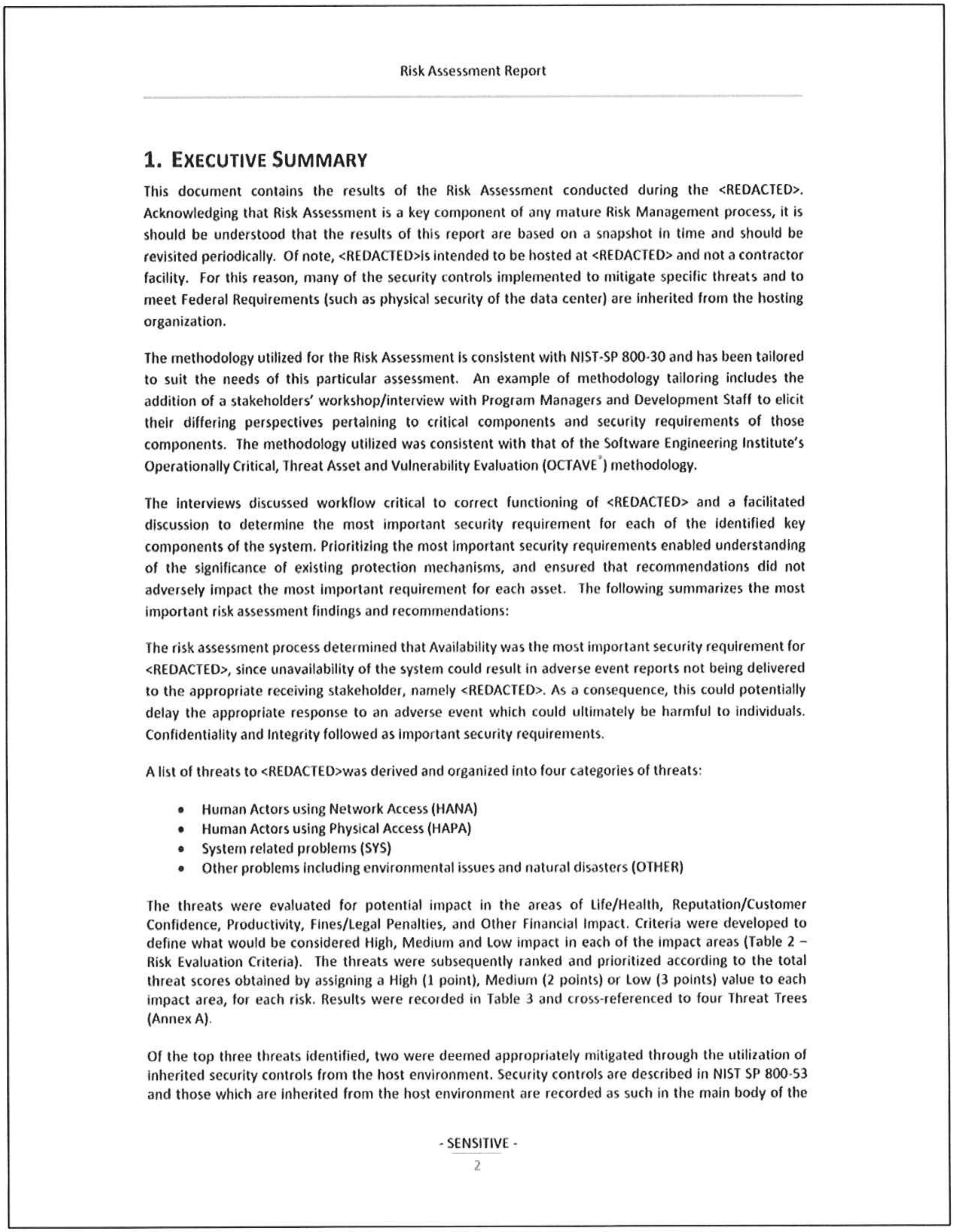


Table of Contents

<REMAINDER OF TABLE REDACTED>



1. Executive Summary

This document contains the results of the Risk Assessment conducted during the <REDACTED>. Acknowledging that Risk Assessment is a key component of any mature Risk Management process, it is should be understood that the results of this report are based on a snapshot in time and should be revisited periodically. Of note, <REDACTED>is intended to be hosted at <REDACTED> and not a contractor facility. For this reason, many of the security controls implemented to mitigate specific threats and to meet Federal Requirements (such as physical security of the data center) are inherited from the hosting organization.

The methodology utilized for the Risk Assessment is consistent with NIST-SP 800-30 and has been tailored to suit the needs of this particular assessment. An example of methodology tailoring includes the addition of a stakeholders' workshop/interview with Program Managers and Development Staff to elicit their differing perspectives pertaining to critical components and security requirements of those components. The methodology utilized was consistent with that of the Software Engineering Institute's Operationally Critical, Threat Asset and Vulnerability Evaluation (OCTAVE®) methodology.

The interviews discussed workflow critical to correct functioning of <REDACTED> and a facilitated discussion to determine the most important security requirement for each of the identified key components of the system. Prioritizing the most important security requirements enabled understanding of the significance of existing protection mechanisms, and ensured that recommendations did not adversely impact the most important requirement for each asset. The following summarizes the most important risk assessment findings and recommendations:

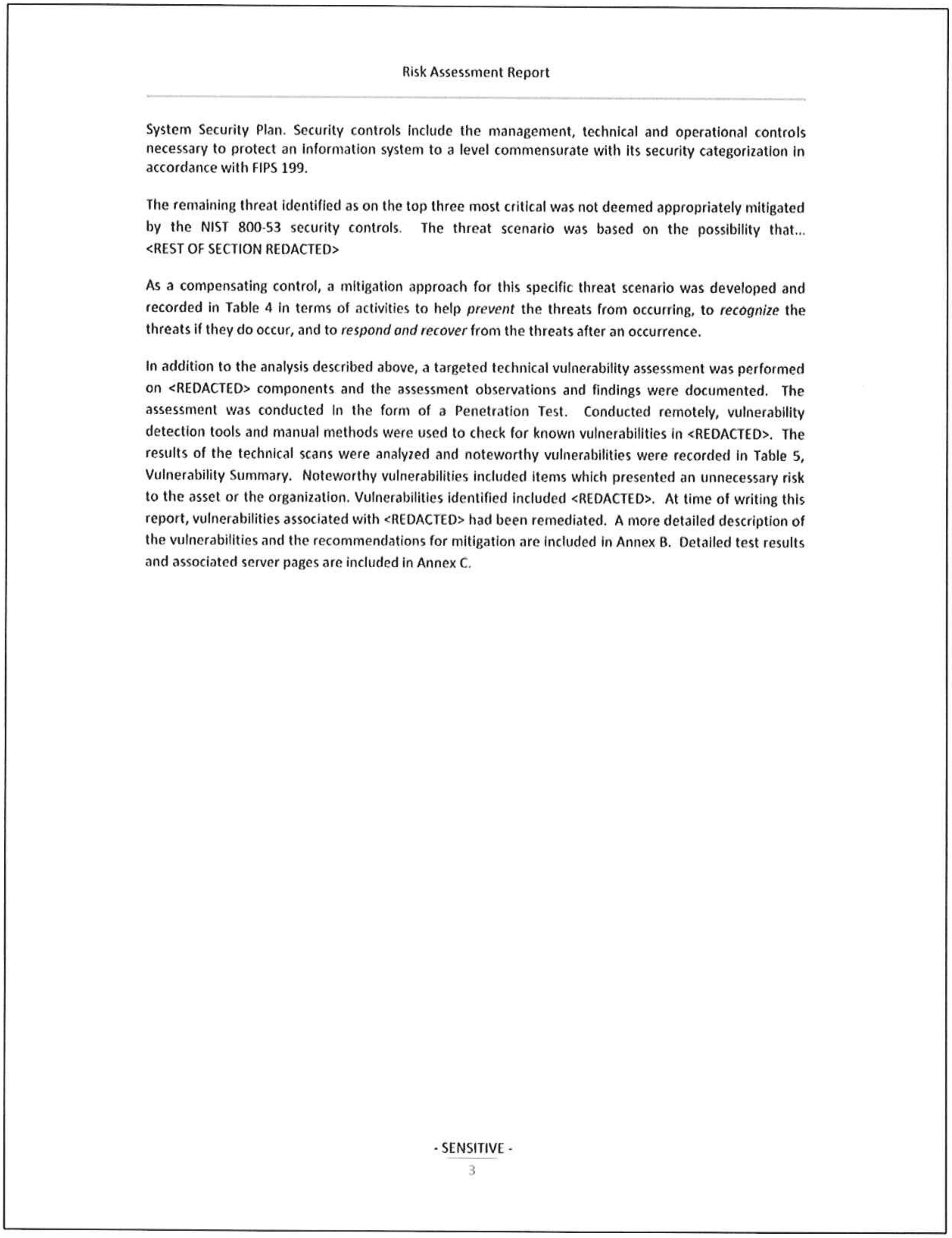
The risk assessment process determined that Availability was the most important security requirement for <REDACTED>, since unavailability of the system could result in adverse event reports not being delivered to the appropriate receiving stakeholder, namely <REDACTED>. As a consequence, this could potentially delay the appropriate response to an adverse event which could ultimately be harmful to individuals. Confidentiality and Integrity followed as important security requirements.

A list of threats to <REDACTED>was derived and organized into four categories of threats:

- Human Actors using Network Access (HANA)
- Human Actors using Physical Access (HAPA)
- System related problems (SYS)
- Other problems including environmental issues and natural disasters (OTHER)

The threats were evaluated for potential impact in the areas of Life/Health, Reputation/Customer Confidence, Productivity, Fines/Legal Penalties, and Other Financial Impact. Criteria were developed to define what would be considered High, Medium and Low impact in each of the impact areas (Table 2 – Risk Evaluation Criteria). The threats were subsequently ranked and prioritized according to the total threat scores obtained by assigning a High (1 point), Medium (2 points) or Low (3 points) value to each impact area, for each risk. Results were recorded in Table 3 and cross-referenced to four Threat Trees (Annex A).

Of the top three threats identified, two were deemed appropriately mitigated through the utilization of inherited security controls from the host environment. Security controls are described in NIST SP 800-53 and those which are inherited from the host environment are recorded as such in the main body of the

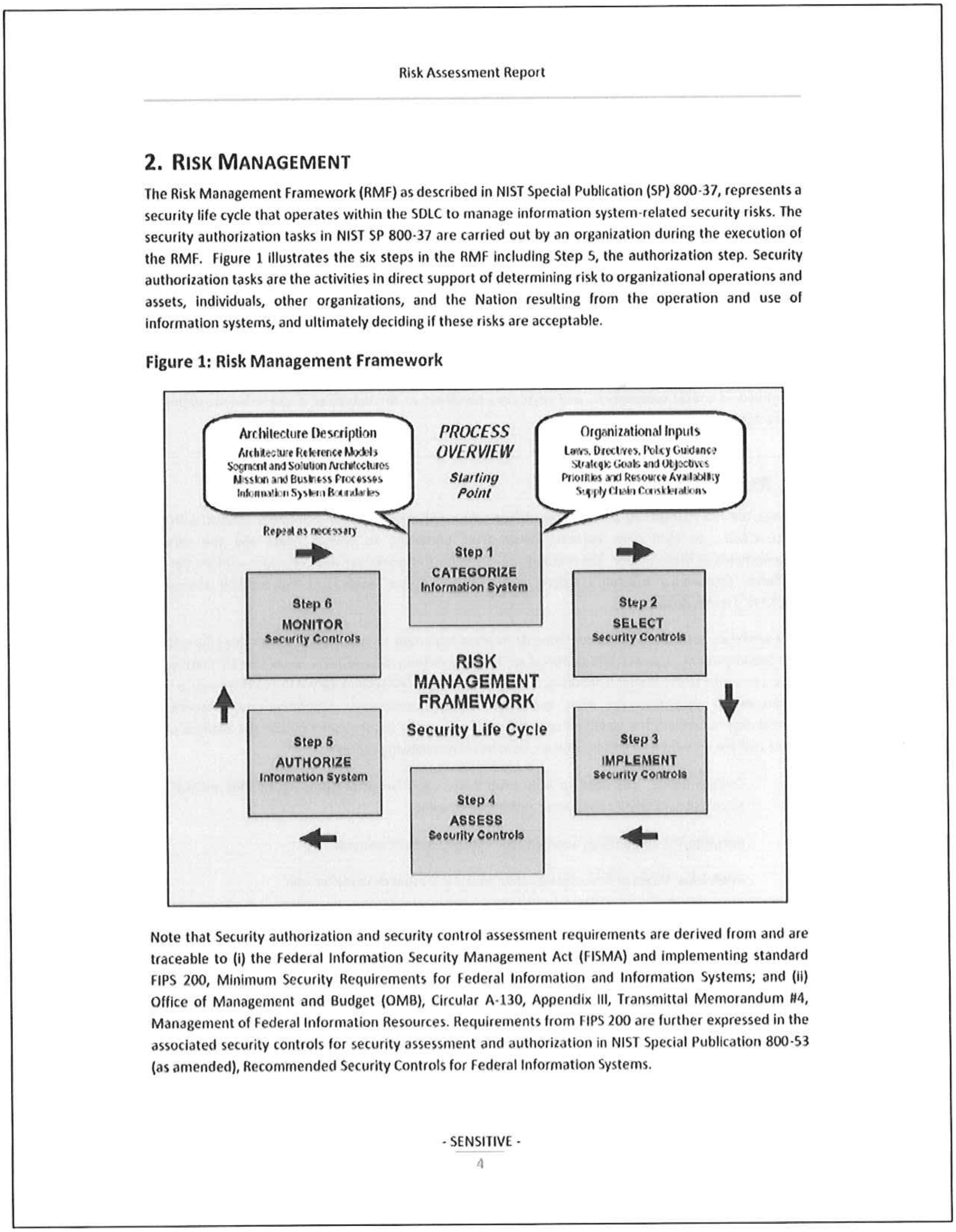


System Security Plan. Security controls include the management, technical and operational controls necessary to protect an information system to a level commensurate with its security categorization in accordance with FIPS 199.

The remaining threat identified as on the top three most critical was not deemed appropriately mitigated by the NIST 800-53 security controls. The threat scenario was based on the possibility that... <REST OF SECTION REDACTED>

As a compensating control, a mitigation approach for this specific threat scenario was developed and recorded in Table 4 in terms of activities to help *prevent* the threats from occurring, to *recognize* the threats if they do occur, and to *respond and recover* from the threats after an occurrence.

In addition to the analysis described above, a targeted technical vulnerability assessment was performed on <REDACTED> components and the assessment observations and findings were documented. The assessment was conducted in the form of a Penetration Test. Conducted remotely, vulnerability detection tools and manual methods were used to check for known vulnerabilities in <REDACTED>. The results of the technical scans were analyzed and noteworthy vulnerabilities were recorded in Table 5, Vulnerability Summary. Noteworthy vulnerabilities included items which presented an unnecessary risk to the asset or the organization. Vulnerabilities identified included <REDACTED>. At time of writing this report, vulnerabilities associated with <REDACTED> had been remediated. A more detailed description of the vulnerabilities and the recommendations for mitigation are included in Annex B. Detailed test results and associated server pages are included in Annex C.

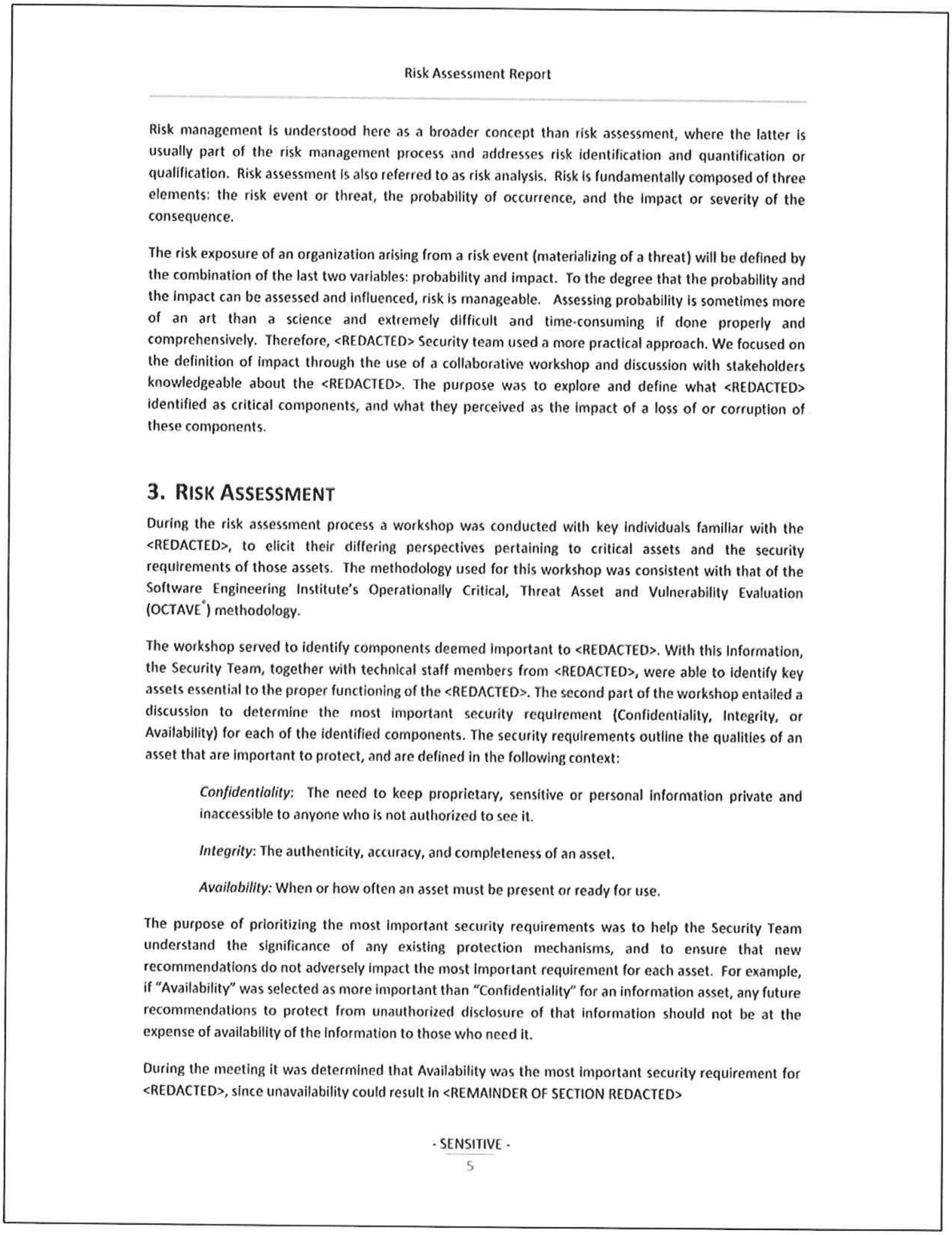


2. RISK MANAGEMENT

The Risk Management Framework (RMF) as described in NIST Special Publication (SP) 800-37, represents a security life cycle that operates within the SDLC to manage information system-related security risks. The security authorization tasks in NIST SP 800-37 are carried out by an organization during the execution of the RMF. Figure 1 illustrates the six steps in the RMF including Step 5, the authorization step. Security authorization tasks are the activities in direct support of determining risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of information systems, and ultimately deciding if these risks are acceptable.

Figure 1: Risk Management Framework

Note that Security authorization and security control assessment requirements are derived from and are traceable to (i) the Federal Information Security Management Act (FISMA) and implementing standard FIPS 200, Minimum Security Requirements for Federal Information and Information Systems; and (ii) Office of Management and Budget (OMB), Circular A-130, Appendix III, Transmittal Memorandum #4, Management of Federal Information Resources. Requirements from FIPS 200 are further expressed in the associated security controls for security assessment and authorization in NIST Special Publication 800-53 (as amended), Recommended Security Controls for Federal Information Systems.



Risk management is understood here as a broader concept than risk assessment, where the latter is usually part of the risk management process and addresses risk identification and quantification or qualification. Risk assessment is also referred to as risk analysis. Risk is fundamentally composed of three elements: the risk event or threat, the probability of occurrence, and the impact or severity of the consequence.

The risk exposure of an organization arising from a risk event (materializing of a threat) will be defined by the combination of the last two variables: probability and impact. To the degree that the probability and the impact can be assessed and influenced, risk is manageable. Assessing probability is sometimes more of an art than a science and extremely difficult and time-consuming if done properly and comprehensively. Therefore, <REDACTED> Security team used a more practical approach. We focused on the definition of impact through the use of a collaborative workshop and discussion with stakeholders knowledgeable about the <REDACTED>. The purpose was to explore and define what <REDACTED> identified as critical components, and what they perceived as the impact of a loss of or corruption of these components.

3. Risk Assessment

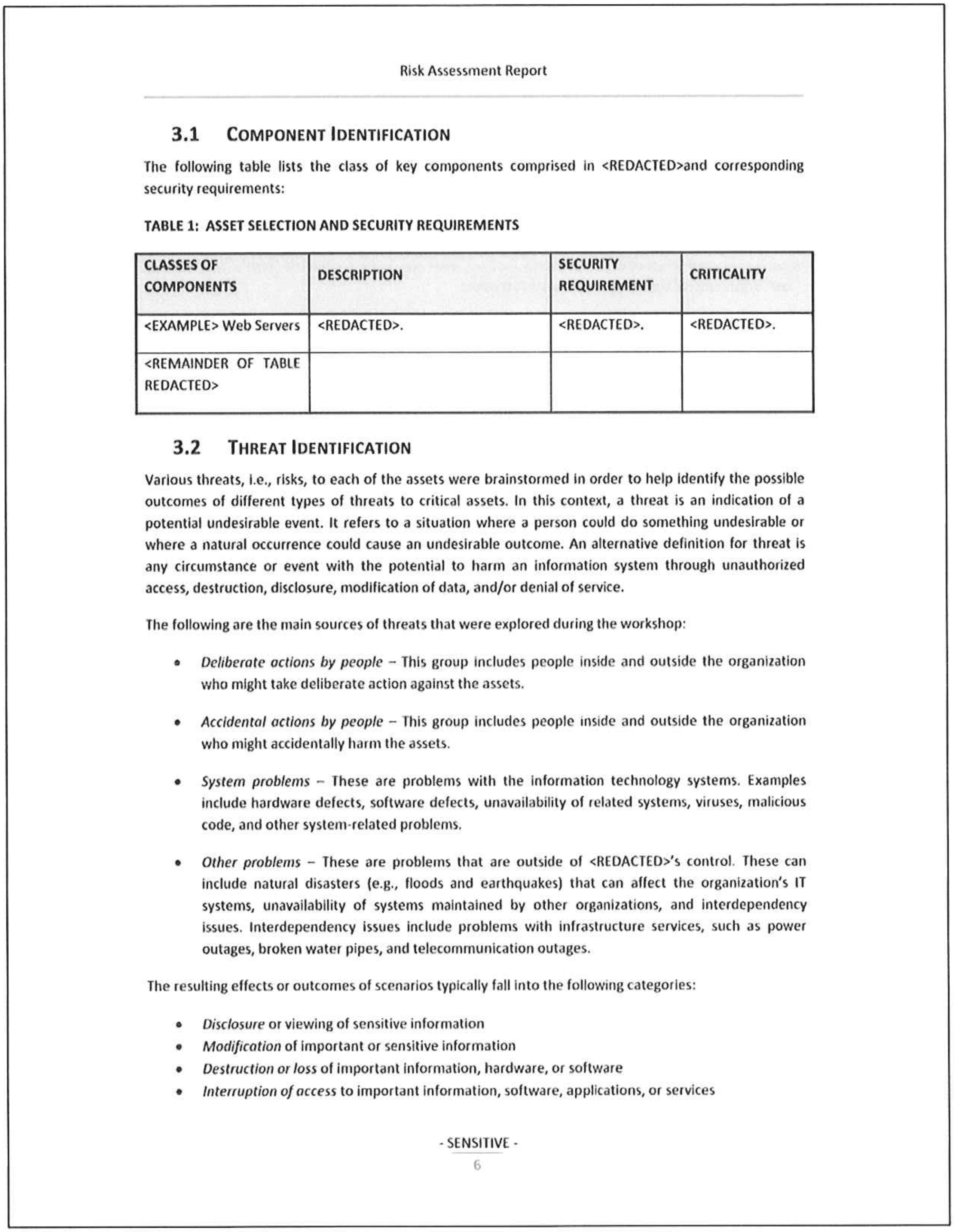
During the risk assessment process a workshop was conducted with key individuals familiar with the <REDACTED>, to elicit their differing perspectives pertaining to critical assets and the security requirements of those assets. The methodology used for this workshop was consistent with that of the Software Engineering Institute's Operationally Critical, Threat Asset and Vulnerability Evaluation (OCTAVE®) methodology.

The workshop served to identify components deemed important to <REDACTED>. With this information, the Security Team, together with technical staff members from <REDACTED>, were able to identify key assets essential to the proper functioning of the <REDACTED>. The second part of the workshop entailed a discussion to determine the most important security requirement (Confidentiality, Integrity, or Availability) for each of the identified components. The security requirements outline the qualities of an asset that are important to protect, and are defined in the following context:

> *Confidentiality*: The need to keep proprietary, sensitive or personal information private and inaccessible to anyone who is not authorized to see it.
>
> *Integrity*: The authenticity, accuracy, and completeness of an asset.
>
> *Availability:* When or how often an asset must be present or ready for use.

The purpose of prioritizing the most important security requirements was to help the Security Team understand the significance of any existing protection mechanisms, and to ensure that new recommendations do not adversely impact the most important requirement for each asset. For example, if "Availability" was selected as more important than "Confidentiality" for an information asset, any future recommendations to protect from unauthorized disclosure of that information should not be at the expense of availability of the information to those who need it.

During the meeting it was determined that Availability was the most important security requirement for <REDACTED>, since unavailability could result in <REMAINDER OF SECTION REDACTED>



3.1 COMPONENT IDENTIFICATION

The following table lists the class of key components comprised in <REDACTED>and corresponding security requirements:

TABLE 1: ASSET SELECTION AND SECURITY REQUIREMENTS

CLASSES OF COMPONENTS	DESCRIPTION	SECURITY REQUIREMENT	CRITICALITY
<EXAMPLE> Web Servers	<REDACTED>.	<REDACTED>.	<REDACTED>.
<REMAINDER OF TABLE REDACTED>			

3.2 THREAT IDENTIFICATION

Various threats, i.e., risks, to each of the assets were brainstormed in order to help identify the possible outcomes of different types of threats to critical assets. In this context, a threat is an indication of a potential undesirable event. It refers to a situation where a person could do something undesirable or where a natural occurrence could cause an undesirable outcome. An alternative definition for threat is any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

The following are the main sources of threats that were explored during the workshop:

- *Deliberate actions by people* – This group includes people inside and outside the organization who might take deliberate action against the assets.

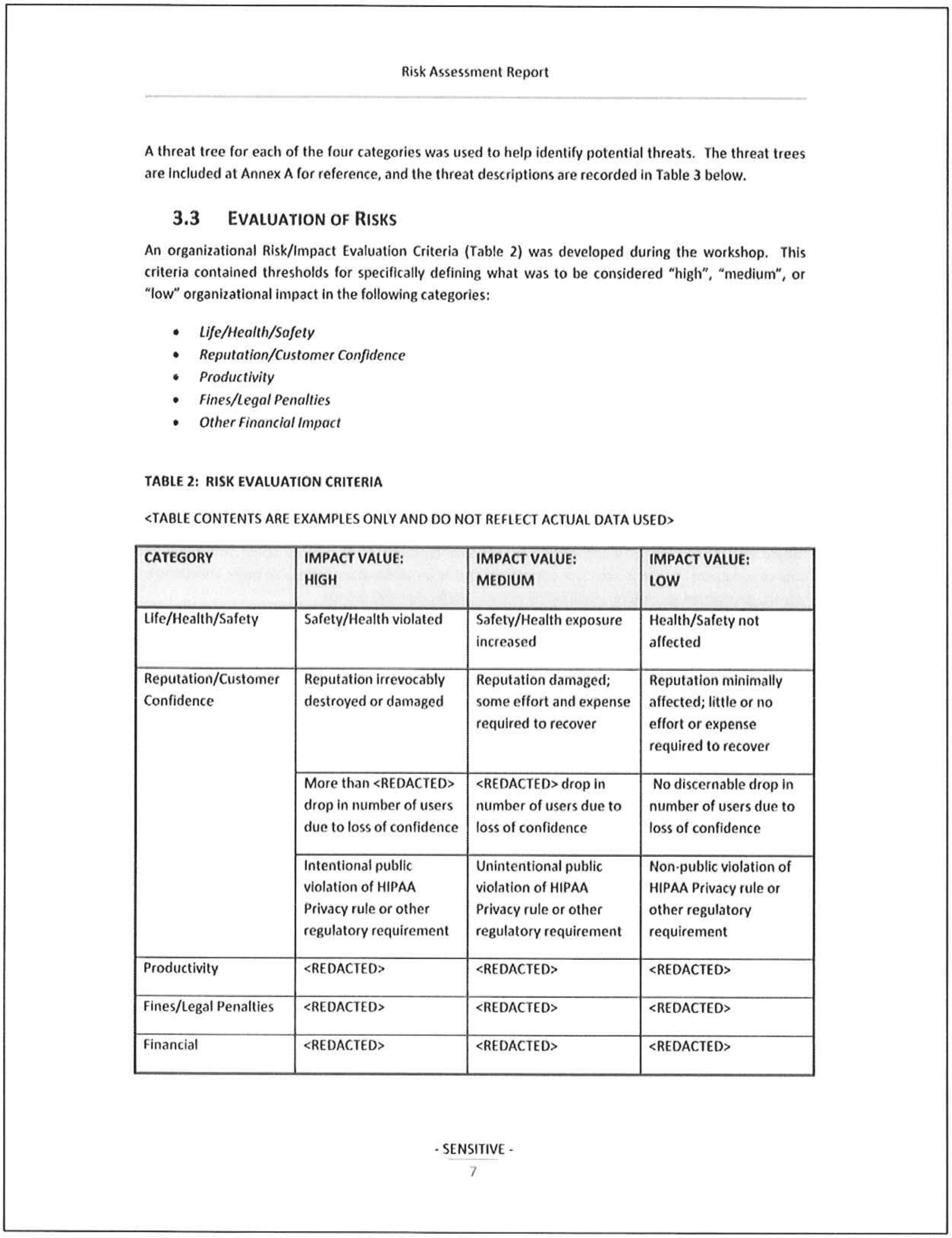
- *Accidental actions by people* – This group includes people inside and outside the organization who might accidentally harm the assets.

- *System problems* – These are problems with the information technology systems. Examples include hardware defects, software defects, unavailability of related systems, viruses, malicious code, and other system-related problems.

- *Other problems* – These are problems that are outside of <REDACTED>'s control. These can include natural disasters (e.g., floods and earthquakes) that can affect the organization's IT systems, unavailability of systems maintained by other organizations, and interdependency issues. Interdependency issues include problems with infrastructure services, such as power outages, broken water pipes, and telecommunication outages.

The resulting effects or outcomes of scenarios typically fall into the following categories:

- *Disclosure* or viewing of sensitive information
- *Modification* of important or sensitive information
- *Destruction or loss* of important information, hardware, or software
- *Interruption of access* to important information, software, applications, or services



A threat tree for each of the four categories was used to help identify potential threats. The threat trees are included at Annex A for reference, and the threat descriptions are recorded in Table 3 below.

3.3 Evaluation of Risks

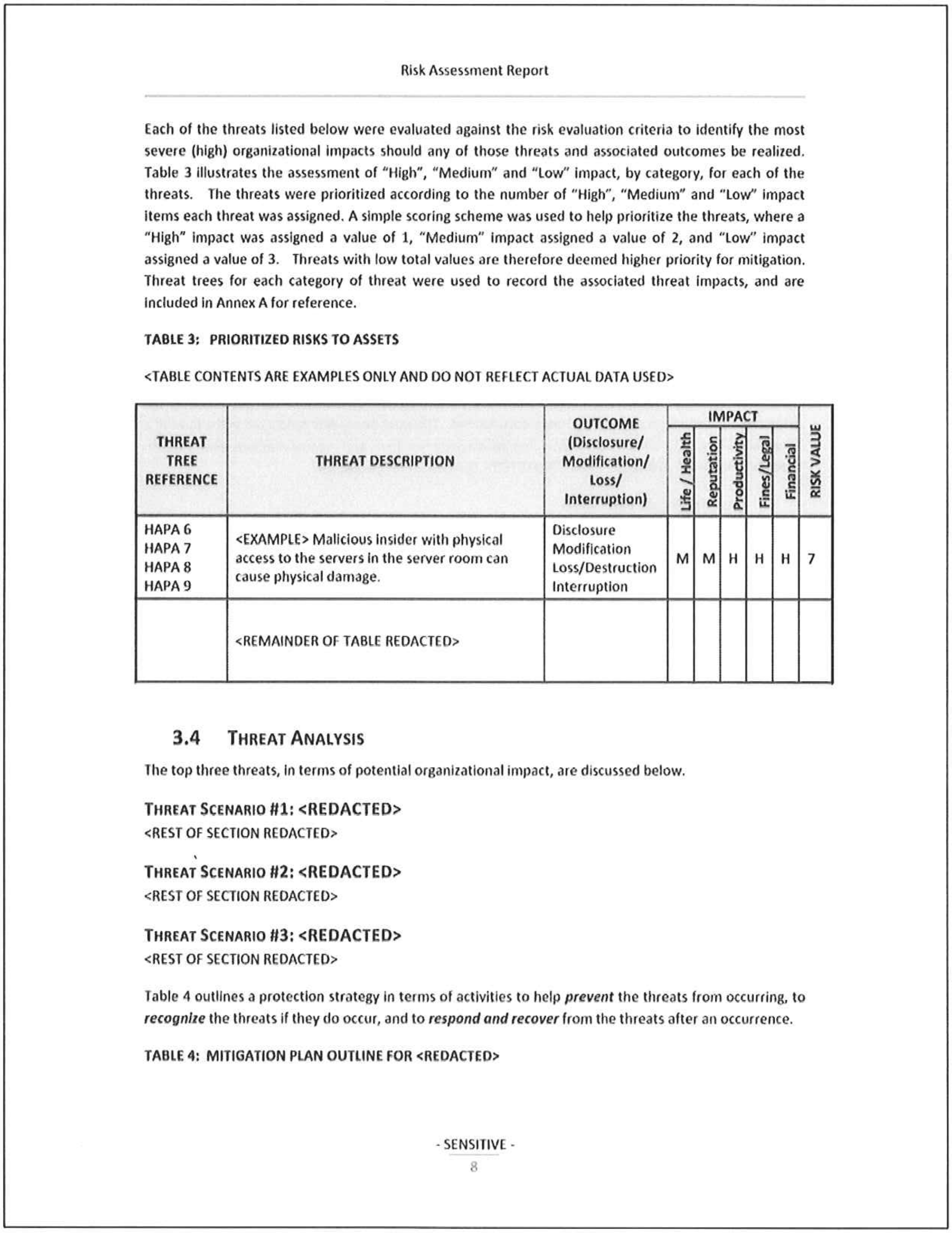
An organizational Risk/Impact Evaluation Criteria (Table 2) was developed during the workshop. This criteria contained thresholds for specifically defining what was to be considered "high", "medium", or "low" organizational impact in the following categories:

- *Life/Health/Safety*
- *Reputation/Customer Confidence*
- *Productivity*
- *Fines/Legal Penalties*
- *Other Financial Impact*

TABLE 2: RISK EVALUATION CRITERIA

<TABLE CONTENTS ARE EXAMPLES ONLY AND DO NOT REFLECT ACTUAL DATA USED>

CATEGORY	**IMPACT VALUE: HIGH**	**IMPACT VALUE: MEDIUM**	**IMPACT VALUE: LOW**
Life/Health/Safety	Safety/Health violated	Safety/Health exposure increased	Health/Safety not affected
Reputation/Customer Confidence	Reputation irrevocably destroyed or damaged	Reputation damaged; some effort and expense required to recover	Reputation minimally affected; little or no effort or expense required to recover
	More than <REDACTED> drop in number of users due to loss of confidence	<REDACTED> drop in number of users due to loss of confidence	No discernable drop in number of users due to loss of confidence
	Intentional public violation of HIPAA Privacy rule or other regulatory requirement	Unintentional public violation of HIPAA Privacy rule or other regulatory requirement	Non-public violation of HIPAA Privacy rule or other regulatory requirement
Productivity	<REDACTED>	<REDACTED>	<REDACTED>
Fines/Legal Penalties	<REDACTED>	<REDACTED>	<REDACTED>
Financial	<REDACTED>	<REDACTED>	<REDACTED>



Each of the threats listed below were evaluated against the risk evaluation criteria to identify the most severe (high) organizational impacts should any of those threats and associated outcomes be realized. Table 3 illustrates the assessment of "High", "Medium" and "Low" impact, by category, for each of the threats. The threats were prioritized according to the number of "High", "Medium" and "Low" impact items each threat was assigned. A simple scoring scheme was used to help prioritize the threats, where a "High" impact was assigned a value of 1, "Medium" impact assigned a value of 2, and "Low" impact assigned a value of 3. Threats with low total values are therefore deemed higher priority for mitigation. Threat trees for each category of threat were used to record the associated threat impacts, and are included in Annex A for reference.

TABLE 3: PRIORITIZED RISKS TO ASSETS

<TABLE CONTENTS ARE EXAMPLES ONLY AND DO NOT REFLECT ACTUAL DATA USED>

THREAT TREE REFERENCE	THREAT DESCRIPTION	OUTCOME (Disclosure/ Modification/ Loss/ Interruption)	IMPACT					RISK VALUE
			Life / Health	Reputation	Productivity	Fines/Legal	Financial	
HAPA 6 HAPA 7 HAPA 8 HAPA 9	<EXAMPLE> Malicious insider with physical access to the servers in the server room can cause physical damage.	Disclosure Modification Loss/Destruction Interruption	M	M	H	H	H	7
	<REMAINDER OF TABLE REDACTED>							

3.4 THREAT ANALYSIS

The top three threats, in terms of potential organizational impact, are discussed below.

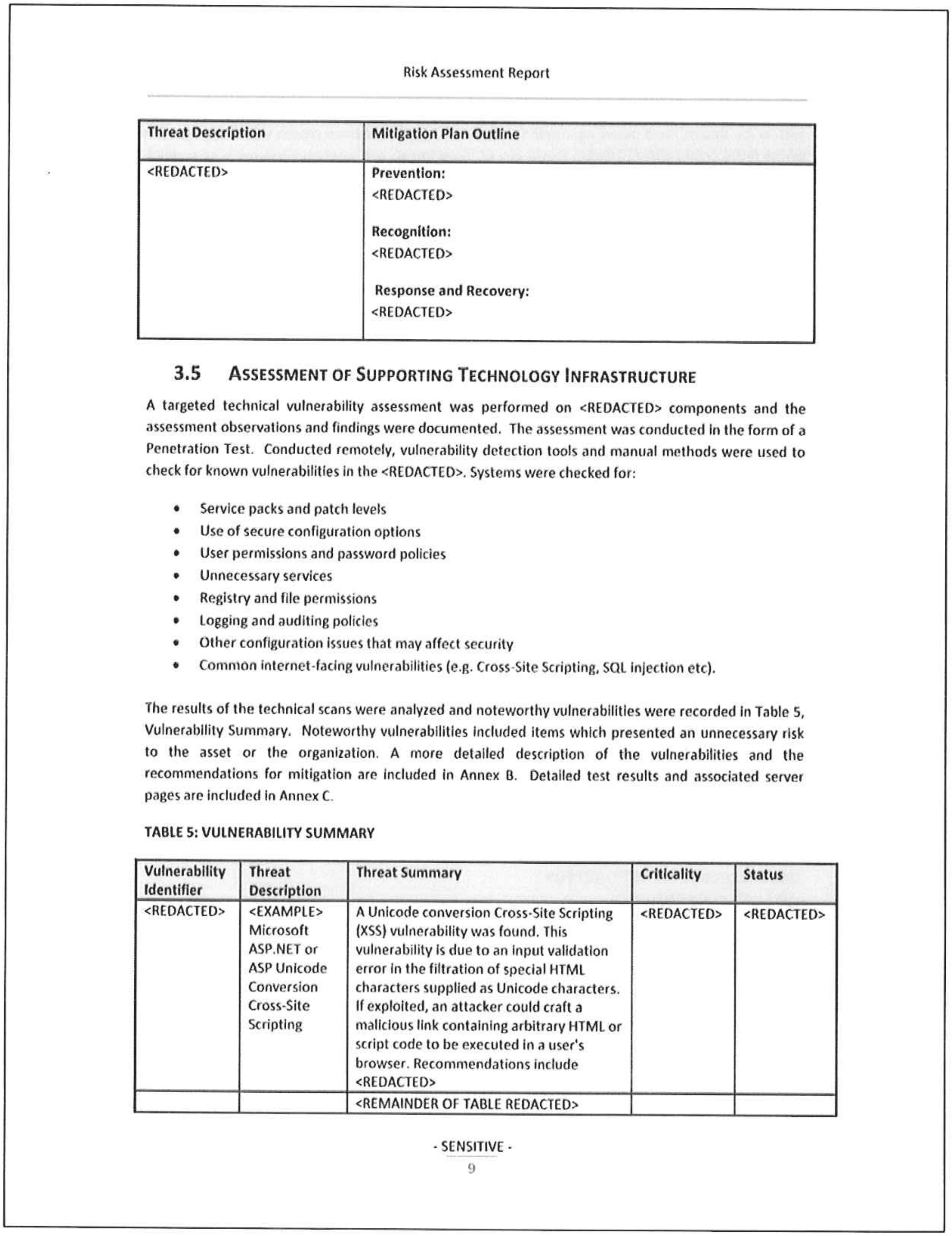
THREAT SCENARIO #1: <REDACTED>
<REST OF SECTION REDACTED>

THREAT SCENARIO #2: <REDACTED>
<REST OF SECTION REDACTED>

THREAT SCENARIO #3: <REDACTED>
<REST OF SECTION REDACTED>

Table 4 outlines a protection strategy in terms of activities to help ***prevent*** the threats from occurring, to ***recognize*** the threats if they do occur, and to ***respond and recover*** from the threats after an occurrence.

TABLE 4: MITIGATION PLAN OUTLINE FOR <REDACTED>



Threat Description	Mitigation Plan Outline
<REDACTED>	**Prevention:** <REDACTED> **Recognition:** <REDACTED> **Response and Recovery:** <REDACTED>

3.5 Assessment of Supporting Technology Infrastructure

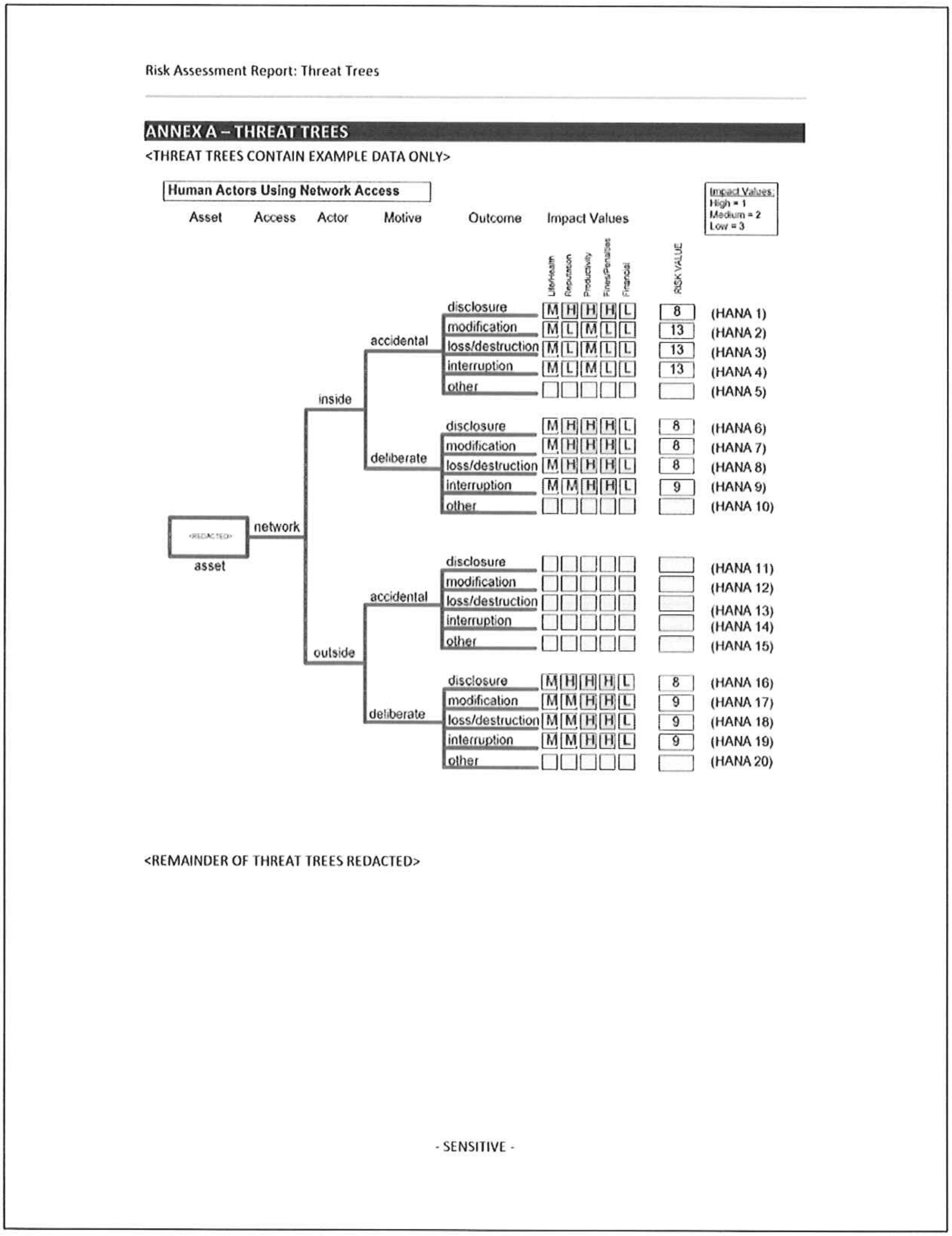
A targeted technical vulnerability assessment was performed on <REDACTED> components and the assessment observations and findings were documented. The assessment was conducted in the form of a Penetration Test. Conducted remotely, vulnerability detection tools and manual methods were used to check for known vulnerabilities in the <REDACTED>. Systems were checked for:

- Service packs and patch levels
- Use of secure configuration options
- User permissions and password policies
- Unnecessary services
- Registry and file permissions
- Logging and auditing policies
- Other configuration issues that may affect security
- Common internet-facing vulnerabilities (e.g. Cross-Site Scripting, SQL injection etc).

The results of the technical scans were analyzed and noteworthy vulnerabilities were recorded in Table 5, Vulnerability Summary. Noteworthy vulnerabilities included items which presented an unnecessary risk to the asset or the organization. A more detailed description of the vulnerabilities and the recommendations for mitigation are included in Annex B. Detailed test results and associated server pages are included in Annex C.

TABLE 5: VULNERABILITY SUMMARY

Vulnerability Identifier	Threat Description	Threat Summary	Criticality	Status
<REDACTED>	<EXAMPLE> Microsoft ASP.NET or ASP Unicode Conversion Cross-Site Scripting	A Unicode conversion Cross-Site Scripting (XSS) vulnerability was found. This vulnerability is due to an input validation error in the filtration of special HTML characters supplied as Unicode characters. If exploited, an attacker could craft a malicious link containing arbitrary HTML or script code to be executed in a user's browser. Recommendations include <REDACTED>	<REDACTED>	<REDACTED>
		<REMAINDER OF TABLE REDACTED>		



Risk Assessment Report: Threat Trees

ANNEX A – THREAT TREES

<THREAT TREES CONTAIN EXAMPLE DATA ONLY>

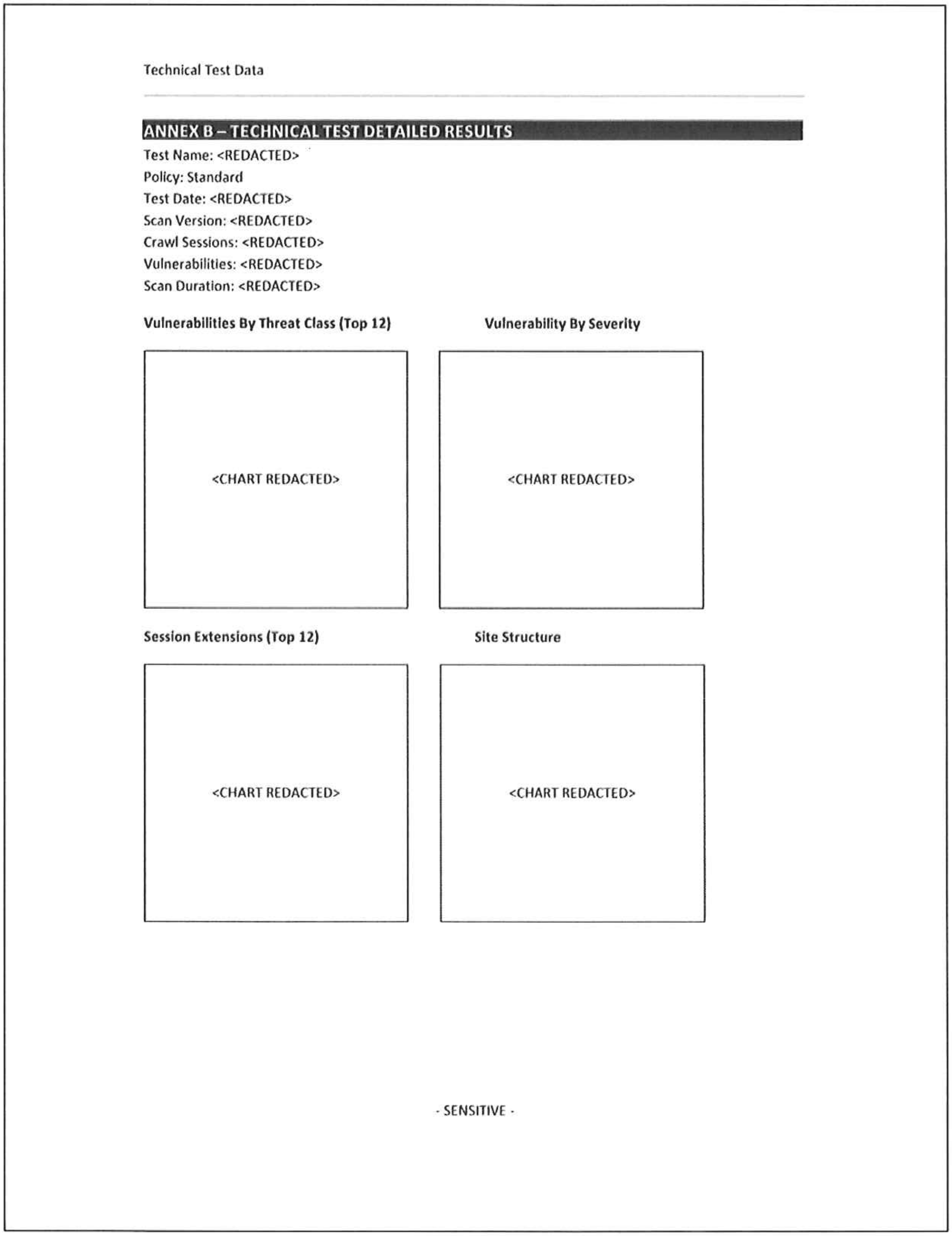
Human Actors Using Network Access

Impact Values:
High = 1
Medium = 2
Low = 3

Asset	Access	Actor	Motive	Outcome	Life/Health	Reputation	Productivity	Fines/Penalties	Financial	RISK VALUE	
<REDACTED> asset	network	inside	accidental	disclosure	M	H	H	H	L	8	(HANA 1)
				modification	M	L	M	L	L	13	(HANA 2)
				loss/destruction	M	L	M	L	L	13	(HANA 3)
				interruption	M	L	M	L	L	13	(HANA 4)
				other							(HANA 5)
			deliberate	disclosure	M	H	H	H	L	8	(HANA 6)
				modification	M	H	H	H	L	8	(HANA 7)
				loss/destruction	M	H	H	H	L	8	(HANA 8)
				interruption	M	M	H	H	L	9	(HANA 9)
				other							(HANA 10)
		outside	accidental	disclosure							(HANA 11)
				modification							(HANA 12)
				loss/destruction							(HANA 13)
				interruption							(HANA 14)
				other							(HANA 15)
			deliberate	disclosure	M	H	H	H	L	8	(HANA 16)
				modification	M	M	H	H	L	9	(HANA 17)
				loss/destruction	M	M	H	H	L	9	(HANA 18)
				interruption	M	M	H	H	L	9	(HANA 19)
				other							(HANA 20)

<REMAINDER OF THREAT TREES REDACTED>

- SENSITIVE -



Technical Test Data

ANNEX B – TECHNICAL TEST DETAILED RESULTS

Test Name: <REDACTED>
Policy: Standard
Test Date: <REDACTED>
Scan Version: <REDACTED>
Crawl Sessions: <REDACTED>
Vulnerabilities: <REDACTED>
Scan Duration: <REDACTED>

Vulnerabilities By Threat Class (Top 12)

<CHART REDACTED>

Vulnerability By Severity

<CHART REDACTED>

Session Extensions (Top 12)

<CHART REDACTED>

Site Structure

<CHART REDACTED>

- SENSITIVE -

Technical Test Data

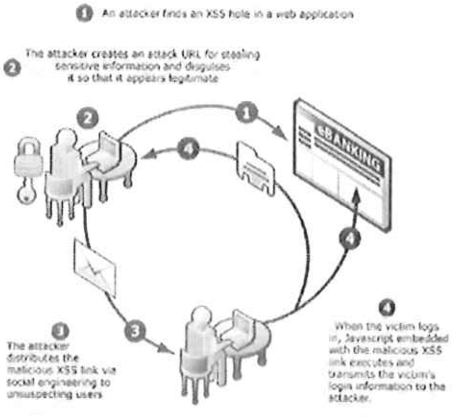
<EXAMPLE VULNERABILITY: CROSS SITE SCRIPTING

SUMMARY

XSS vulnerability found in <REDACTED> The following attack targets all browser(s) and was successful using plain encoding:

<ATTACK STRING REDACTED>

Cross-Site Scripting vulnerabilities were verified as executing code on <REDACTED>. Cross-Site Scripting occurs when dynamically generated web pages display user input, such as login information, that is not properly validated, allowing an attacker to embed malicious scripts into the generated page and then execute the script on the machine of any user that views the site. In this instance, <REDACTED> was vulnerable to an automatic payload, meaning the user simply has to <REDACTED> to make the malicious scripts execute. If successful, Cross-Site Scripting vulnerabilities can be exploited to manipulate or steal cookies, create requests that can be mistaken for those of a valid user, compromise confidential information, or execute malicious code on end user systems. Recommendations include <REDACTED>.


1 An attacker finds an XSS hole in a web application
2 The attacker creates an attack URL for stealing sensitive information and disguises it so that it appears legitimate
2
1
4
eBANKING
4
3
3 The attacker distributes the malicious XSS link via social engineering to unsuspecting users
4 When the victim logs in, Javascript embedded with the malicious XSS link executes and transmits the victim's login information to the attacker.

Execution:

<REDACTED>

Implication:

<REDACTED>

<REMAINDER OF APPENDICES REDACTED>

- SENSITIVE -