

State of West Virginia

Office of Technology

ORIGINAL

Response to Solicitation #: ISC2000000001 Amendment #2

Technical Proposal

Cyber Security Program

Submitted by

Security Risk Solutions, Inc.
698 Fishermans Bend
Mount Pleasant, SC 29464

(Tel) 843-647-1556

(Fax) 270-423-9104



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.

VENDOR: Security Risk Solutions, Inc.

DESIGNATED REPRESENTATIVE:

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

Tel: 843-647-1556, Fax: 270-423-9104, Email: jc@securityrs.com

DATE: 26 August, 2019

SIGNATURE:

A handwritten signature in black ink, appearing to read "Johnathan Coleman", is written over a horizontal line.

Security Risk Solutions, Inc.

698 Fishermans Bend
Mount Pleasant, SC 29464
Tel: (Tel) 843-647-1556



RECEIVED

2019 AUG 28 AM 9:37

WV PURCHASING
DIVISION

26 August, 2019

Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Attn: Jessica S Chambers

Proposal for State of West Virginia Office of Technology (WVOT) Cyber Security Pr

Dear Ms. Chambers,

Security Risk Solutions, Inc. is pleased to submit this proposal for solicitation ISC2000000001. 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 jc@securityrs.com
Incorporation Status	S-Corporation (South Carolina)
Years in Business:	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 and SIN 132-56

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

1. At time of printing/shipping our proposal, two addenda have 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. Upon award, Security Risk Solutions, Inc is both willing and able to perform the terms indicated in our proposal.
3. We hereby confirm acceptance of all Terms and Conditions as described, incorporated or referenced in the RFP.
4. Our online Representations and Certifications Application (ORCA) are current and up-to date.
5. We are submitting a Fixed Price proposal.
6. Our proposal will remain in full force and effect for 180 days from bid open date.
7. SRS is hereby identifying itself as a non-resident small business and women-owned business for consideration to be provided the same preference made available to any resident vendor under W. Va. CSR §148-22-9.

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

Sincerely,

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

Table of Contents

RFP §4.2: PROJECT GOALS AND MANDATORY REQUIREMENTS	2
§4.2.1: Goals and Objectives - Cyber Risk Program	2
§ 4.2.1.1 - Framework Development.....	2
§ 4.2.1.2 - Cyber Risk Program Documentation	5
§ 4.2.1.3 - Compliance Audit Solicitation	6
§ 4.2.1.4 - Governance, Risk & Compliance Tool Solicitation.....	7
§ 4.2.1.5 - Full Cyber Risk Program Implementation.....	8
§ 4.2.1.6 - Ongoing Support	10
§ 4.2.1.7 - Communication	11
§ 4.2.2 - Mandatory Project Requirements	12
§ 4.2.2.2 - Project Plan Legal Standing	12
§ 4.2.2.3 - Cyber Risk Program Adherence.....	12
§ 4.2.2.4 - Cyber Risk Program Documentation Ownership.....	13
§ 4.2.2.5 - Industry Standard Framework:.....	13
§ 4.3 - QUALIFICATIONS AND EXPERIENCE	15
§ 4.3.1 - Qualifications and Experience Information.....	15
§ 4.3.2 - Mandatory Qualification/Experience Requirements	26
Appendix A: Addendum Acknowledgement Form	A-1
Appendix B: State of West Virginia Purchasing Affidavit.....	B-1
Appendix C: Professional Certifications	C-1
Appendix D: Key Resumes	D-1

RFP §4.2: Project Goals and Mandatory Requirements

§4.2.1: Goals and Objectives - Cyber Risk Program

Security Risk Solutions, Inc., (SRS) is well versed in helping organizations identify, tailor, adopt and implement established cybersecurity standards. We have experience establishing cybersecurity frameworks within large private organizations and Government agencies, spanning a broad range of critical infrastructure sectors including healthcare, aviation, electrical infrastructure (power grid), and defense. **Our core business is Information/Cyber Security Risk Management for complex organizations.** SRS has been developing, refining, implementing, and transitioning Cybersecurity Programs to our clients for over 15 years, and is widely published and recognized as a leading industry expert. A partial list of our publications and national/international proceedings are available on our website, at www.securityrisksolutions.com. We are confident that our approach in identifying a suitable industry standard for WV, tailoring the standard to remove superfluous / inapplicable security controls, piloting the approach, and ultimately transitioning the framework to WV will provide the State with an efficient, repeatable, and self-sustaining cybersecurity program. We have done exactly this with other customers of similar or larger size and complexity.

§ 4.2.1.1 - Framework Development

Vendor should define an enterprise set of policies supported by a tactical framework aligned to a shared view of critical risk areas.

For this project, SRS proposes to work with WVOT to identify and select an established Cybersecurity Standard. SRS proposes a tailored version of the National Institute of Standards and Technology (NIST) Cybersecurity Framework¹ (CSF) be considered a strong candidate for the initial baseline/starting reference for this project. This voluntary Framework of standards, guidelines, and best practices to manage cybersecurity-related risk is becoming the defacto standard by which all other cybersecurity frameworks are being measured. SRS is participating in cybersecurity programs for Federal Agencies who are now cross referencing their cybersecurity programs to align with the NIST CSF. Within this proposed framework, SRS will help WV define and establish a set of policies, consistent with those already in use by the WV Office of Administration and other functional groups within WV, that will establish a mechanism for identifying, monitoring, and addressing cybersecurity risk in the State.

Looking ahead to the future adoption and implementation of a Governance, Risk, Compliance (GRC) tool, SRS will ensure that the tactical framework, overarching policies, and supporting implementation procedures can be readily utilized by a Commercial Off the Shelf (COTS) GRC tool.

Within the CSF, SRS will identify and document a specific methodology for conducting cybersecurity risk assessments. The methodology, supported by referenceable security controls (e.g. selected applicable controls from NIST Special Publication 800-53²) will be supported by procedures we develop to document processes that enable repeatable and objective assessment of an organization's security posture.

¹ <https://www.nist.gov/cyberframework>

² Security and Privacy Controls for Federal Information Systems and Organizations, <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>

§ 4.2.1.1.1: Identify most critical information assets and align to applications and agencies.

Immediately upon award, SRS will work with the West Virginia Office of Technology (WVOT) to schedule a project kick-off meeting. This meeting will address all aspects of program management to establish expectations for execution and delivery of the services. In addition, SRS will conduct a “critical information assets” working meeting with key representatives from WVOT. SRS will leverage our extensive experience in conducting critical information asset workshops to ensure time spent with senior management is efficient and productive, resulting in leadership buy-in which ultimately shape the parameters and scope for the rest of the project. Our experience in this regard includes refinement and implementation of two of the Software Engineering Institute’s (SEI) Computer Emergency Response Team (CERT) Risk Assessment Methodologies:

- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) methodology³, and
- Mission Assurance Analysis Model (MAAP®) – Assessing Risk in Complex Environments⁴

Note that SRS is NOT proposing to use these methodologies as the proposed tactical framework, but since **SRS has personnel who are acknowledged contributors to the SEI/CERT body of knowledge** in this domain, SRS is able to leverage this experience to ensure that the methodology chosen and tailored for WVOT is appropriate, efficient, and defensible. Using results from the “critical information assets” meeting to determine the scope and boundary for the rest of the project, SRS will provide WVOT with a “document request list” and discuss the organization and prioritization of the 210 entities within the departments. Findings will be documented and security categorizations will be applied based on the WVOT Data Classification⁵ levels already aligned with industry standard structures (FIPS 199 Security Categorization, etc.).

§ 4.2.1.1.2: Evaluate agencies with the highest risk exposure based off their assets and any mandated compliance requirements.

SRS will demonstrate how to conduct a comprehensive evaluation to ascertain the full risk exposure of the agencies and assets identified in the “critical information asset” meeting. This process will involve interviews with technical, operational, and administration staff in order to better understand and document cybersecurity risk at different hierarchical levels across differing functional groups within the enterprise. SRS will document the process used to evaluate risk, while ensuring full knowledge transfer from our team to WV staff members participating in the process.

§ 4.2.1.1.3: Develop and consolidate evaluation framework. Framework should account for maturity of varying organizations with option of 'tiering' framework alignment. Framework detail should be aligned with overarching State policies and standards.

As a matter of consistent practice, SRS deliverables and operational activities conform to applicable Federal, industry, and local jurisdictional standards and parameters in the creation of a risk management framework. 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 comprehensive Information Security Requirements Traceability Matrix (SRTM). An example representation/snapshot of a SRTM dashboard we developed for a large Federal Agency is shown in Figure 1.

³ <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473>

⁴ <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7505>

⁵ Based on West Virginia Office of Technology (WVOT) Data Classification Policy (Doc. Ref: WVOT-PO1006)

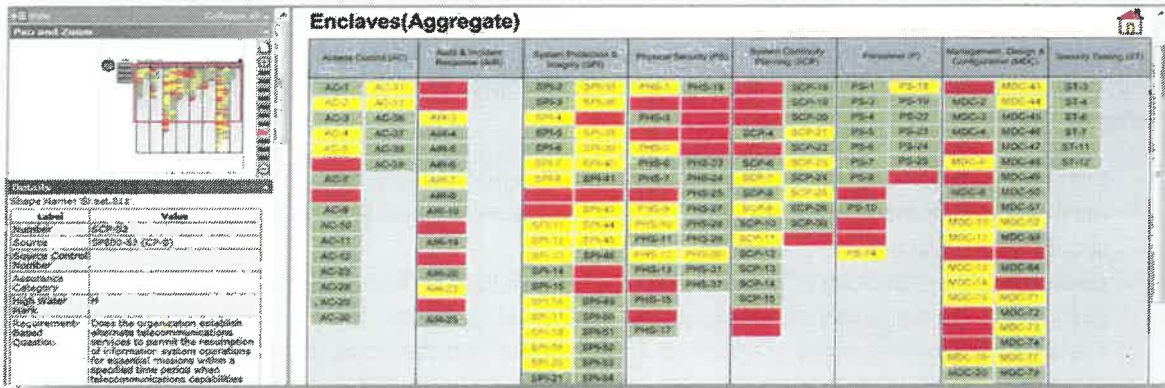


Figure 1: Risk Management Framework Tool (Snapshot)

The SRTM will be fundamentally based on a Framework adopt by WVOT, such as the NIST Cybersecurity Framework⁶, with additional security controls and tiers of requirements tailored to the security posture of agencies and/or groups of agencies within the state. Agency-specific criteria such as HIPAA/HITECH Security Rule requirements, or overlays with respect to WV law can be applied selectively to the SRTM, which will ultimately become the tactical set of security controls against which risk can be measured and documented in a GRC tool. This approach provides a tailorable, scalable, and consistent method of identifying compliance with a defined set of security controls, which in turn are mapped to Federal, State, or Agency requirements.

§ 4.2.1.1.4: Establish a Risk Profiling Procedure and pilot the results of the risk profile.

SRS will fully document the proposed, tailored, risk profiling procedure and work with WVOT to pilot the procedure as shown above. SRS will develop a set of “user guides” that describe *how* the framework is intended to operate, and will ensure that full knowledge transfer exists between the SRS team facilitating the process, and the WV representatives participating. SRS will incorporate lessons learned and feedback from the pilot into the methodology. As an example of our experience establishing and implementing cybersecurity risk assessment processes, SRS personnel authored (in conjunction with the SEI, the Advanced Technology Institute, and Georgetown University) a “train-the-trainer” guide and syllabus for use by the Department of Defense in training regional security officers to teach local security officers from over 200 facilities how to implement a risk assessment methodology in their environment. This program was hugely successful, and resulted in the DoD being able to adopt and successfully transition the risk assessment methodology into their own environment. In another program, SRS defined and implemented a Cybersecurity Risk Management program for the Airport Authority who runs the Charleston (SC) International Airport and other regional airports. This was based on the NIST CSF and incorporated controls from NIST SP 800-53, State requirements, and local policies and procedures. Collectively, this method was used to assess information security risk in the airport authority spanning from FAA and Police system interfaces to Payment Card Industry (PCI) security for airport terminal parking systems.

⁶ NIST Cybersecurity Framework, Version 1.1 <https://www.nist.gov/cyberframework/framework>

§ 4.2.1.2 - Cyber Risk Program Documentation**§ 4.2.1.2.1: Develop Policies and operations procedures, reporting templates, and program roadmap.**

SRS will build on experience in developing and implementing a Cyber Risk Program for large publicly traded corporations (such as McKesson Corporation), Government Agencies (including components of the Department of Defense), and numerous other large/complex organizations. We will fully document the program, by:

- Instantiating the new and existing policies and procedures into a tactical framework, showing how each technical control traces back to a policy requirement, regulatory requirement, or cyber security best practice.
- Coordinating the piloting of the assessment methodology with the selected state agencies.
- Facilitating the execution of the assessment with each pilot site.
- Fostering the development of a body of knowledge within the State, comprised of those individuals and agency representatives at all levels who participate in the pilots.
- Refining and evaluating the process, based on operational constraints, unique requirements, and practical experience with each participating agency.

The policies, procedures, worksheets, reporting templates, and all artifacts needed to successfully pilot the program will be furnished to WVOT and posted electronically (in the WVOT environment) for all stakeholders and participants to access as needed. We will exceed the minimum requirements of this task by not only ensuring that the documentation deliverables are first class, but that they are communicated effectively, tailored specifically for WV, and are able to be implemented by agency personnel. We believe knowledge transfer at this stage of the project is critical to the State's buy-in of the cybersecurity risk management program, and effective knowledge transfer/on-the-job training will help foster a culture of responsible cybersecurity risk management within the state.

§ 4.2.1.2.2: Define roles and responsibilities between central teams and agencies.

SRS personnel will adopt a "train-the-trainer" approach to ensure the knowledge transfer remains within each agency participating in the program. Similar to our approach for instituting a cyber security risk management program for over 200 DoD security officers around the world, SRS will work with WVOT to establish and maintain the following roles:

- SRS Role: SMEs will work with WVOT to lead develop of the processes, training materials, risk management implementation procedures, worksheets and artifacts. SRS will facilitate the process with the WVOT leads, pilots/early adopter POCs, and monitor/refine the processes during subsequent implementations.
- WVOT core team: SRS will help WVOT identify a core group of WV POCs who will serve as the long-term stakeholder leads for ultimate transition and ownership of the program. SRS will ensure the WVOT core team is comfortable with the procedures, artifacts, and training material so that the program can be fully adopted and maintained wholly by the State.
- Agency Leads: SRS will work with WVOT to identify leads within each agency who will be the primary Cybersecurity Risk Management representative and champion for their agency.
- Agency Team Members: SRS will support the WVOT and agency leads by helping them identify and train their own team members who will be responsible for implementing the various aspects of the program within their respective agencies.

§ 4.2.1.2.3: Document approach, tools, and templates for agencies to apply framework and manage audit and assessment activities.

SRS will use their experience developing OCTAVE® training materials, Train-the-Trainer content for DoD security officers, and requirements traceability processes (e.g. the Multi-Dimensional Resiliency Model we co-developed for the National Reconnaissance Office and Army National Guard Bureau) to ensure a concise yet sufficiently detailed methodology is documented for use by the agencies. This includes the development of a shared knowledge resource for state employees to access, a logical flow/model of the steps required for implementation of the methodology, and the templates required for agencies to capture their decisions (for due diligence) and for reporting the results. SRS will work with WVOT to establish expectations for execution / implementation of the methodology within each pilot site or participating site, including establishing phases for each step which includes on-the-job training and just-in-time training for each phase of the assessment, reporting requirements, opportunities to provide feedback, and review of the materials/artifacts being produced at each pilot site.

§ 4.2.1.2.4: Pilot the program with at least one small and one large agency.

SRS will work with at least two pilot agencies to implement the processes as described above. SRS will conduct the “train-the-trainer” sessions with the WVOT core team and the Agency representatives to teach/empower each pilot to be responsible and have ownership of their own process. That said, recognizing the importance of successful completion of pilot activities, SRS will work very closely with the WVOT core team and with each pilot to ensure they are continuing to make satisfactory progress and can benefit from the broader team’s experience in conducting similar assessments.

§ 4.2.1.2.5: Assess the results and document lessons learned from Pilot program. Remediation of issues should be accounted for in the milestones and deadlines.

SRS will objectively review the results from each pilot, including the interim artifacts, worksheets, process steps, and effectiveness of the program. Results will be reviewed with WVOT and any areas of the methodology or process artifacts that have been identified for improvement will be addressed. In addition to the review/assessment of the effectiveness of the risk management framework and methodology, SRS will work with the pilot sites and WVOT to help them identify appropriate mitigation strategies to the risks (ranked by impact) that they identify through the course of their pilots.

§ 4.2.1.3 - Compliance Audit Solicitation

§ 4.2.1.3.1: Assist WVOT in developing solicitation.

As a vendor neutral organization that does not resell any third party software, hardware or systems, SRS has conducted numerous impartial compliance audits for various customers – commercial and government. SRS will conduct the necessary market research, using various techniques (including Requests for Information where appropriate) to appropriately specify the requirements for a comprehensive yet achievable compliance audit procurement. SRS understands that it will not be eligible to bid on the compliance solicitation, but will leverage it’s experience in conducting compliance audits to help ensure that the compliance audit solicitation specifically addresses the necessary components of the cybersecurity risk management program. SRS will help draft and review the solicitation, and will provide feedback based on real experience and our understanding of the legal/policy framework that supports it.

§ 4.2.1.3.2: Vendor should provide expertise in identifying, analyzing and evaluating agency risk and applying the appropriate security controls relevant to the information custodians.

SRS has significant expertise implementing a number of different IT risk assessment and cybersecurity assessment methodologies, including the HIPAA/HITECH Security Risk Assessment conducted by SRS for the State of West Virginia Public Employees Insurance Agency (WV PEIA). During that effort, SRS demonstrated our ability to identify technical, physical, and administrative (organizational) risk and to help develop and implement corresponding mitigation plans. SRS will leverage this expertise and institutional knowledge of the WVOT environment to ensure the compliance audit solicitation includes appropriate requirements for assessing compliance with the requisite security controls selected in the framework. We will ensure that the appropriate security controls are assigned to information custodians within agencies that have functional responsibility for implementing those controls.

§ 4.2.1.3.3: Review vendor responses and advise reviewers.

SRS has experience conducting reviews of vendor responses and for acting in an advisory capacity to a selection committee. SRS has experience reviewing proposals for Government clients, providing objective evaluation, and providing scoring and recommendations based on vendor responses. For example, SRS recently helped the US Department of Health and Human Resources review a number of vendor responses to their "Challenge Grants", where the Government awarded money to vendors based on their technical proposals and ability to implement/demonstrate associated capabilities. SRS understands the careful conflict of interest requirements in making sure that any reviews of vendor responses are strictly confidential and that no perceived or actual conflicts of interest may arise. Furthermore, SRS understands and respects our role as advisors, and that we have no authority or implied authority for source selection activities on behalf of the Government.

§ 4.2.1.3.4: Provide guidance and assistance to WVOT to process and assist agencies in using the solicitation.

SRS will work with WVOT to ensure that agencies are aware of the scope of the solicitation, expected outcomes/deliverables of the solicitation, and how the results of the work obtained through the solicitation can help them improve their cybersecurity posture and validate their implementation of the risk management program.

§ 4.2.1.4 - Governance, Risk & Compliance Tool Solicitation

§ 4.2.1.4.1: Assist WVOT in developing a solicitation for a governance tool.

SRS has experience in helping agencies develop requests for information for technical products, tools, and subsequent support, including for GRC tools. SRS has considerable experience in the evaluation of different cyber security tools, and has experience evaluating, implementing, and tailoring a variety of GRC tools. For example, SRS worked with DoD customers to review a number of GRC tool demonstrations and to pilot GRC implementations at the DoD Space and Naval Warfare Center (SPAWAR). As another example of our experience implementing enterprise-wide GRC tools, SRS worked with McKesson Corporation (a large, international corporation) to tailor the risk assessment methodology and GRC tool (Archer) controls to create a standardized assessment and reporting capability for their subsidiary business units to use. The business units were given the option to conduct the assessments and complete their risk assessment reports in-house using the centrally provided GRC tool, or to leverage the SRS team's expertise to facilitate their assessments (with a service-center/fee approach) with McKesson Corporate. SRS will make sure the GRC solicitation includes appropriate requirements for tailoring the security controls and the

methodology in a way that aligns with the Cybersecurity Framework proposed by SRS, yet remains tailorable so that additional controls or refinement can be readily implemented by WVOT in years to come. Examples include the ability to customize reports, create new standardized reports, or refine reporting dashboards.

§ 4.2.1.4.2: Implement the governance tool to support future assessment.

SRS will work with WVOT to institutionalize use of the GRC tool procured by the State. This will include ensuring that the policies and procedures implemented as part of the cybersecurity risk assessment program require utilization of the GRC tool (where appropriate) for compliance tracking, reporting, and plan of action and milestone (POA&M) tracking. SRS will ensure the cybersecurity risk assessment methodology aligns with the GRC tool capabilities and vice-versa, to enable effective implementation without duplication of effort or overly burdensome assessment steps.

§ 4.2.1.4.3: Establish baseline security and use procedures for the tool.

Recognizing the potential sensitivity of the aggregate security risk information and documented vulnerabilities identified by the agencies while conducting their assessments, SRS will work with WVOT to ensure the baseline security for the tool (hosting, storing reports, data access, user access control etc.) are properly documented and implemented, and are consistent with state requirements for data security.

§ 4.2.1.4.4: Customize the tool to align with state specific requirements established during programs development.

SRS will ensure that the GRC tool vendor selected by WV works with the SRS SMEs to make sure any tool customization is clearly aligned with the processes defined in the Cybersecurity Framework and associated assessment methodologies developed for the agencies. Furthermore, SRS will ensure that the GRC tool allows for WVOT to have the capability to make tailoring changes as needed (e.g. developing standardized reports for agencies to use).

§ 4.2.1.4.5: Train users to utilize the governance tool and develop policies and procedures for the governance tool.

SRS will work with WVOT to ensure that GRC tool users understand how to use the tool in the context of the State Cybersecurity Framework. For example, SRS will train and demonstrate how users can record threats to critical information assets, identify impact levels, and assign overall risk scores to the threats they identify. SRS will help users understand how to develop and record mitigation strategies, and tie them to their POA&Ms to ensure progress is made in mitigating the risks.

§ 4.2.1.5 - Full Cyber Risk Program Implementation

§ 4.2.1.5.1: Include a communications plan.

SRS will develop a phased implementation plan to institutionalize the Cyber Security Program. The plan will include resources, timelines, dependencies, and will build on the pilot results and experiences. It will describe to the agencies who, how, where, and when the Cybersecurity Program will be rolled-out, and will include expectations and commitments required from agency personnel in order for them to be successful. SRS will help WVOT prioritize the order of participation by each agency (or group of agencies) by utilizing information learned from the "information asset identification" step described earlier. That

information, combined with input from WVOT and Department of Administration leadership will be used to develop a plan for incremental adoption across the agencies.

§ 4.2.1.5.2: Include education and enablement of tools

Full implementation of the program will include training for users:

- Just-in-time training for individuals participating in leadership or group activities
- Self-directed training for participants by reading the process documentation we will develop
- Train-the-trainer sessions for those WVOT and agency participants who will have a long-term ownership role in maintaining the program
- Specific training to address any problem areas encountered by pilots (e.g. risk scoring, or documenting results in the GRC tool).

§ 4.2.1.5.3: Incrementally expand pilot program

As described earlier, SRS will adopt a phased, incremental approach to full implementation. This includes expanding the initial group of participants (WVOT core team and Agency Representatives) who prioritized the information assets according to criticality to the first two pilot agencies (one small and one large). From there, SRS will help WVOT expand the program by implementing the communications plan, championing utilization of the process and artifacts, and providing the necessary support needed for the WVOT to help the agencies succeed. SRS has demonstrated experience implementing and expanding programs of this nature. For example, SRS developed a training program for the State of Alabama to use to train their IT Risk Assessment personnel across the state on how to conduct risk assessment that meet Federal requirements for HIPAA/HITECH Risk Assessments. SRS worked with the Alabama Regional Extension Center (AL-REC) to develop the methodology, train champions, and provide second and third tier support to the champions as they implemented the methodology throughout the state. SRS was able to help Alabama incrementally expand the program throughout the state using this approach.

§ 4.2.1.5.4: Plan for framework deployment and audit execution across the enterprise

SRS will work with the WVOT and agencies to promote use of the Compliance Audit solicitation and GRC Tool solicitation to help agencies fully implement and validate their cybersecurity programs.

§ 4.2.1.5.5: Include the performance of audit of enterprise services

SRS will help the WVOT utilize the compliance audit contract to not only obtain third party evaluations of agency compliance with the security controls, but to feed that information back into the cyber security program itself. SRS has experience implementing feedback cycles into the cybersecurity frameworks and security programs it has developed. For example, for the DoD, SRS was able to help facilities compare results of their security posture assessments with those of other facilities. At the aggregate level, higher level (regional) representatives were able to view trending and identify organizational deficiencies that were affecting more than one facility or institution. Using these techniques, SRS will be able to help WVOT leverage the results of enterprise audit services to identify additional services, tools or training that may be needed more broadly across the state. Examples include anti-phishing education or phishing awareness testing across the state.

§ 4.2.1.5.6: Support agencies with utilizing the third-party vendor contract to perform assessments

As previously described, SRS will ensure the Cybersecurity Program includes utilization of the audit services contract, and will assist agencies who use the audit compliance contract by showing them how to produce evidentiary artifacts which show compliance with the security controls.

§ 4.2.1.6 - Ongoing Support**§ 4.2.1.6.1: Ensure that its Cyber Risk Program services are trackable in accordance with WVOT charge back model**

SRS will work with WVOT to develop a tiered program of services that cover the projected operational expenses of the program. These expenses may include the consultant costs, time/costs associated with WVOT Core Personnel, and will be attributable to each agency or group conducting assessments. This will include setting appropriate job/codes for each assessment being conducted, and for each phase of the assessment.

§ 4.2.1.6.2: Identifying appropriate points for fee assessment

There are a number of potential points for assessment of fees. SRS will work with WVOT to clearly define appropriate points and the level of effort/fee associated with each assessment point. Examples include:

- Conclusion of Phase 1 of an assessment: Asset identification, criticality, and prioritization
- Conclusion of Phase 2: Identification of threats (technical, operational, physical, environmental etc.) and assignment of potential impact level according to risk criteria/scoring rubric.
- Conclusion of Phase 3: Development of mitigation plans, POA&M, and supporting report documents
- Increments of additional support from consultants, and/or WVOT core team personnel
- Utilization of WVOT personnel in providing support to agencies for GRC tool, and support on the compliance audit contract

§ 4.2.1.6.3: Assist WVOT in establishing pricing for various aspects of the Cyber Risk Program.

SRS will help WVOT estimate level of effort for each phase of the Cybersecurity Risk Program, allowing appropriate pricing to be developed for blocks of time, deliverables, and / or phases of program implementation by agencies.

§ 4.2.1.6.5: Recommendations should take into considering cost-sharing and economies of scale

SRS will identify cost-sharing opportunities, which may include joint/inter-agency efforts, such as:

- Critical Asset Identification meeting
- Sharing of threat information for assets with joint/shared utilization (e.g. shared network infrastructure, shared physical security controls, shared IT contingency plans for data center activities, shared processes for HR/background check procedures etc).
- Collaborative efforts where the program supports combined/joint participation by more than one government organization (agency), such as a department.

§ 4.2.1.6.6: Implemented and delivered as an enterprise/managed service, addressing cyber workforce challenges

SRS recognizes that agencies or even departments may not have the requisite skills, training, time, or resources to implement a compliant cybersecurity program without assistance from WVOT and the successful awardee of this contract. To that end, SRS will ensure that economies of scale, re-use of artifacts, and systematic repeatable processes are documented, implemented, and fully transferred. There is a delicate balance between having a vendor “do the assessment” which may then end up as shelf-ware, vs. being too theoretical and not enabling the Government to successfully implement. SRS strikes this balance by providing comprehensive documentation of the processes, that are intuitive and iterative. We facilitate the implementation of these processes by conducting pilots *with* Government representatives, thereby ensure knowledge transfer of the processes from our team to the Government, while allowing the Government to have ownership and buy-in to the content. Where we identify areas for re-use of risk information (e.g. compliance with security controls in a data center), the results and rationale will be provided to the agency or department along with the justification for the findings. This enables the agencies to work hand-in-hand with WVOT’s centrally managed services, and receive full value and understanding for previously charged-back shared services they are benefiting from.

§ 4.2.1.7 - Communication**§ 4.2.1.7.1: The State can apply custom branding to all documents and materials.**

SRS will provide source files (e.g. Microsoft Word documents, Visio flow-charts etc.,) for all documents and materials to allow WVOT to apply custom branding at their discretion. Any reference material/sources cited will include full citations and references. Proprietary/third party licensed content will not be used unless specifically requested by WVOT and approved by the license holder. Open source, Government, or other public domain information (e.g. threat data) will be utilized wherever possible. Methods and techniques adopted during the development of the framework will be based on industry standards and widely recognized best practices, and will not be considered by SRS to be proprietary.

§ 4.2.1.7.2: Vendor should establish regular communications to discuss project status at a minimum of every two (2) weeks

Upon award, SRS will establish a bi-weekly conference call (or weekly if requested by WVOT) for distribution to all stakeholders. SRS will provide follow-up weekly meeting minutes within one business day for review and comment by stakeholders. Furthermore, SRS will utilize project management practices consistent with The Program Management Institute’s (PMI’s) Body of Knowledge®, thus allowing for programmatic risk to be monitored and addressed, and effective communication and project progress to be demonstrated. We have certified Project Management Professionals on staff who will be responsible for day to day management of project tracking artifacts.

§ 4.2.1.7.3: Vendor should provide communications to different levels of stakeholders identified in the project proposal

SRS will provide, through regular reporting, communications to different levels of stakeholders as identified in the project plan. This will include reporting on project deliverables (status), risks relating to contract deliverables, financial status reporting, and leadership communications such as executive level briefings or findings reports.

§ 4.2.1.7.4: Vendor should provide on-site support for major milestones and project initiatives

SRS will ensure that major milestones (e.g. executive level briefings, presentation of findings, group sessions with agencies for mitigation planning, etc.,) are attended on-site.

§ 4.2.2 - Mandatory Project Requirements

SRS agrees that all mandatory project requirements will be met, and also proposes to exceed them as described in each section below:

§ 4.2.2.1 - Project Timeline: *The proposed project timeline must be provided with key goals and objectives within the first sixty (60) working days following award of a contract.*

SRS will develop a comprehensive project plan and deliver within the mandatory time period.

Exceeds Requirement: In addition, SRS will include a program project plan and maintain it for the life of the project. The project plan will include resources, responsibilities, and dependencies, and will be provided in editable format allowing it to be maintained and updated. Furthermore, SRS proposes to provide WVOT with a draft project plan within thirty days of project award to afford the Government the opportunity to provide review and comment before it is finalized as the baseline timeline and submitted by SRS.

§ 4.2.2.2 - Project Plan Legal Standing

SRS will ensure the project plan complies with applicable West Virginia state and federal laws.

Exceeds Requirement: SRS proposes that one of our key personnel, Amber Patel L.L.M. conduct an analysis to identify and document applicable State and Federal project plan requirements. Ms. Patel is an experienced Project Manager and has a post-graduate degree of Latin Legum Magister (LLM) which means Master of Laws. The resulting analysis will be provided to WVOT.

§ 4.2.2.3 - Cyber Risk Program Adherence

SRS agrees that all mandatory project requirements will be met, and also proposes to exceed them as described in each section below:

§ 4.2.2.3.1: *The program must enable a 3-tiered organizational hierarchy allowing for cyber risk ownership to be assigned to a single government organization (agency), a collection of government agencies (department) and the collection of government departments (state).*

As described in our response to § 4.2.1.6.1, SRS will work with WVOT to develop a tiered program of services that maximizes efficiencies and allows agencies and departments to share/collaborate on certain tasks within the Cybersecurity Program.

Exceeds Requirement: In addition to enabling a 3-tiered organizational hierarchy, SRS will enable further flexibility and opportunities for efficiencies by allowing re-use of shared artifacts by multiple agencies (e.g. agencies and departments utilizing a shared data center, shared HR hiring/termination procedures, shared physical security requirements).

§ 4.2.2.3.2: *The program must account for the standardization of the impact risk variable.*

SRS will include a standardized rubric for the impact risk variable. SRS has experience defining the initial rubric (through collaboration with stakeholders and senior leadership) during the project kickoff meeting and “information asset identification” meeting.

Exceeds Requirement: SRS has demonstrated experience identifying a standardized mechanism to assess risk that removes bias and allows for threats to be measured according to organizational impact, severity, and likelihood of occurrence. There are a number of well documented methods to do this, including those described in NIST Special Publication 800-30 (Guide for Conducting Risk Assessments) Appendix H (Impacts). SRS has experience implementing this approach for Government Agencies, as well as the OCTAVE® method for prioritizing risks. SRS proposes to adopt a tailored approach of the NIST 800-30 method for this work.

§ 4.2.2.3.3: The program must include the capability to leverage both qualitative and quantitative risk assessments and provide recommendations how to effectively and efficiently leverage both

SRS will include the capability to leverage both qualitative and quantitative risk assessments and to provide recommendations on how to leverage both. For example, SRS proposes to use these impact descriptions from NIST SP 800-30 Appendix H (which is qualitative) as a starting baseline and enhance it by adding a numeric scale for each impact category in order to provide a quantitative score for each identified threat. This tailoring allows what would otherwise be qualitative risks to be prioritized according to score, and to also group ranges of scores into categories of “high”, “medium” and “low” as applicable.

Exceeds Requirement: SRS will ensure that tailoring to include quantitative prioritization (by impact score) of qualitative threat scenarios will align with typical scoring of risks in GRC tools, ensuring future compatibility between the Cybersecurity Framework method and the tools that will likely be in consideration for future use.

§ 4.2.2.4 - Cyber Risk Program Documentation Ownership

SRS agrees that all documentation and materials associated with the development and implementation of the Cyber Risk Program will be owned by the State of West Virginia. SRS will ensure that all raw materials and workflow diagrams etc. are not branded so that they may be customized by the State as needed.

Exceeds Requirement: SRS will provide all artifacts in native, editable format to enable WVOT to apply its own branding as needed. SRS will also ensure that any third-party references (e.g. to NIST Special Publications or to regulatory requirements) are properly cited. This will ensure no inadvertent assumption of authorship and that full traceability to the appropriate sources of security controls, best practices, or other requirements are appropriately preserved. This is an important aspect of any credible Cybersecurity Program, as compliance with National Standards, well known industry best practices, and regulatory requirements must all be traceable if the program is to have credibility and standing in its own right.

§ 4.2.2.5 - Industry Standard Framework:

SRS agrees wholeheartedly that the project MUST be based on an industry standard framework, such as the Cybersecurity Framework, and that it be selected by the State of West Virginia. As described earlier, being able to reference an industry standard framework is an important aspect of any credible Cybersecurity Program. Compliance with National Standards, well known industry best practices, and regulatory requirements must all be traceable if the program is to have credibility and standing.

Exceeds Requirements: SRS has extensive experience developing crosswalks between numerous industry frameworks, including the NIST Cybersecurity Framework, NIST SP800-53 (Security and Privacy Controls for Federal Information Systems and Organizations), NIST SP800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations), and requirements from various regulatory frameworks such as the HIPAA Security Rule. As a recent example, SRS helped a workgroup from the

Federal Health Architecture (Work Group of Office of General Counsel and Policy representatives from approximately 10 Federal Agencies) cross-walk technical and policy requirements from the HIPAA Security Rule, the NIST Cyber Security Framework, and NIST SP800-171. Agencies represented included the DoD, Department of Veterans' Affairs (VA), HHS Office of Civil Rights (OCR), HHS Office of the National Coordinator (ONC), Social Security Administration (SSA) and Indian Health Service (HIS). SRS was able to successfully demonstrate the overlap between proposed security requirements in the draft HHS/ONC Trusted Exchange Framework and Common Agreement (TEFCA) and the proposed requirements of the Federal Acquisition Regulation (FAR) 52.204-21 as it pertains to NIST SP800-171. Based on this experience and the expected changes to FAR 52.204-21, SRS is well positioned to help the State of West Virginia make an informed, forward-thinking selection.

§ 4.3 - Qualifications and Experience

SRS is a small, woman owned business that has been providing Cybersecurity Framework related services for over 15 years. Information Security Risk Management and the associated tasks of security control selection, implementation, mitigation, and continuous monitoring is our core business. We do not resell any third-party solutions, software, or products, and as such remain completely impartial and able to provide professional and honest consulting services.

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, CBCP, CBRM, Security+, CRISC and PMP. Copies of a sampling of staff certifications and degrees applicable to this project are attached at Appendix C, 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 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 Security Risk Assessments. 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:

- **Meaningful Use Risk Assessments: Requirements, Methodology, Challenges and Lessons**, J.Pritts, JD (HHS/ONC Chief Privacy Officer) & J.Coleman: HIMSS 2014 Conference and Exhibition, Orange County Convention Center, February 25, 2014
- **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.
- 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 the "NIST/CMS Workshop on HIPAA Security Rule Implementation and Assurance" (January 16, 2008; NIST Main Campus, Gaithersburg, MD; and a Presentation on behalf of the Office of the National Coordinator for Health Information Technology (ONC) for the first Nationwide Health Information Network Forum on Functional Requirements for Security; Authorization, Authentication, Confidentiality, and Credentialing (June 28-29, 2006; Natcher Center, National Institutes for Health).

§ 4.3.1 - Qualifications and Experience Information

§ 4.3.1.1: Vendor should specify previous experience in deploying and developing Cyber Security Risk Programs, preferably with government organizations. Vendor should include the scope of programs implemented. Vendor should also include any contacts at the specified entity who can be contacted for verification.

Table 1, below, provides a snapshot of some of our qualifications and experience in developing Cyber Security Risk Management programs. In some cases, contact information for personnel at the client site has been omitted in order to preserve the confidentiality of their identities. The information will be included as clarifying information during oral presentations, if requested.

Table 1: Relevant Project Experience

Client/Location	Project Focus	Reference Name/Contact Info	Relevance to Solicitation		
			Cybersecurity Risk Assessment	Policies and Procedures Review	Compliance with Frameworks/Standards/Best Practices
WV PEIA	Develop and implement information security risk assessment process for HIPAA/HITECH security. Review policies and procedures and map to regulatory requirements.	Thomas D. Miller, MA, LPC, ALPS, ADC Privacy & Security Officer West Virginia Department of Administration West Virginia Public Employees Insurance Agency Tel 304-558-7850, Extension 52663 thomas.d.miller@wv.gov	✓	✓	✓
McKesson	Implement Cybersecurity Risk Assessment Program	Ted LeSeur +1 480-381-3522, ted@cyberriskhelp.biz	✓	✓	✓
National Reconnaissance Office and US Navy	Develop and Implement Cybersecurity Risk Management Framework and Processes. Pilot methodology.	Will be provided upon request	✓	✓	✓
Army National Guard Bureau Risk Management Framework for ESS	Develop and Implement Cybersecurity Risk Management Framework for ESS systems throughout USA	Will be provided upon request	✓	✓	✓
Comparative Billing Reports (CBR) Producer System for the Centers for Medicare & Medicaid Services (CMS)	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 facilities throughout USA, Asia and Europe	Security Testing and Evaluation, Risk Assessment, Compliance, and IT Contingency Planning for 29 Major Hospitals and 27 Major Information Systems, with approximately 55,000 users and 86,000 end nodes.	Will be provided upon request	✓	✓	✓
Georgetown University Medical Center (GUMC)/ Washington DC	Information Security Risk Assessment – Global Argus System	Jeff Collmann, PhD collmanj@georgetown.edu Tel: (202)-870-2196	✓	✓	✓

Client/Location	Project Focus	Reference Name/Contact Info	Relevance to Solicitation		
			Cybersecurity Risk Assessment	Policies and Procedures Review	Compliance with Frameworks/Standards/Best Practices
Princeton Healthcare System/ Princeton, NJ	HIPAA Security Risk Assessment	Cornelia Dorfschmid cdorfschmid@strategicm.com Tel: (703) 683-9600, x.419	✓	✓	✓
Department of Veterans' Affairs (VA) Post 9/11 Veterans Benefits Program (Chapter 33), and Joint Federal Health Care Center (FHCC)/ Washington DC/ Charleston SC/ Chicago IL	Large-Scale Risk Management for major information systems (\$250M project)	Will be provided upon request	✓	✓	✓
National Institutes of Health (NIH) / Bethesda, MD	Federal Safety Reporting Portal (SRP) Technical Risk Assessment and Certification & Accreditation	Latif Khalil L.Khalil@JBSInternational.com Tel: (240) 645-4124	✓	✓	✓
Defense Healthcare Information Assurance Program (DHIAP) for Military Health System / Washington DC	Security Training, Testing, and Risk Assessment for 200+ DoD Facilities Worldwide	Jeff Collmann, PhD collmanj@georgetown.edu Tel: (202)-870-2196	✓	✓	✓
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	Will be provided upon request	✓	✓	✓

§ 4.3.1.2: Vendor should list all references and/or examples for previous experiences in deploying and creating Cyber Security Risk Programs.

SRS offers the following project summaries as representative examples of our past performance. In order to preserve the confidentiality of customer points of contact for specific projects, contact information will be provided to WVOT upon request (e.g. if WVOT requests contact information be provided as clarifying information through the oral presentation process, SRS will make the contact information available to WVOT at that time).

- 1) Information Security Assessment Program – McKesson Corporation
- 2) Navy Medicine Information Systems Support Activity (NAVMISSA)
- 3) State of West Virginia Public Employees Insurance Agency (PEIA) / West Virginia Children's Health Insurance Program (CHIP) Security Risk Assessment
- 4) Alabama Regional Extension Center (AL-REC)
- 5) Multi-Dimensional Resiliency Model – National Reconnaissance Office (NRO)
- 6) Army National Guard Risk Management Framework for ESS

1) Information Security Assessment Program – McKesson Corporation	
Contracting Organization	McKesson Corporation
Description and relevance to solicitation requirements:	
<p>SRS provided Information Security Risk Management Framework and security risk assessment services to McKesson to conduct independent, third party Security and NIST compliance assessments against applications within McKesson Med Surgical, McKesson Health Solutions, McKesson specialty Health, and McKesson connected care analytics business units. SRS implemented a risk assessment program for McKesson Corporate to utilize with their business units in order to assess them for compliance with regulatory requirements, McKesson Corporate policies and procedures, and applicable NIST standards and special publications. Results and raw data were recorded using the McKesson Archer Governance, Risk Management, and Compliance (GRC) platform and SharePoint. As part of the assessments, SRS:</p> <ul style="list-style-type: none"> • Provided project management Services adhering to McKesson’s internal processes and was responsible for all project management activities of the project. • Created business process documentation and questionnaires for McKesson’s Application Risk Management processes based on Federal requirements and NIST Special Publications to frame, assess, respond, and monitor a variety of critical information assets utilizing the McKesson’s Archer GRC platform and other tools as specified by McKesson. • Performed Risk Assessments framed around the HIPAA Security Rule with applicable NIST Special Publications such as 800-66 Appendix D - Security Rule Standards and Implementation Specifications Crosswalk, 800-53 revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations as controls, and the test cases from 800-53A revision 4. <p>For each risk assessment, SRS developed and delivered an Executive Briefing Report which included an executive summary, risk matrix ranking each threat on a scale utilizing probability of the threat occurring and the impact of the treat if exploited, observations and recommendations on how each risk can be mitigated, a Plan of Actions and Milestones (POA&M) to help facilitate McKesson with the tracking and resolution of the mitigation plan.</p> <p>SRS also delivered a high-level findings presentation for each of the business units to explain and summarize the key elements of the assessment for each of their applications and to provide a forum to answer any questions. The briefing also includes recommendations for process improvement, including suggestions for preparing for any external audit.</p>	
Points of Contact: Ted LeSeur, +1 480-381-3522, ted@cyberriskhelp.biz	

2) Defense Health Agency (DHA)	
Contracting Organization	Department of Defense/Defense Health Agency (DHA)
Description and relevance to solicitation requirements:	
<p>SRS is tasked to provide Technical and Programmatic Services including IA Risk Management, IT Contingency Planning (ITCP), IA Compliance and IT support to Navy Medicine and the Defense Health Agency (DHA) Cyber Security Division. This support assists the CIOs and Information Assurance Managers at 27 Navy Medical Treatment Facilities and many more Branch Clinics world-wide, which collectively mass to approximately 55,000 users and 86,000 end nodes. The support helps DHA in identifying and mitigating IT issues, and addressing compliance considerations in substantive Information Technology domains such as IT Contingency Planning and Technical Risk Management.</p> <p>In addition SRS is tasked with providing technical, security, and policy related Subject Matter Expertise to DHA. This includes conducting reviews, analysis, and providing input to a variety of healthcare policy and technical specifications such as regulatory requirements, 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.</p> <p>As a part of this tasking, SRS is tasked with conducting Cyber Security Inspections (CSI) Stage II support for the US Cyber Command (USCYBERCOM) readiness team. SRS travels to sites selected for inspection by the Office of Compliance and Assessment (OCA) to assess the security of Navy networks through a comprehensive, graded inspection involving all Cyber Security areas, specifically: Leadership Management, Physical Security, Administration, Training, Network Configuration, Network Operations, and Human Factors and Command Operational Behavior.</p> <p>SRS has conducted policy, technical, and compliance reviews for IT security and privacy compliance within the existing policy framework, including providing recommendations on emerging DHA IT policy. SRS conducted system hardware and software design reviews – not only as part of the System Security Verification process, but in special cases where system changes may impact accreditation decisions. For example, SRS conducted a PKI Root-Trust Certificate Risk Assessment to determine the impact to Navy Medicine and DoD for installing VA root certificates in the NAVMED Active Directory. Resulting documentation included test plans, test reports, and security assessment reports.</p> <p>SRS produced a detailed and comprehensive IA Risk Management Framework (IA-RMF) implementation model from inception through to institutionalization and sustainment and has been asked to support the DoD/Intelligence Community Privacy Overlay Work Group and provide input to the DoD and NIST (on behalf of Navy Medicine) on matters concerning updates to DoD policy for the security and privacy.</p>	
Points of Contact: Available upon request – can be provided during oral presentations if requested.	

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

4) Alabama Regional Extension Center (AL-REC)	
Contracting Organization	University of South Alabama
Description and relevance to solicitation requirements	
<p>SRS was 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 regulatory requirements 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.</p> <p>Under this tasking, SRS is reviewed the Security policies and procedures used internally by ALREC and provided written comment and/or recommendations for updates. In particular, the policies and procedures were being reviewed to assess their completeness and suitability for addressing requirements of the HIPAA Security Rule and to serve as the foundation for a corporate information security risk management program. Deliverables included 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 provided subject matter expertise on Security and Privacy related matters, changes resulting from the HIPAA/HITECH Omnibus rule, and upcoming requirements still under development at ONC or CMS (such as Meaningful Use requirements). SRS developed training materials and implemented a train-the-trainer program to prepare the ALREC core team with the tools needed to train and prepare risk assessment teams throughout the state.</p>	
Points of Contact: Available upon request – can be provided during oral presentations if requested.	

5) Multi-Dimensional Resiliency Model – National Reconnaissance Office	
Contracting Organization	US Navy
Description and relevance to solicitation requirements	
<p>SRS developed the Multi-Dimensional Resiliency Model (MDRM) under tasking to the National Reconnaissance Office (NRO) and later adapted for use by the US Navy, to serve as the foundation for conducting information security risk management improvement activities within the enterprise. It leveraged methods described in NIST Special Publications, The Mission Assurance Analysis Protocol (MAAP) developed at the SEI/CERT (with acknowledged contribution by Johnathan Coleman, SRS), the CMMI, and ITIL processes. Additionally, the methodology leverages Business Impact Analysis techniques as an integrate part of the analysis process. Another example of our experience and expertise in this area is demonstrated through our selection as part of a closed committee to review the Certification and Accreditation processes employed at the Nuclear Regulatory Commission (NRC). As part of that review, SRS investigated the methods, costs, and results associated with the NRCs FISMA activities and provided testimony on results during a closed session of the Agencies Commissioners.</p>	
Points of Contact: Available upon request – can be provided during oral presentations if requested.	

6) Risk Management Framework for ARNG ESS	
Contracting Organization	US ARMY Engineering & Support Center
Description and relevance to solicitation requirements	
<p>SRS provided direct support to the Army National Guard (ARNG) Program Management Office (PMO) by developing, defining, and implementing a Cybersecurity Risk Management process for the ARNG Electronic Security Systems (ESS) Program. This included providing subject matter expertise on matters relating to information assurance, risk management, certification and accreditation, configuration management, test and evaluation, and security configuration and architecture of Electronic Security System (ESS) 3.0 and emerging ESS 4.0. SRS applied methodologies to manage risks associated the ESS risk management and Type Security Certification and Accreditation, and more recently Assessment and Authorization Processes.</p> <p>SRS conducted security engineering analysis and developed the ESS technical, hardware and software systems architecture in accordance with RMF, DoD, Army, NGB and industry regulations and best practices. This was achieved through development of execution of formal procurement, integration, test and evaluation, remediation, mitigation and authorization processes. SRS provided SME support and fulfilled the role of ISSO reporting directly to the ESS IAM, CCB, PMO and DAA. This required development of technical documents to describe the ESS systems security architecture and technical description of the IDS environment, and options for integrating Environmental Sensors, Access Control Systems and video surveillance systems into the ESS architecture. SRS conducted third party security testing of vendor ESS components, and worked with vendors to mitigate vulnerabilities identified in the component software and firmware. SRS has worked closely with SPAWAR Atlantic SME's, vendor technical teams and the ARNG ESS PMO to ensure IA and security engineering principles are incorporated into ESS v2.0 design, integration and implementation processes.</p> <p>SRS has been an integral part of the execution of IA, C&A and RMF requirements in support of the ARNG ESS 1.0 and 2.0 programs since 2008. SRS developed the original DIACAP packages for ESS1.0 and 2.0, and has worked with the ARNG to map all the security controls to the NIST SSP RMF approach in anticipation of the transition to continuous monitoring under RMF. SRS has developed ESS v3.0 System Security Plan and Security Assessment Report as well as revisions of supporting artifacts in an effort to align with RMF guidance. SRS has worked closely with the ESS PMO and the DAA in preparation for the transition from DIACAP to RMF to minimize impacts to system authorization and deployment.</p> <p>SRS developed and implemented the ARNG ESS vulnerability management plan, which contains procedures necessary to identify, mitigate, and report security status for ESS assets. The plan demonstrates the ESS procedures for addressing vulnerability notice issuance and response, mitigation plan development, approval and execution, technical testing and implementation, and formal reporting. This affects all ESS locations and interfaces, including IDS Monitoring Stations, ARNG JTF Locations, and gaining systems such as ARNG Guardnet. SRS provided technical support for compliance analysis, and tracking for the integrated ESS baseline. SRS created, updated, and maintained the POA&M, as well as other pertinent RMF documentation such as the System Security Plan (SSP), Raw Test Results, Risk Assessment Report, Mitigation Plan, IT Contingency Plan, Privacy Impact Assessment, and all supporting artifacts as required to be loaded into eMASS.</p> <p>Additionally, SRS instituted robust CM procedures, which proactively identified, responded to and mitigated vulnerabilities and potential security concerns affecting the ESS v2.0 system. Vulnerability and security concerns, along with corrective actions, were detailed in formal reports and submitted to regional ISSO's/IAM's through the ESS PMO. SRS provided guidance to the ARNG ESS CCB on a number of Cyber Security and RMF related issues. For example, SRS worked with the ARNG G6 to help the ILI PMO draft the Interconnection Security Agreement for each of the ARNG State's to sign and comply with, to maintain the correct baseline security posture of the ESS system.</p>	
<p>Points of Contact: Available upon request – can be provided during oral presentations if requested.</p>	

§ 4.3.1.3: Vendor should provide resumes for staff that will be responsible for overseeing and completing the work on this contract.

Detailed resumes are included in Appendix D to this proposal. Professional Certifications are included at Appendix C. The following summary introduces key personnel proposed on this project:

Overall Lead/Program Manager: Mr. Coleman (SRS), is proposed as the Program Manager and will coordinate and administer all SRS contractor tasking; will have final oversight of SRS resource availability; guide and monitor technical and cost performance on tasks; and coordinate with WVOT.

Mr. Coleman is an experienced, credible subject matter expert in the field of Cyber Security Risk Management. In 2018, Mr. Coleman participated as part of a small group session at the White House (Roosevelt Room/West Wing) for meetings on Security and Privacy Interoperability with Senior Advisors to the President, the CMS Administrator, and the National Coordinator for Health IT. He has provided testimony to Federal Advisory Committees, supported the Federal Health Architecture (FHA) Security Strategy Committee, and has participated as an invited speaker at a seminar hosted by NIST/CMS on HIPAA Security Rule Implementation and Assurance. He is a co-chair for the HL7 International WG which addresses privacy and collaborative care standards, and has led and co-developed several standards which have gained normative, ANSI accreditation, including: Cross Enterprise Security and Privacy (XSPA) healthcare profiles (through OASIS) and HL7 Version 3 Implementation Guide: Data Segmentation for Privacy (DS4P). He has led numerous security framework implementations and IT Security Assessments for large complex organizations, including: The National Guard Bureau, the National Reconnaissance Office, McKesson Corporation, and the West Virginia Public Employees Insurance Agency's (PEIA).

Project Manager: Amber Patel, LLM (SRS), is the proposed Project Manager. She will facilitate the weekly meetings, coordinate development of deliverables, ensure Quality Assurance and Risk Management activities are conducted, and facilitate efficient execution of the project. She has considerable experience managing and facilitating large, complex IT projects for Government Agencies, including the US Department of Health and Human Services. In this capacity she has led the program management and piloting of IT projects at several large facilities, including Yale and Indiana University. Ms. Patel has also been working closely with ONC leadership collecting and compiling input from various federal agencies, industry, and other related stakeholders on the draft Trusted Exchange Framework and Common Agreement (TEFCA). Ms. Patel and her SRS colleagues analyzed and arranged by theme each comment received and presented critical issues and potential solutions to ONC leadership, specifically in relation to privacy and security. Ms. Patel also provides legal subject matter expertise and has worked on several projects conducting compliance gap and risk analyses to determine compliance with Federal, state, and local laws, policies, standards, and specifications related to privacy, breach notification, consent, and security. Ms. Patel also reviews and analyzes existing policies and procedures and contracts to identify deficiencies, providing tactical compliance approaches, and developing strategic recommendations for clients. Ms. Patel has a BA, Psychology and Linguistics from the University of Texas, a PgDL/CPE (Law) from the University of Westminster (London, England), and LLM (Masters in Law) from the University of Texas School of Law.

Framework / Policy Lead: Ronald Krutz, PhD, CISSP-ISSEP, is proposed as the Framework / Policy Lead for this project. As the Chief Scientist for SRS, Dr. Krutz provides analysis, interpretation, and validation of mappings between discreet security controls and corresponding policies, regulatory requirements, and information security frameworks such as the NIST Cyber Security Framework. 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

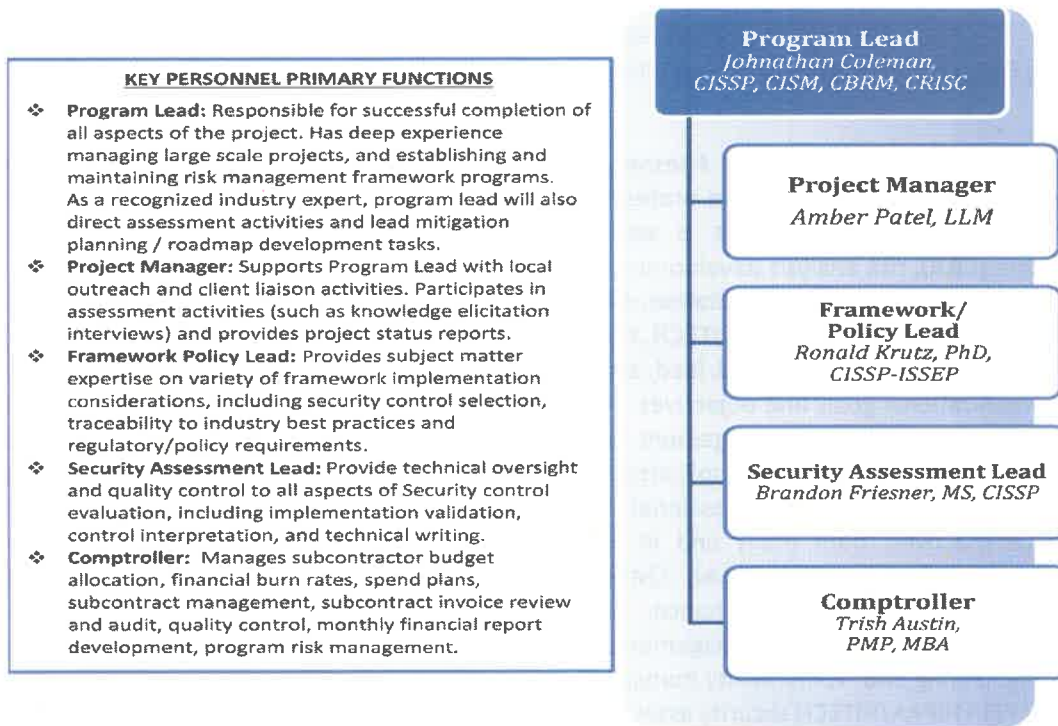
computing systems, computer architectures, information assurance methodologies, industrial automation and control systems, and information security training. He has been a Senior Information Security Consultant at Lockheed Martin, BAE Systems, and REALTECH Systems Corporation, an Associate Director of 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.

Security Assessment Lead: Brandon Friesner, MS, CISSP. Mr. Friesner is a technically proficient and decisive senior information assurance professional offering over 15 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, Assessment and Authorization (A&A), CMMI, configuration management, enterprise architecture, incident response, IT policy/governance, OCTAVE®, process improvement, project management, requirements management, risk management, security test and evaluation, strategic planning, systems security engineering and vulnerability management. Mr. Friesner served as the lead technical assessor for the WV PEIA HIPAA/HITECH security assessment, and serves as the lead assessor for the Army National Guard Bureau's Electronic Security Systems Risk Management Framework project. Mr. Friesner provided information security services to the Charleston International Airport. **In this capacity he authored the Information Security Framework, which provides an overview and comparative analysis of three frameworks tailored to meet the needs of the Airport Authority.** He demonstrated the recommended Information Security Framework, and provided training on activities required to implement it. 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 Airport Authority security posture in the form of an Information Security Framework matrix to support the mitigation process. He also 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.

§ 4.3.1.4: Vendors should provide staff with the appropriate background, education, and experience to address all components and phases of the project.

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 for the cyber risk program development, acquisition assistance, and overall cyber risk program adherence for the state of WV. As shown in Figure 2, below, our staffing plan consists of an experienced and proven Expert Program Lead, a project manager, several Subject Matter Experts (including & policy experts, and technical security experts), and the necessary program support staff.

Figure 2: Staffing Plan



The labor matrix in Table 2 demonstrates the qualifications and certifications held by key personnel proposed and available to support this project. Other SRS personnel are also available to support the project as needed.

Table 2: Staff Qualification Matrix

Name	Proposed Role	Certification(s)	Degrees
Johnathan Coleman	Program Manager	CISSP, CISM, CBRM, CRISC	BEng, Aeromechanical Systems Engineering
Ronald Krutz	Framework/Policy Lead	CISSP, ISSEP	PhD, Electrical and Computer Engineering
Brandon Friesner	Security Assessment Lead	CISSP, Security+, CCNA, DAWIA IT Level 1	MS, Systems Engineering
Amber Patel	Project Manager	Security+	BA, PgDL/CPE (Law), LLM
Trish Austin	Financial Comptroller*	PMP	MBA, Finance

§ 4.3.2 - Mandatory Qualification/Experience Requirements

The following paragraphs describe how SRS personnel meet and exceed the mandatory qualification and experience requirements.

§ 4.3.2.1: Vendor must have fully implemented a Cyber Risk management program within an organization of similar size and complexity or larger.

SRS is compliant with the mandatory requirement of implementing a Cyber Risk Management Program given the performance history as specified in Section 4.3. Notably, For the McKesson Corporation, SRS led the development of an enterprise-wide security assessment framework, which McKesson Business Units were tasked with implementing. With help from SRS, McKesson was able to develop the cybersecurity program, document the program, pilot it at various McKesson Business Units, institutionalize it within the company as a service-center/chargeback capability with McKesson Corporate, and manage risks through the implementation of an enterprise-wide GRC tool. SRS piloted the program by conducting cybersecurity risk assessments at various McKesson business units and tailoring the approach and enterprise strategy as a result of lessons learned.

SRS has successfully implemented a comprehensive Cyber Risk Management program for the Army National Guard (ARNG) Bureau, which resulted in the Senior Authorizing Official for the ARNG providing an unprecedented accreditation for the Program and information Systems in the Program to be given a "type" authorization, approved for implementation in all 50 US States.

As another example, SRS developed a Cyber Risk Management program for the Defense Health Agency, which resulted in the adoption of a Risk Management program that includes Risk Posture Assessments and DoD facilities in the US and overseas. The results of this program are fed into a compliance reporting dashboard, also conceived and designed by SRS, for reporting trends and issues associated with how specific security controls are implemented throughout the enterprise.

Exceeds Requirement: In particular, it should be noted that SRS implemented a comprehensive HIPAA/HITECH Security Assessment for the WV PEIA and as such has institutional knowledge and experience with the Policies and Procedures implemented in the State of WV, as well as the WVOT and Office of Administration.

Appendix A: Addendum Acknowledgement Form

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: ISC200000000

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)

<input checked="" type="checkbox"/> Addendum No. 1	<input type="checkbox"/> Addendum No. 6
<input checked="" type="checkbox"/> Addendum No. 2	<input type="checkbox"/> Addendum No. 7
<input type="checkbox"/> Addendum No. 3	<input type="checkbox"/> Addendum No. 8
<input type="checkbox"/> Addendum No. 4	<input type="checkbox"/> Addendum No. 9
<input type="checkbox"/> Addendum No. 5	<input type="checkbox"/> 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

26 August 2019

Date

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

Appendix B: State of West Virginia Purchasing Affidavit

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

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

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

DEFINITIONS:

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

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

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

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (W. Va. Code §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: Security Risk Solutions, Inc.

Authorized Signature: [Handwritten Signature] Date: 8/26/2019

State of SOUTH CAROLINA

County of Berkeley, to-wit:

Taken, subscribed, and sworn to before me this 26 day of AUGUST, 2019

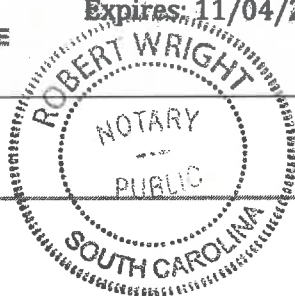
My Commission expires My Commission, 20

Expires: 11/04/2026

AFFIX SEAL HERE

NOTARY PUBLIC

[Handwritten Signature]



Purchasing Affidavit (Revised 01/10/2013)

Appendix C: Professional Certifications





IEEE
Leading Technology
for Humanity

The world's largest technical professional organization for the advancement of technology

Home > My Account > Membership and Subscription Information

Settings
Manage Your Profile
Personal Profile
Email Address and

Membership and Subscription
Current membership profile
Member information ⓘ
Member number: [REDACTED]
Grade: Life Senior

Krutz:
Senior Life Member IEEE



CompTIA

Amber Patel

has successfully completed the requirements to be recognized as

Security+
CERTIFIED - CE

COMPTIAC21002482
Expires on July 06, 2015
Signature: [REDACTED]



Commonwealth of Pennsylvania
Department of State
Bureau of Professional and Occupational Affairs
PO BOX 2649 Harrisburg PA 17105-2649

19 0799219

License Type: Professional Engineer
License Status: Active
Initial License Date: 03/22/1988

RONALD L. KRUTZ
2008 PLYMOUTH COURT
GIBSONIA, PA 15044

Expiration Date: 09/30/2021

License Number: [REDACTED]

Avigil, Commissioner of Professional and Occupational Affairs



CERTIFICATE OF APPOINTMENT

03 April 2012

Johnathan Coleman

MEETS THE REQUIREMENTS AND HAS BEEN APPOINTED AS A

Fully Qualified Navy Validator

Paul K. Hilton
Paul K. Hilton
Navy Certification Authority

CERTIFICATE NUMBER: [REDACTED]



Certificate of Completion

Awarded to
Johnathan Coleman

For the successful completion of
DIACAP Advanced Validator Course

Cert No. [REDACTED]
Date of Completion: 02 March 2012
Instructor Signature: [REDACTED]



Project Management Institute

1975 to the present day

Trish Austin

HAS BEEN FORMALLY EVALUATED FOR DEMONSTRATED EXPERIENCE, KNOWLEDGE AND PERFORMANCE IN ACHIEVING AN ORGANIZATIONAL OBJECT BY THROUGHLY DEFINING AND MANAGING PROJECTS AND RESOURCES AND SUCCESSFULLY ESTABLISHED THE GLOBAL CRITERIA.

Project Management Professional

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

Paul M. Hannon
Paul M. Hannon
President

William C. Rife
William C. Rife
President

1975 to the present day
1975 to the present day
1975 to the present day

Appendix D: Key Resumes

Johnathan Coleman, BEng. CISSP, CISM, CBRM, CRISC



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

2005 - Present: Mr. Coleman is the Principal Consultant at Security Risk Solutions, Inc., a small, woman owned vendor neutral consulting business specializing in Information Security Risk Management.

Relevant Experience in Program and Project Management, and Ability to provide technical expertise related to health IT initiatives such as pilots, use cases, balloting:

Mr. Coleman has served as Health IT Program Manager for the CDC Opioid Prescribing Guideline CDS project (CDS for CDC Guideline). He also served as the Initiative Coordinator for several standards and interoperability initiatives at the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology (ONC), including: Data Segmentation for Privacy (DS4P), Prescription Drug Monitoring/Health IT Integration (PDMP/HITI), Data Provenance, Data Access Framework (DAF), Patient Choice Technical Project (PATCH), and served as the overall coordinator for the ONC Standards and Interoperability (S&I) Framework, which provided **guidance and coordination for all S&I projects, including CDC Opioid Guideline**. Mr. Coleman is currently supporting ONC with analysis, development of Policy Recommendations, and development of Implementation Guides for the Trusted Exchange Framework and Common Agreement (TEFCA). He is a co-chair at HL7 for the Community Based Care and Privacy Work Group, and member of the US Realm Steering Committee, Previous work with ONC includes leading the Sync-for-Science Security and Privacy Assessment project, which required engagement and technical testing of various EHR systems and implementations. Mr. Coleman led an independent privacy and security technical and administrative testing, analysis, and assessment of a voluntary subset of S4S pilot organizations' implementations of the S4S API. This project ultimately produced the ONC publication "Key Privacy and Security Considerations for Healthcare Application Programming Interfaces (APIs)", and resulted in technical updates to HL7's Fast Healthcare Interoperability Resources (FHIR) Security Specification.

Mr. Coleman has supported ONC since 2005, where he supported the Health Information Technology Standards Panel (HITSP) as WG facilitator and co-chair of the HITSP Security, Privacy and Infrastructure ARRA tiger team which was chartered by HHS to develop Interoperability Specifications to meet the requirements of the AHIC Use Cases and new provisions under HITECH.

Mr. Coleman has been directly responsible for the convening and coordinating of ONC projects for the last fourteen years. This experience directly includes facilitating and leading consensus stakeholder groups within standards organizations, and public/private joint projects (such as S&I initiatives). All of these projects required strong leadership and communication skills, as well as proficiency in working through various IT platforms (e.g., Confluence, JIRA, SharePoint, Microsoft, GoToMeeting, WebEx, etc.).

In 2018, Mr. Coleman participated as part of a small group session at the White House (Roosevelt Room/West Wing) for meetings on Healthcare Interoperability with Senior Advisors to the President, CMS Administrator, and the National Coordinator for Health IT. He has provided testimony to Federal Advisory Committees including NCVHS (the advisory committee to HHS), the Health IT Policy Committee (HITPC), and the Health IT Standards Committee (HITSC). He has also briefed the National Governors Association (NGA) State Alliance for eHealth, the Federal Health Architecture (FHA) Security Strategy Committee, and has participated as an invited speaker at a seminar hosted by NIST/CMS on HIPAA

Security Rule Implementation and Assurance. He is a co-chair for the HL7 International WG which addresses privacy and collaborative care standards, and has led and co-developed several standards which have gained normative, ANSI accreditation, including: Cross Enterprise Security and Privacy (XSPA) healthcare profiles (through OASIS) and HL7 Version 3 Implementation Guide: Data Segmentation for Privacy (DS4P).

In addition to his work at HHS, Mr. Coleman assists organizations with the development and implementation of information security programs including information security needs analysis, regulatory compliance, organizational resiliency planning, institutionalization of Risk Assessment and Business Impact Analysis methodologies, and facilitation of HIPAA/HITECH compliance reviews. Other experience includes providing SME support for a joint Food and Drug Administration (FDA) and National Institutes of Health (NIH) sponsored Adverse Event Reporting project, and in conjunction with Georgetown University Medical Center, supporting the Intelligence Community on a Biosurveillance and early warning system which operates as a primer for U.S. countermeasure response plans in the context of a potentially catastrophic bioevent.

For the DoD, he worked closely with the Intelligence and Information Warfare Department of the Space and Naval Warfare (SPAWAR) Systems Center to conduct research and requirements traceability analysis for the National Reconnaissance Office (NRO) through development of a mission focused risk assessment methodology and associated automated tool entitled "Multi-Dimensional Resiliency Model" (MDRM), and supports the Technical Information Assurance Risk Management for 29 medical treatment facilities in the Navy Medicine enterprise.

1989 – 2005: Mr. Coleman held various positions as an active duty communications officer in the British Army. Experience includes the redesign and operational management of the Multi-National Division Communications Headquarters as part of the US led IFOR operations in Bosnia-Herzegovina, multinational amphibious force tasking in Sardinia, United Nations attachment at the Greek-Turkish border in Cyprus, and training for special duties in Northern Ireland. Private sector experience includes consulting for commercial Health IT organizations on security and privacy programs, and conducting HIPAA security assessments for organizations including Memorial Sloan Kettering Cancer Center, McKesson Corporation, Princeton Healthcare System, and Cancer Treatment Centers of America. He has provided Program Management and oversight for various DoD projects, including the Defense Health Agency (DHA) Cybersecurity Division Policy Support efforts, part of a \$35M DHA HIT program.

Certifications and Public Service:

Mr. Coleman is a Co-chair for the Health Level 7 International (HL7) Community-Based Care and Privacy (CBCP) Work Group, a Navy Certification Authority (CA) Fully Qualified Navy Validator (FQNV), a Certified Information Systems Security Professional (CISSP), accredited by the International Information Systems Security Certification Consortium and is a Certified Information Security Manager (CISM) and Certified in Risk and Information Systems Control (CRISC) as accredited by the Information Systems Audit and Control Association (ISACA). He served for 7 years as a Visiting Scientist at the Software Engineering Institute/CERT® Coordination Center (SEI/CERT) at Carnegie Mellon University, and participated in research, training and delivery of the Operationally Critical, Threat, Asset and Vulnerability Evaluation (OCTAVE®) and Mission Assurance Analysis Protocol (MAAP).

Education:

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 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 military academy graduating class.

Education

Royal Military College of Science (Shrivenham, England): BEng, Aeromechanical Systems	1992
6 th Military Intelligence Detachment (England): Information Security	1994
Royal School of Signals (Blandford, England): Cryptology and INFOSEC	1996

Clearance: Active Top Secret DoD Clearance.

Published work: <http://www.securityrisksolutions.com/publications.html>

- **Demystifying TECCA: HIMSS 2018 Conference and Exhibition, Orlando, FL**
- **Protecting High Stakes PHI;** Journal of AHIMA, April 2014, ©2014
- **Meaningful Use Risk Assessments: Requirements, Methodology, Challenges and Lessons,** Joint presentation / education session with the Chief Privacy Officer, Office of the National Coordinator for Health IT, Department of Health and Human Services. *J.Pritts, JD & J.Coleman: HIMSS 2014*
- **Extra-Sensitive PHI: Appropriate Sharing using Data Segmentation for Privacy,** HIMSS 2013 Conference and Exhibition, Ernest N. Morial Convention Center, New Orleans, LA.
- **Segmenting Data Privacy;** Journal of AHIMA, February 2013 ©2013 American Health Information Management Association
- **Privacy Protection for Substance Abuse Treatment Information,** Presentation on behalf of the Data Segmentation for Privacy Initiative, Office of the Chief Privacy Officer, Office of the National Coordinator for Health IT, Department of Health and Human Services, *HIMSS 2012, February 23, 2012, Sands Convention Center, Las Vegas, NV.*
- **Privacy Consent and Access Control: Cross Enterprise Security and Privacy Authorization (XSPA),** Presentation and Advanced Technology Demonstration on behalf of the Organization for the Advancement of Structured Information Standards (OASIS), *HIMSS 2009, April 4-8 2009, McCormick Place, Chicago IL.*
- **Presentation to Federal Health Architecture (FHA) Security Strategy Committee:** Briefing on relationship between FISMA, HIPAA, NHIN, CCHIT, and HITSP. *November 7, 2008; Department of Health and Human Services, Washington DC.*
- **NIST/CMS Workshop: HIPAA Security Rule Implementation and Assurance;** Presentation on HITSP Security and Privacy Standards *January 16, 2008; NIST Main Campus, 100 Bureau Dr, Gaithersburg, MD*
- Acknowledged Contributor: **Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process**, *Richard A. Caralli et al; May 2007, Technical Note CMU/SEI-2007-TR-012 ESC-TR-2007-012; © Copyright 2007 Carnegie Mellon University*
- **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
- 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
- **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

Amber Patel, LL.M., Security +

2014 – Present: Ms. Patel is a Senior Health Systems Policy Analyst at Security Risk Solutions, Inc. (SRS), a small, woman owned vendor-neutral consulting business specializing in Information Security Risk Management.

Relevant Experience in Program and Project Management, and Convening and coordinating federal agencies, industry, and other stakeholders:

Ms. Patel has served as the Project Manager for the CDS for CDC Opioid Guideline project. She has provided program and project management support on several initiatives led by the Office of the National Coordinator for Health Information Technology (ONC), including the electronic Long Term Services and Supports (eLTSS), all phases of The Patient Choice Technical Project (PATCH), Data Provenance, Prescription Drug Monitoring Program and Health Information Technology, and Data Segmentation for Clinical Decision Support. Recently, she was the lead interviewer and writer for the ONC's Patient Choice landscape assessment which assessed current practices in research consent technology and management, identified gaps in exchange of research consent, and provided ONC with recommendations to improve the research consent process and facilitate the exchange of research consent. In this task, she conducted more than twenty-five hour-long discussions with industry leaders to identify where exchange of research consent would provide a benefit to the community. Using the information gathered during this report, Ms. Patel drafted and presented Phase 2 use case scenarios to a large community of interested stakeholders, further refining the use cases to reflect the needs of the community. Ms. Patel also provides subject matter expertise on legal and policy related issues for PATCH as a result of her ten years in the health and legal industries. Ms. Patel was also author on ONC's Clinical Decision Support for Data Segmentation landscape assessment completed in 2015.

Ms. Patel has also been working closely with ONC leadership collecting and compiling input from various federal agencies, industry, and other related stakeholders on the draft Trusted Exchange Framework and Common Agreement (TEFCA). Ms. Patel and her SRS colleagues analyzed and arranged by theme each comment received and presented critical issues and potential solutions to ONC leadership, specifically in relation to privacy and security.

Ms. Patel also provides legal subject matter expertise and has worked on several projects conducting compliance gap and risk analyses to determine compliance with Federal, state, and local laws, policies, standards, and specifications related to privacy, breach notification, consent, and security. Ms. Patel also reviews and analyzes existing policies and procedures and contracts to identify deficiencies, providing tactical compliance approaches, and developing strategic recommendations for clients.

Ms. Patel provided the Alabama Regional Extension Center (ALREC) staff with accessible and easy-to-follow HIPAA compliant risk assessment training. The goal of this training was to enable staff understanding of the requirements and reasons behind HIPAA regulations so that they could, in turn, provide useful assistance to their member organizations looking to understand the intent of HIPAA regulations generally. Beyond covering the Privacy Rule regulations, Breach Notification regulations, and Security Rule regulations, she also trained staff on a risk assessment tool geared towards small- to medium-sized practices. The risk assessment training was based on Centers for Medicare & Medicaid Services (CMS) guidance and Office of the National Coordinator for Health Information Technology (ONC) best practices that would help ALREC members with achieving Stages 1 and 2 of Meaningful Use.

2008 – 2012: Ms. Patel served in various positions, ultimately as Director of Policy and Compliance for the Primary Care Information Project (PCIP) and NYC-designated Regional Extension Center (NYC REACH) at the New York City

Department of Health and Mental Hygiene. She was a member of the leadership team that operated and managed the Federal government-funded Meaningful Use program for NYC, which was designed to promote health IT and assist with the adoption of Electronic Health Records (EHR) among NYC-based physicians. Ms. Patel oversaw the legal work for the bureau, from analyzing Federal and state laws affecting health IT, including the exchange of health data, to negotiating, drafting, managing a variety of contracts, and designing the contractual structure between NYC REACH and its partners. The latter included drafting contracts between NYC REACH and EHR vendors ensuring certain reportable data elements were collected from member organizations; membership agreements with NYC-based physicians and hospitals authorizing the collection of those data elements; and Business Associate Agreements (BAAs) establishing a tri-party data stream between PCIP, NYC REACH (which collected certain data elements), and member organizations. Furthermore, Ms. Patel revised EHR vendors' BAAs on behalf of member organizations to ensure newer requirements contained in the Health Information Technology for Economic and Clinical Health Act 2009 (HITECH) were appropriately reflected, and educated EHR vendors on these new requirements where necessary.

Ms. Patel also managed the internal and external operations for the health IT privacy and security program. She developed and disseminated community health materials for the NYC physician and hospital community to help this audience navigate the complex legal requirements of HIPAA and HITECH. These materials – the Privacy & Security Toolkit – included best IT practices for safeguarding data, template policies and procedures required under Federal law, and guidance notes on other applicable health laws. Ms. Patel also visited over forty member organizations that utilized EHRs to ensure these organizations met the non-technical components of HIPAA risk assessments, implementing best practices when necessary. Additionally, Ms. Patel developed a training program and educated NYC physicians and their staff on HIPAA privacy and security laws and HITECH breach notification laws, all of which are reinforced under the Meaningful Use program. Her training program was delivered to over 2,500 health care professionals in NYC.

In her role, Ms. Patel worked closely with officials at city, state, and Federal agencies, including the Office of the National Coordinator for Health Information Technology (ONC) in order to identify policy needs and coordinate strategies and proposals around barriers to electronic exchange of information. One representative emphasis within this collaboration included identifying how to electronically parse out services to which a minor has consented without parental knowledge so that these services could remain private after electronically exchanging the minor's medical record. The result of this work led to the co-authored whitepaper, "Barriers to the Exchange of Pediatric Health Information" published by the New York eHealth Collaborative in 2010. She also partnered with other Federal grant awardees to form a national taskforce on emerging health IT issues, including directing a national strategy on best practices to secure electronic patient data and identifying overlaps in EHR vendor and clinician liability for electronic breaches of patient information. She was the designated policy liaison teaming with state regional health information organizations to analyze and update existing state policies and procedures for exchanging information within such organizations. Furthermore, Ms. Patel consulted with colleagues on distinct public health initiatives, providing legal oversight on contracting with outside parties, including an initiative to provide free blood pressure monitoring at houses of worship and organizing pharmacist-managed care. Ms. Patel also participated in annual conferences with EHR vendors and provided information on privacy and security best practices to attendees.

Ms. Patel served on the Board of Directors and as Compliance Director for the non-profit organization, Council for American Students in International Negotiations (CASIN) from 2008-2010. She managed the compliance team, completing and updating all outstanding filings with New York State. She also co-developed the 2009/2010 strategy for leading student delegations to meetings on international policy, and led delegations to the Commissions on Population and Development and Sustainable Development at the United Nations in 2009. She secured special consultative status with the United Nations Economic and Social Council on behalf of the

organization, which remains in effect today. Additionally, she reviewed articles, specifically regarding global public health, for CASIN's journal, Eyes on the ICC (International Criminal Court).

2007 – 2008: Returning to The University of Texas, Ms. Patel obtained her LL.M. focusing on constitutional law and public policy. During this year, Ms. Patel was awarded a public interest internship at the Mississippi Center for Justice, where students assisted those affected by Hurricane Katrina with FEMA applications. Her LL.M. thesis titled "Undermining the National Security and Civil Liberties Debate: The Recurrence of Politically-Motivated Actions" was published in 2010 by the University of Tennessee Baker Center Journal of Applied Public Policy.

2005 – 2007: Ms. Patel honed her legal skills while working at Epstein Becker & Green, P.C., a pre-eminent Health Care and Life Sciences law firm in New York City. She drafted BAAs, employment contracts, shareholder and board resolutions, and client memos explaining recent changes in health care laws for a variety of clients, from large organizations, including hospitals and pharmaceutical companies, to small biotechnology start-ups and non-profit clinics. During her time here, she co-authored a chapter detailing the Indiana licensure procedure for health care facilities, which was published by the American Health Lawyers Association in 2007.

2002 – 2004: Ms. Patel obtained her Postgraduate Diploma in Law and Legal Practice Course certification abroad in the United Kingdom at the University of Westminster.

2001 – 2002: Ms. Patel worked as a Marketing Assistant at Ameritas Direct, and life insurance company in Houston, Texas. Her article titled "A New Kind of Insurance: No-Load Universal Life" was published in Vision Magazine in Summer 2002.

Education

The University of Texas (Austin, Texas): BA, Psychology and Linguistics	2001
University of Westminster (London, England): PgDL/CPE (Law)	2004
The University of Texas School of Law (Austin, Texas): LL.M.	2008

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			
<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>			
EXPERIENCE SUMMARY			
<p>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 authored white papers on a variety of information assurance-related topics.</p>			
<p>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.</p>			
<p>Lockheed Martin/The Sytex Group, Advanced Technology Research Center Senior Infosec Consultant (2003-2007)</p>			

Ronald L. Krutz, Ph.D., P.E., CISSP, ISSEP	Chief Scientist, Security Risk Solutions
<p>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.</p>	
<p>BAE Enterprise Systems/Corbett Technologies Senior Technical Staff (2000-2003)</p> <p>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.</p>	
<p>Carnegie Mellon University Faculty and Associate Director, Carnegie Mellon Research Institute (1975-2000)</p> <p>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 in 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.</p>	
<p>Certifications, and Affiliations</p>	
<p>Certifications</p> <ul style="list-style-type: none"> • Registered Professional Engineer in Pennsylvania • CISSP • ISSEP • Life Senior Member, IEEE <p>Publications</p> <p>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:</p> <ul style="list-style-type: none"> • <i>The CISSP Prep Guide</i> • <i>The CISSP Prep Guide, Advanced Q&A</i> • <i>The CISSP Prep Guide, Gold Edition</i> • <i>The Security+ Prep Guide</i> • <i>The CISM Prep Guide</i> • <i>The CISSP Prep Guide, 2nd Edition: Mastering CISSP and ISSEP</i> • <i>The Network Security Bible 8. The CISSP and CAP Prep Guide, Platinum Edition: Mastering CISSP and CAP</i> • <i>Securing SCADA Systems</i> • <i>Certified Ethical Hacking (CEH) Prep Guide</i> • <i>Network Security Fundamentals</i> • <i>Project Manual--Network Security Fundamentals</i> • <i>The CSSLP Prep Guide.</i> • <i>Cloud Computing Security</i> • <i>Web Commerce Security.</i> <p>He also authored two university texts on microprocessors and logic design and digital interfacing techniques for John Wiley & Sons, and recently authored <i>Industrial Automation and Control System Security Principles</i> for the International Society of Automation (ISA) (2013.)</p>	

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 Oklahoma City University	BS (Bachelor of Science) MBA (Master of Business Administration)	1993 2000	Accounting Business Administration with a Concentration in Finance
Qualifications Summary			
<p>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.</p>			
Experience Summary			
Security Risk Solutions, Inc.		Comptroller (Feb 2012 – present)	
<p>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.</p>			
South Carolina Research Authority (SCRA)		Project Manager and Financial Analyst (2001-2012)	
<p>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.</p>			
Logix Communications		Business Analysis Manager and Financial Analyst (1998 – 2001)	
<p>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.</p>			
MCI-Worldcom Telecommunications		Revenue Reporting Analyst (1995 – 1998)	
<p>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.</p>			
Certifications and Affiliations			
<ul style="list-style-type: none"> • Certified Project Management Professional (PMP) • Current member of the Project Management Institute, Charleston SC Chapter 			

Brandon Friesner, MS, CISSP
 Senior Cybersecurity Analyst/Subject Matter Expert
 Facility Security Officer
 Security Risk Solutions, Inc.

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

CERTIFICATIONS
 Certified Information Systems Security Professional (CISSP)

CLEARANCE
 DoD Top Secret

QUALIFICATIONS SUMMARY

Mr. Friesner is a technically proficient and decisive senior information assurance professional offering over 19 years of experience in Information Technology, Information Assurance, Cybersecurity, Information Systems Security Engineering and Risk Management. He is well-versed in network security testing, Assess and Authorization (A&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 Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA)/ Health Information Technology for Economic and Clinical Health (HITECH), Office of Management and Budget (OMB) Circular A-130, National Institute of Standards and Technology (NIST) SP-800 Series, Federal Information Processing Standards (FIPS), and Department of Defense (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, Assess and Authorization (A&A), Capability Maturity Model Integration (CMMI), configuration management, Risk Management Framework (RMF), enterprise architecture, incident response, information assurance, cybersecurity, HIPAA/HITECH, Information Technology (IT) contingency planning, IT policy/governance, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®), process improvement, project management, requirements management, risk management, security test and evaluation, strategic planning, systems security engineering, Transmission Control Protocol/Internet Protocol (TCP/IP), technical leadership, telecommunications and network security, vulnerability management.

EXPERIENCE SUMMARY

Security Risk Solutions, Inc. (SRS) – Mount Pleasant, SC **Mar 2012 – Present**

Senior Cybersecurity Analyst/Subject Matter Expert

- Army National Guard (ARNG), Electronic Security Systems (ESS) Program, Information Systems Security Officer (ISSO)
- Served as Information Systems Security Officer (ISSO), responsible for the management and execution of Cybersecurity, Risk Management Framework (RMF), Assessment and Authorization (A&A) and Continuous Monitoring activities for the Army National Guard (ARMG) Electronic Security Systems (ESS).
 - Developed and directed the institutionalization of processes and procedures for sustainment of the ESS RMF type-authorization.
 - Responsible for the achievement of ESS 2.0 accreditation, and recently obtained the first ARNG Type authorization under RMF
 - Coordinated development of the technical testing environment, encompassing numerous vendors’ products into a single “system of systems”. Components included CISCO 5500 series Security Appliances, Windows Server 2016, Microsoft SQL Server 2016, Microsoft Public Key Infrastructure (PKI), Windows 10, VMWare vSphere/vCenter/ESXi, and ACAS/NESSUS.
 - Performed security testing on the components and worked with the various vendors to mitigate and harden their components to meet DoD and Army requirements for Information Security.

Defense Health Agency (DHA), DAD IO (J-6), Cyber Security Division, Policy Branch Team Member/Subject Matter Expert

- Works on DHA's inter-agency efforts to align technical security and privacy standards for interoperability between the DoD, VA, SSA, CMS, ONC, and other Agencies within the Federal Health Architecture (FHA).
- Evaluated and provided analysis of Federal, DoD, Industry and other standards, policies, best practices and issuances to identify potential cybersecurity impacts and facilitate necessary response through the revision of existing or develop of new DHA policy.

Navy Medicine (NAVMED), Enterprise Cybersecurity (ECS) Program, Continuity of Operations (COOP), Team Lead

- Contributed to the improvement in quality and effectiveness of enclaves and Programs of Record (PORs) across the Enterprise in performing their COOP related activities in accordance with Federal and departmental policies and guidelines (e.g., FISMA, DoDI 8500.2, NIST SP800-30, NIST SP800-34).
- Ensured a common approach across the enterprise to identify critical and secondary systems, and the priorities for their resumption and/or recovery against Mission Essential Function (MEF) criteria including Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- Engaged program and system owners, Information Assurance Managers (IAMs), User Reps, etc. involved in the NAVMED server consolidation initiative (e.g., Network Protection Suite [NPS]) to ensure COOP and contingency protocols are well established and account for NAVMED enclave upstream and downstream dependencies.
- Ensured that the COOP plans for core enterprise services (e.g., MHS, ESOC, MCiS) were created, maintained and included such critical information as products and services supported, points of contact, Service Level Agreements (SLAs), recovery procedures, and protocols.

Navy Medicine (NAVMED), Enterprise Cybersecurity (ECS) Program, Continuous Risk Management (CRM), Subject Matter Expert

- Led and performed numerous technical risk assessments to address specific requirements needing additional validation or evaluation in order to recommend solutions to the ODAA on complex technical issues.
- Provided solutions and support to the NAVMED Enterprise to reduce the level of security risk across the networks and systems.
- Examined Enterprise risks across multiple facets and mitigation strategies developed to reduce the identified risks.
- Managed the strategy, framework and Enterprise plan to:
 - Secure the IT systems that store, process, or transmit organizational information,
 - Enable management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget and
 - Assist management in authorizing (or accrediting) the IT systems based on the supporting documentation resulting from the performance of risk management.
 - Conducted annual comprehensive and manual IA assessments at Navy Medicine sites to estimate the overall security posture of the Enterprise and PORs.

Space and Naval Warfare Systems Center, Atlantic – North Charleston, SC

May 2009 – Feb 2012

Senior Systems Security Engineer/IT Specialist (INFOSEC), Civilian

Department of the Navy, Data Center Consolidation Task Force (DCCTF), IA Subject Matter Expert/Team Lead

- Evaluated Department of the Navy (DON) systems design, functionality and security posture prior to transition to SPAWAR's Cloud Infrastructure/Platform as a Service Delivery Model.
- Facilitated the consistent application of IA policies across hosted systems improving overall cybersecurity posture.
- Supported the rationalization and modernization of the existing DON system portfolio to a much more consistent footprint.

Naval Medical Information Systems Support Activity (NAVMISSA), Enterprise Services Operations Center (ESOC), Information Assurance Manager (IAM)

- Implemented and enforced Federal, Department of Defense (DoD), Department of Navy (DoN), and BUMED specific policies and procedures reflecting the legislative intent of applicable laws and regulations regarding the management and operations

of NOSC/CERT assets, including centrally managed PORs.

- Prepared, distributed, reviewed, tracked, and maintained plans, instructions, guidance, and standard operating procedures concerning the security of NOSC/CERT assets, including centrally managed PORs
- Reviewed the selected security safeguards to determine that security concerns identified in the approved security plan have been fully addressed
- Developed security requirements specific to CERT/NOSC IT acquisitions (hardware, software, and services) for inclusion in statements of work and other procurement documents
- Evaluated the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents for the NOSC/CERT and centrally managed PORs
- Monitored contract performance and periodically review deliverables to NAVMISSA for conformance with contract requirements related to the IA, security, and privacy of the NOSC/CERT and centrally managed PORs
- Participated in the development or modification of the IA security program plans and requirements for NOSC/CERT assets, including centrally managed PORs
- Ensured that all NOSC/CERT assets, including centrally managed PORs with IA enabled software, hardware, and firmware comply with appropriate DoD, DoN, and BUMED security configuration guidelines, policies, and procedures
- Identified functional IA security strategies to address organizational NOSC/CERT and centrally managed POR security concerns
- Provided leadership and direction to CERT personnel by ensuring that IA security awareness, basics, literacy, and training are provided to CERT personnel commensurate with their responsibilities
- Validated NOSC/CERT users' designation for IT Level I or II sensitive positions, per DoD Instruction 8500.2 "Information Assurance (IA) Implementation"
- Ensured all CERT/NOSC system users have signed System Authorization Access Requests and have demonstrated their awareness of their IA responsibilities per requirements stated Statements of Work and annual IA training before granting access to Navy Medicine information systems (Deliverable 7)
- Implemented programs to ensure that users are aware of, understand, and follow NOSC/CERT IA policies and procedures
- Recognized a possible security violation and take appropriate action to report the incident to the Navy Medicine CNDSP, as required by DoD and DoN directives
- Assisted in the gathering and preservation of evidence used in the prosecution of computer crimes
- Supervised and managed protective and corrective measures when an IA incident or vulnerability is discovered that impacts the operations of NOSC/CERT assets, including centrally managed PORs
- Ensured that system security configuration guidelines are followed for all NOSC/CERT assets, including centrally managed PORs
- Ensured that IA requirements are integrated into the Continuity of Operations Plan (COOP) for NOSC/CERT assets, including centrally managed PORs
- Ensured that IA security requirements are appropriately identified in computer environment operation procedures
- Monitored the performance of NOSC/CERT assets, including centrally managed PORs and will review NOSC/CERT assets and centrally managed PORs for compliance with IA security and privacy requirements
- Ensured that IA inspections, tests, and reviews are coordinated for NOSC/CERT assets, including centrally managed PORs
- Participated in an IS risk assessment during the Certification and Accreditation process of NOSC/CERT assets
- Conducted physical security assessments of the NOSC/CERT working spaces and server rooms at SPAWARSSYSCEN-Atlantic and work with NAVMISSA and SPAWAR facilities to correct physical security weaknesses
- Prepared IA certification and accreditation documentation for the NOSC/CERT and centrally managed PORs
- Ensured compliance monitoring of NOSC/CERT assets and centrally managed PORs occurs, and review results of such monitoring
- Advised NAVMISSA IA Leadership of any changes affecting the NOSC/CERT IA posture
- Collect and maintain data needed to meet IA reporting requirements for NOSC/CERT assets, including centrally managed PORs
- Managed and reported to NAVMISSA senior management on behalf of all CERT functional teams

Naval Medical Information Systems Support Activity (NAVMISSA), Enterprise Cybersecurity (ECS) Program, Cyber Evaluation Readiness Team (CERT), Project Manager/Lead

- Managed and executed the NAVMED Enterprise Information Assurance CERT Technical Teams, including: Enterprise Technical Risk Management, Information Assurance Directives Validation and Verification, Enterprise Technical Systems Support, and Enterprise Incident Response and Analysis.
- 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.
- Responsible for establishing, implementing and maintaining the DoD information system IA program, and for documenting the DoD C&A process for NAVMED networks and information systems located at SPAWAR Atlantic and Enterprise deployed Programs of Record.
- Efforts resulted in NAVMED ESOC's receipt of a three year Authority to Operate (ATO) from the Navy Certification Authority, a first for the organization.
- Tracked compliance of centrally managed assets and POA&M progress against Security Requirements Matrices created in XACTA IA Manager or Governance, Risk, and Compliance (GRC) tools
- Provided direction to the Directives Verification and Validation Team as applicable to validating compliancy of centrally managed assets
- Completed and submitted enterprise mitigation plans received from EIA Systems Support on behalf of the NOSC into OCRS
- Tracked and reported Enterprise IAVA/B, CTO, and INFOCON compliancy for centrally managed assets in OCRS and, as required and appropriate, VMS, based on validation metrics received from the Directives Verification and Validation task
- Maintained and made updates, as required and in coordination with the EIA C&A team, to the DIACAP packages for the NAVMEDES, NitroView SIEM, and NPS PORs, as well as the NOSC/CERT site accreditation
- Provided weekly IAVM and INFOCON status reports to NOSC/CERT IAM and NAVMISSA Senior Management for centrally managed assets
- Supported implementation of ITIL Security Management process activities as appropriate to Information Assurance Vulnerability Management
- Developed mitigation plans and POA&Ms for centrally managed devices¹
- Drafted test plans to support the execution of proof of concept technical risk management and compliance strategies within the non-operational environment as applicable for endpoint systems and networks, as well as centrally managed PORs (NAVMEDES, NitroView SIEM, NPS) and NOSC/CERT assets, and provide results to all relevant execution stakeholders, NOSC/CERT IAM, and NAVMISSA leadership (Deliverable 12)
- Provided remote and on-site Tiger Team support to the NOSC and sites as required for system and network-based situations that negatively affect technical security posture.
- Provided IA validation of LAN and WAN changes recommended and/or implemented on Navy Medicine site LANs and WANs by Engineering Services
- Defined, governed, and managed changes to the baseline configurations and technical policy of all EIA technical tools in the operational and virtual lab environments, to include all NPS devices, HBSS, SCTS, XACTA, and others as applicable. This includes providing guidance and IA validation of all requests to the NOSC resulting in changes to NPS device configurations, such as changes to:
 - IronPort/Foundry Layer 4 policies,
 - OSSR ACLs,
 - Service and Site Context firewall rules,
 - IPS blocking categories and User Defined Signatures,
 - IPS exceptions, and
 - Network routing changes.
- In conjunction with the NOSC, developed automated workflows to track the process of receiving change requests to the NPS devices, capturing the validation of the changes, and transferring implementation of those change requests from the CERT to

the NOSC for implementation.

- Provided technical subject matter expertise to NOSC teams for NPS, NAVMEDES, network, and system vulnerability remediation
- Conducted periodic IA assessment of all Navy Medicine NPS device configuration
- Provided Local Registration Authority (LRA) support for Navy Medicine servers and other security certifications.
- Supported the use of scanning and patching tools (WSUS, SMS, AD, HBSS, etc) as necessary to maintain sites' security postures
- Provided subject matter expertise for PKI to include CAC/PIV implementation, as well as identification, authentication, and authorization policy and strategies
- Reviewed HBSS deployment to ensure site assets are adequately protected and properly managed
- Reviewed HBSS deployment to ensure assigned policies supported the expected security posture of the sites in accordance with applicable CTO requirements
- Provided periodic knowledge transfer regarding the use and configuration of IA tools from Tiger Team subject matter experts to the stakeholder community for HBSS, SCTS, XACTA and other tools for which sites share access
- Supported NAVMISSA Technical Risk Management for initial tool selection, deployment, configuration, and population
- Provided technical recommendations and support for Enterprise Cyber Incident Response and Analysis teams, including on-site incident response activities as required
- Governed the use of all EIA technical tools by NOSC/CERT in support of the ITIL Security Management process activities
- Continuously monitored (24x7) all centrally managed assets (NAVMEDES, Nitro, and NPS PORs, as well as NOSC/CERT assets) and analyze possible cyber security events, intrusions, and anomalies impacting site and centrally controlled assets, as detected by Enterprise-managed IA tools, to include, but not limited to, the Nitro Security Event Information Manager, AD servers, HBSS servers, and network-based IPS systems
- Analyzed cyber security events, intrusions, anomalies, and events using network and host-based tools, Nitro SIEM, network-based IPS, and other supporting tools
- Liaised, when necessary, with Tiger Team subject matter experts to correlate information from detected events with system states as reported by vulnerability scanning and patching tools.
- Served as central POC to the Navy Medicine CNDSP for all reported cyber incidents on Navy Medicine networks
- Responded to and Investigate Cyber Incidents as required
- Maintained, executed, and updated the Enterprise Incident Response Standard Operating Procedures to be consistent with ITIL Security Management functions for incident response
- Supported ongoing investigations and forensic analysis to include intrusion modeling and simulation in virtual environments
- Provided Enterprise-wide Cyber Incident Metrics and Threat Analyses to NAVMISSA Senior Management
- Liaised, as necessary, with Tiger Team subject matter experts to develop recommendations for technical policy changes (IPS Blocks, DNS Blackholes, etc.) to NAVMISSA Senior Management in response to detected threats and other emerging changes in the cyber landscape as detected by the Navy Medicine CNDSP and Navy Medicine cyber security stakeholders and subject matter experts

Science Applications International Corporation (SAIC) – North Charleston, SC

Dec 2005 – May 2009

Systems Security Analyst

Navy Medicine Information Management Command (NMIMC), Enterprise Host Based Security System (HBSS), Technical Lead

- Executed HBSS project initiation, planning, design, configuration and deployment preparation tasks.
- Conducted in-depth research, evaluation, and testing in the development of the Navy Medicine Enterprise HBSS architecture to ensure design complied with DoD and DoN policies.
- Provided subject matter expertise and advanced solutions relating to all technical aspects of the NAVMED Enterprise HBSS deployment to include systems and virtualization design, deployment coordination and preparation, hardware selection and procurement, technical training and documentation, and management of personnel.

Navy Medicine Information Management Command (NMIMC), Enterprise Engineering and Technical Services Team (EETS), Subject Matter Expert

- 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.

Navy Medicine Information Management Command (NMIMC), Enterprise Active Directory, Deployment Lead

- Responsible for the implementation and migration of an Enterprise Active Directory solution across NAVMED MTF's, remote clinics, and supporting agencies.
- Administered network security and access devices, DNS, access control lists (ACL's), TCP/IP, systems management and monitoring technologies, Quest Migration Manager and MS Exchange.
- Provided training to on-site operators and performed System Operational Verification and Testing (SOVT) on deployed network security systems.

WareOnEarth Communications, Inc. – North Charleston, SC

Aug 2003 – Dec 2005

Network Engineer

Navy Medicine Information Management Command (NMIMC), Last Mile/Community of Interest (COI) Program, Team Lead

- 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.
- Led the implementation of secure Internet connectivity solutions including firewalls, router ACL's, demilitarized zones (DMZ), VPN's, IDS's, and DNS.

Navy Medicine Information Management Command (NMIMC), Defense Medical Logistics Standard Support, (DMLSS) Secure Wireless Deployment, Team Lead

- Contributed to the operation, design, and implementation of 802.11 technologies and standards for the Tri-Service Infrastructure Management Office (TIMPO).
- Deployed 802.11 wireless solutions providing encryption, authentication, data integrity checking, key exchange, and data compression to ensure integrity of enterprise applications and network resources.

United States Marine Corps (USMC) – Camp LeJeune, NC

Sep 1999 – Sep 2003

Small Computer Systems Specialist/Network Engineer (Enlisted)

II Marine Expeditionary Force (MEF), 8th Communications Battalion

- Primary responsibilities included the design, implementation, administration, and sustainment of Cisco Firewalls, Routers and Switches, Microsoft Server/Windows, Microsoft Exchange Server and other network systems in support of operations worldwide, including both tactical and garrison.
- Provided network and systems support while deployed with the 22nd Marine Expeditionary Unit (MEU) Joint Task Force (JTF) in 2002 during Operation Enduring Freedom and with the II Marine Expeditionary Brigade, 8th Communications Battalion in 2003 during Operation Iraqi Freedom.