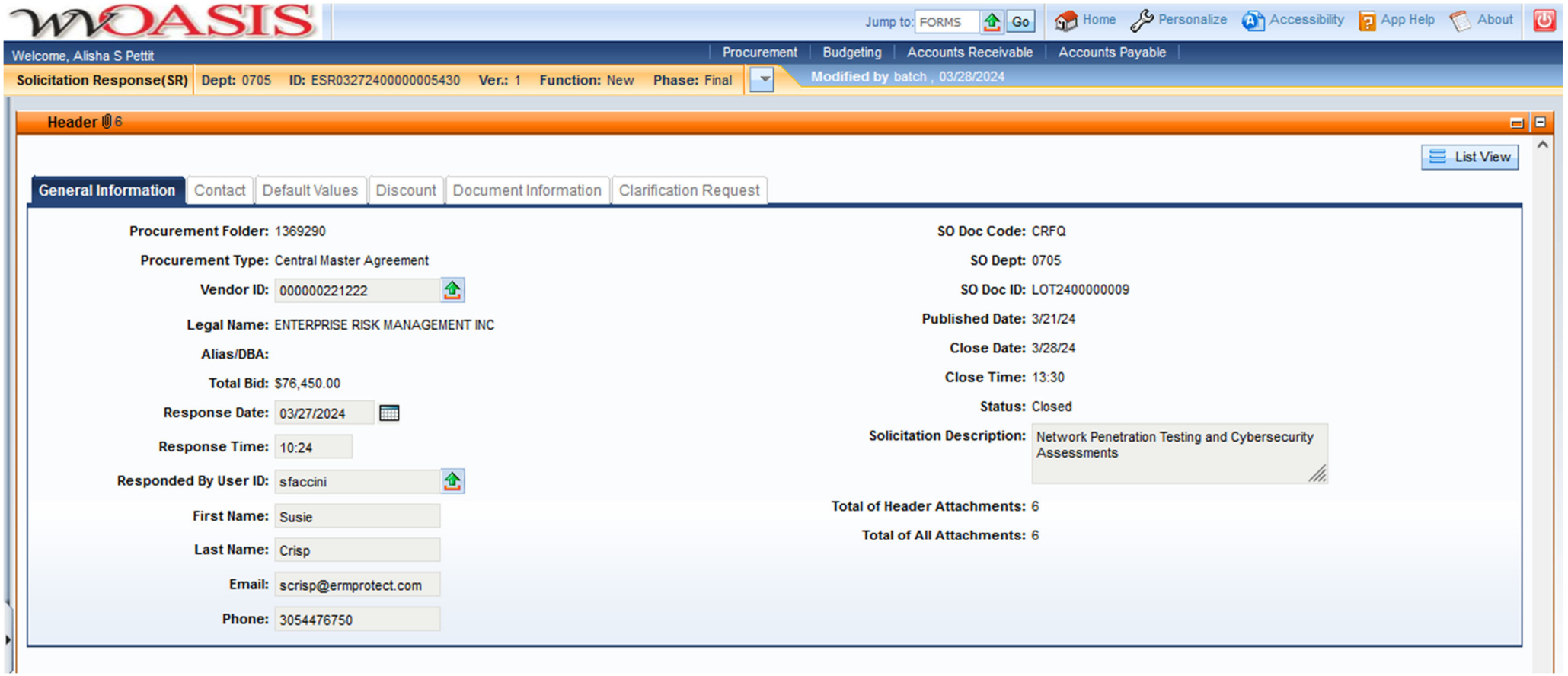
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency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


wvOASIS
Jump to: FORMS Go
Home
Personalize
Accessibility
App Help
About
Welcome, Alisha S Pettit
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR)
Dept: 0705
ID: ESR03272400000005430
Ver.: 1
Function: New
Phase: Final
Modified by batch , 03/28/2024
Header 6
List View
General Information
Contact
Default Values
Discount
Document Information
Clarification Request
Procurement Folder: 1369290
Procurement Type: Central Master Agreement
Vendor ID: 000000221222
Legal Name: ENTERPRISE RISK MANAGEMENT INC
Alias/DBA:
Total Bid: $76,450.00
Response Date: 03/27/2024
Response Time: 10:24
Responded By User ID: sfaccini
First Name: Susie
Last Name: Crisp
Email: scrisp@ermprotect.com
Phone: 3054476750
SO Doc Code: CRFQ
SO Dept: 0705
SO Doc ID: LOT2400000009
Published Date: 3/21/24
Close Date: 3/28/24
Close Time: 13:30
Status: Closed
Solicitation Description: Network Penetration Testing and Cybersecurity Assessments
Total of Header Attachments: 6
Total of All Attachments: 6

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

State of West Virginia
Solicitation Response

Proc Folder:	1369290
Solicitation Description:	Network Penetration Testing and Cybersecurity Assessments
Proc Type:	Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2024-03-28 13:30	SR 0705 ESR03272400000005430	1

VENDOR

000000221222
ENTERPRISE RISK MANAGEMENT INC

Solicitation Number: CRFQ 0705 LOT2400000009

Total Bid: 76450 **Response Date:** 2024-03-27 **Response Time:** 10:24:11

Comments:

FOR INFORMATION CONTACT THE BUYER
Brandon L Barr
304-558-2652
brandon.l.barr@wv.gov

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

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	External Network Penetration Testing				11880.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: External Network Penetration Testing - two full assessments for eight locations per year

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Website Penetration Testing				7160.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Website Penetration Testing: two full assessments per year

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Internal/Client-Side Network Penetration Testing				25530.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Internal/Client-Side Network Penetration Testing: two full assessments for eight locations per year. completed in one trip.

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Wireless Penetration Testing				31880.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Wireless Penetration Testing: two full assessments for eight locations per year. completed in one trip.

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

ERMProtect
Cybersecurity Solutions

Enterprise Risk Management, Inc. dba
ERMProtect™
Response to Request for Proposal
March 27, 2024

State of West Virginia
Request for Proposal
Network Security Penetration Testing Services
CRFQ LOT2400000009

ERMProtect
Cybersecurity Solutions

Table of Contents

ERMProtect
Cybersecurity Solutions

Company Overview

Enterprise Risk Management, Inc. (dba ERMProtect) appreciates the opportunity to introduce out company and present this proposal to the State of West Virginia in response to its Request for Quotations: **Network Penetration Testing and Cybersecurity Assessments** (CRFQ LOT2400000009) for the West Virginia Lottery.

ERMProtect™ is a Florida corporation that began business in 1998 and provides Cybersecurity Professional Consulting services. Our offices are located in Coral Gables, FL, where we employ 20 professionals. The following is our general contact information:

Name of Principal:	Silka M. Gonzalez, President
Business Name:	Enterprise Risk Management, Inc. dba ERMProtect™
Business Address:	800 S. Douglas Rd. Suite 940 North Tower, Coral Gables, FL 33134
Business Phone:	(305) 447-6750
Email Address:	sgonzalez@ermprotect.com
Website:	https://ermprotect.com

ERMProtect is a minority-owned firm that has adapted, evolved, and excelled because it emphasizes education, training, integrity, adaptability, service, and diversity of people and ideas. We are a Women Business Enterprise (WBE) certified in Miami-Dade County and by the US Small Business Administration (SBA) for the Women-Owned Small Business Federal Contract Program (WOSB Program).

With twenty-six (26) years of experience in information security, ERMProtect is a trusted, go-to provider of comprehensive information security services to more than 450 clients in 39 industry verticals in the United States, Latin America, the Caribbean and Europe. Government clients at the County, City and Local level make up one of the most important groups we serve. We have actually performed Penetration Testing services for the State of West Virginia State's Treasurer's Office for more than 3 years.

We have extensive knowledge and experience with cybersecurity assessments, penetration testing, cybersecurity audits, different types of security risk assessments (FACTA, GLBA, HIPAA, GDPR, NIST, etc.), outsourced security services and co-sourcing, remediation, cybersecurity controls implementation, incident response, digital forensics, cybersecurity awareness training, cryptocurrency investigations and cybersecurity products. This knowledge and experience give us the background required to provide you with in-depth IT security services.

While ERMProtect has extensive experience in all areas mentioned above, **Penetration Testing and Cybersecurity Assessments** are services that account for a large percentage of our work and revenues. Our security consultants perform different types of penetration tests on a weekly basis. We are always improving our methods, tools, and learning new techniques to improve our penetration tests.

Our professionals have achieved excellence in education from some of the nation's most prestigious institutions and hold some of the highest certifications in our profession. These certifications include PCI QSA, PCI PFI, CISSP, CISA, CRISC, CIPP, CISM, CIA, C|EH, GPEN, CPA and many others.

In the sections of the response below, we will provide a more comprehensive description of our services and experience to demonstrate our qualifications.

ERMProtect
Cybersecurity Solutions

Qualifications and Experience

Services Provided

ERMProtect provides services in four (4) major areas:

1. **Cybersecurity Assessments and IT Audits**

   Through its years in service, ERMProtect has performed thousands of security assessments and IT control reviews of various types to help clients identify vulnerabilities and build up their defenses. This area has always been one of our leading sources of revenue.

   The most common are:

   - All types of Penetration Testing (external, internal, web/mobile applications, wireless, segmentation tests and others required by the Payment Card Industry (PCI) Council, Cloud Infrastructure, ICS/SCADA, Physical Site, IoT, Social Engineering and Regulatory Compliance).
   - Assessments required by the Payment Card Industry (PCI) Council – PCI QSA, PCI Scans, PCI Penetration Tests
   - General Risk Assessments oriented towards the compliance of different federal, state or local laws (HIPAA, FISMA, FERPA, GDPR, GLBA, FACTA, FedRamp), for the Information Technology Area, or the entire organization.
   - Different types of Cybersecurity Assessments with different scopes, requirements and use of various security standards such as NIST, ISO27001 and CIS security model.
   - SOC 2 Attestations and Comprehensive security and IT Audits with varying scopes.

2. **Co-Sourcing of Cybersecurity Services**

   We have provided consulting, guidance, implementation, and remediation services to many clients, both fully and partially depending on their needs. Some examples of these include:

   - Review/Implementation of security plan, standards, policies, procedures
   - CISO co-sourcing or full outsourcing.
   - Incident Response on-demand
   - Implementation/remediation of security for specific areas and technologies
   - On-demand security advisory services
   - Performance of third-party vendor security assessments

3. **Digital Forensics**

   Digital Forensics is one of ERMProtect's fastest growing areas of business. Our digital forensic and incident response experts help organizations stop, recover from, and get to the bottom of a breach with a thorough forensic investigation. This area includes:

   - Investigation of Security Incidents and Data Breaches of all types
   - Investigation of security breaches related to the Payment Card Industry (PCI PFI)
   - Fraud or internal misconduct investigations
   - Litigation Support
   - Crypto Investigations

4. **Security Awareness Training and Social Engineering**

   ERMProtect has developed various types of security awareness training content which can be delivered in any of the following ways:

   - Through an LMS System, by subscription – many courses covering many security areas.
   - "A la Carte" – clients can choose courses in SCORM version to download into their own LMS system.
   - Customized security training, tailored to the needs of the client – technical and non-technical.

   ERMProtect also developed its own tool for performing phishing, vishing and smishing tests. These tests are customized and automated for the needs of each client.

ERMProtect Experience – similar projects and references

The following are a few examples of projects we have performed and attest to our experience. For each of the examples, we provide references whom you can contact to verify information regarding our company and our team members who have participated in various of these projects.

- **State of West Virginia – State Treasurer's Office**
  ERMProtect has performed annual external penetration testing services to the West Virginia State Treasurer's Office for over three years.

Contact Name:	Lisa Rutherford, Lisa.Rutherford@wvsto.com
Contact Title:	Director of Internal Audit
Telephone:	(304) 341-0718

- **Broward County** – In the last two years we have performed several projects for the Broward County including an IT Risk Assessment and PCI Security Assessment for the Aviation Department and an IT Audit and a SCADA Security Review for the Water and Waste Department. We are also currently working on a project to review the Broward County Incident Response Plan.

  Broward Waste and Wastewater Services

Contact Name:	Alan Garcia, agarcia@broward.org
Contact Title:	Director
Telephone:	(954) 831-0702

  Broward County - ETS

Contact Name:	Gail McGowan, gmcgowan@broward.org
Contact Title:	ETS, IT Business Services, Security & Compliance
Telephone:	(954) 357-6147

  Broward County – Aviation Department

Contact Name:	Karen Macdougall – kmacdougal@broward.org
Contact Title:	Information Technology Specialist
Telephone:	954 359-7213

- **Miami-Dade County** – For the past several years, we have performed various types of penetration testing (external, internal, web application and wireless) for Miami-Dade County,

the 7th largest county in the United States, with an annual operating budget of more than $9 billion. We completed a five-year contract to provide penetration testing, PCI QSA services, digital forensic services, and security risk assessments. The engagement includes testing of 500 internal IP addresses, 210 external IP addresses and 28 applications used by executive, administrative, operational, transportation service departments and airports. ERMProtect was just awarded the contract to provide these services for the next five years.

Contact Name:	Lars Schmekel - lars.schmekel@miamidade.gov
Contact Title:	Chief Security Officer
Telephone:	305 596-8779

- **Metropolitan Washington Airport Authority (MWAA)** – For the past several years, we have performed internal network, external network and web application penetration testing for the Metropolitan Washington Airport Authority, which operates Reagan National and Dulles International Airports. The engagement involves testing 1,100 internal IP addresses and 12 external IP addresses. We also perform PCI QSA services for MWAA.

Contact Name:	Kevin James - kevin.james@MWAA.com
Contact Title:	Chief Information Security Officer
Telephone:	(703) 417-8600 703-417-8389

- **Port of Oakland** - we recently entered into a seven-year contract to perform all types of penetration test including external, internal and wireless network penetration tests, application penetration tests and vulnerability and security assessments for the Port of Oakland.

Contact Name:	Chris Hanna - channa@portoakland.com
Contact Title:	IT Security Manager
Telephone:	510-627-1125

- **Other Municipalities** – We perform internal network, external network and web application penetration testing, for all departments of the following cities. We have also performed PCI QSA assessments, digital forensics, security risk assessments and security training for some of them.

City of Miramar

Contact Name:	Junior Ambresena - jambresena@miramarfl.gov
Contact Title:	Cybersecurity Manager
Telephone:	954-602-3434

City of Cape Coral

Contact Name:	Elizabeth Merriken - emerrike@capecoral.net
Contact Title:	IT Security Manager
Telephone:	239 573-3085

City of Coral Gables

Contact Name:	Nelson Gonzalez - ngonzalez@coralgables.com
Contact Title:	Assistant Information Technology Director
Telephone:	305 460-5076

City of Deerfield Beach

Contact Name:	Ronald McKenzie – rmckenzie@deerfield-beach.com
Contact Title:	Chief Information Officer
Telephone:	954 571-7577

City of Lake Worth Beach

Contact Name:	Nelly Peralta – nperalta@lakeworthbeachfl.gov
Contact Title:	Assistant Information Technology Director
Telephone:	561 719-2700

City of Sanibel

Contact Name:	Bert Smith – Bert.Smith@mysanibel.com
Contact Title:	IT Director
Telephone:	239 472-3700

City of St. Petersburg

Contact Name:	Brian Campbell – brian.campbell@stpete.org
Contact Title:	Information Technology Security Officer
Telephone:	727 892-5503

City of Melbourne

Contact Name:	Howard Cheatham – howard.cheatham@mlbf.org
Contact Title:	Information Systems Security Officer
Telephone:	321 608-7700

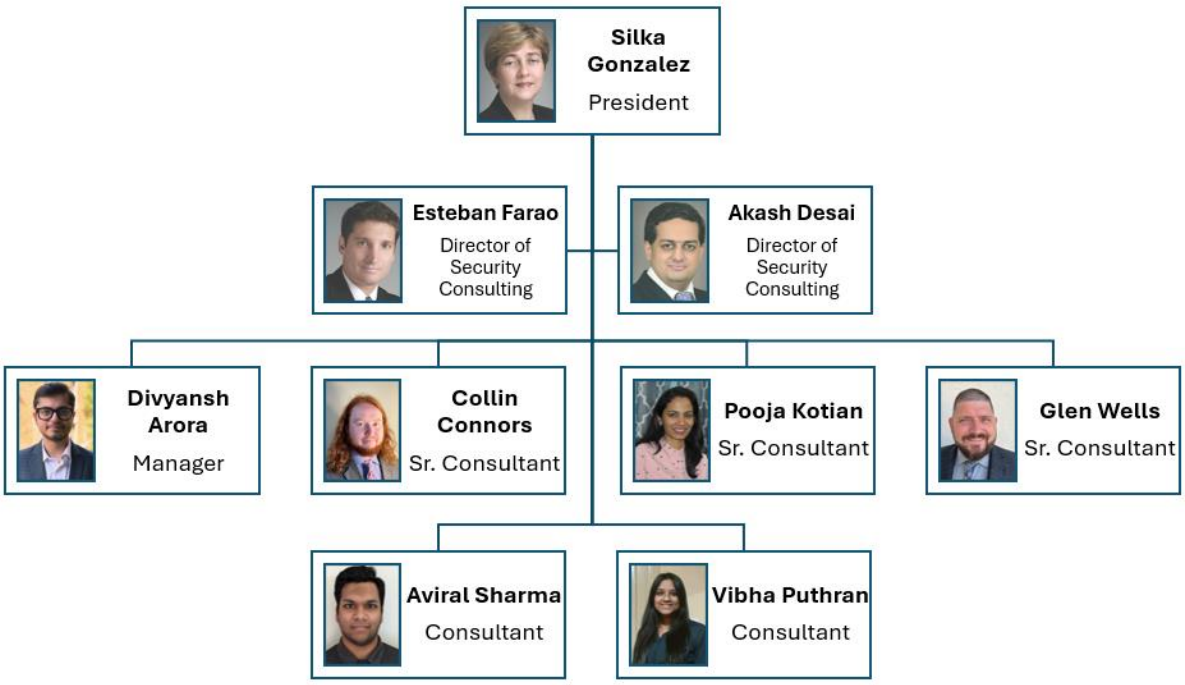
City of West Palm Beach

Contact Name:	Paul Jones - pjones@wpb.org
Contact Title:	Chief Information Officer
Telephone:	561 578-2420/561 822-1258

ERMProtect Team

ERMProtect's team has highly respected educational and professional qualifications. Our professionals have earned master's degrees, specifically in information security and networking, from esteemed institutions of learning such as the Carnegie Mellon University, Purdue University, John Hopkins, MIT, Georgia Tech and the University of Miami, and hold reputed professional information security certifications such as the Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker ((IEH), PCI Approved Qualified Security Assessor (QSA), PCI Professional Forensic Investigator (PFI) and the Certified Information Systems Auditor (CISA), to name only a few.

The following is an organizational chart depicting our proposed project team and below also a summary of their qualifications:



Silka Gonzalez

President and Founder of ERMProtect. Silka has more than 35 years of experience in the field of cybersecurity. Since 1998, ERMProtect has provided cybersecurity, computer forensics and technical compliance services to more than 450 recurring clients in 39 different industries worldwide. Prior to founding ERMProtect, she was a manager of IT and business services at Price Waterhouse. She also served as Manager of Information Systems Auditing for Diageo PLC and Manager of Information Systems Security for American Bankers Insurance Group (now Assurant Solutions).

Silka received Bachelor's degrees in both Computer Information Systems and Accounting from Xavier University in Cincinnati, Ohio and she received a Master's degree in Accounting Information Systems from Florida International University in Miami. Silka also completed an Entrepreneurial Master's Program at the Massachusetts Institute of Technology (MIT) in Boston. Silka's certifications include CISSP, CISM, CISA, CITP, CRISC, PCI-QSA, CPA and ISO27001 Auditor.

Silka is a published author, addressing current issues in cybersecurity, IT auditing, regulatory compliance and computer forensics. Silka is frequently sought out by local and national newspapers and magazines as a subject matter expert in cyber security. She also appears in local and national news as a cybersecurity expert.

Silka previously served as a board member of the Florida International Bankers Association (FIBA), as member of Florida International University's President Council, as president of the Miami chapter of the Institute of Internal Auditors, and the boards of ISACA South Florida (Information Systems Audit and Control Association) and ALPFA (Association of Latino Professionals in Finance and Accounting). She has also served on Florida's judicial nomination commission for workman's compensation judges.

Esteban Farao

Director of Information Security Consulting Services. Esteban has worked at ERMProtect for 21 years and has more than 29 years in the Cybersecurity industry. As a cybersecurity expert, he has extensive experience in all types of ethical hacking, performance of IT and\or cybersecurity audits, performance of security implementations, performance of all types of cybersecurity risk assessments using all types of NIST cybersecurity standards, ISO27001 standards, state and federal cybersecurity laws and regulations, and cybersecurity frameworks. Esteban has also been involved in many large PCI Cybersecurity audits, compliance, and remediation projects for all the largest and most complex clients of ERMProtect. He also has extensive experience in digital forensics project investigating regular security breaches, credit card breaches, fraud investigations, internal misconduct, and litigation support cases. Additionally, Esteban has developed, enhanced, and tested many business continuity plans and security incident response plans as well as security strategies, plans, policies and procedures. He also has developed and delivered different types of cybersecurity trainings, (including complex security incident response table talk training to an entire City), assist many large clients with on-going consultation, publish cybersecurity articles and is frequently interviewed by television networks to share his security expertise.

Prior to joining ERMProtect, Esteban worked 6 years for PwC Argentina where we performed different types of cyber security projects. He also participated in global attack and penetration testing assignments for PwC in London. Esteban hold a Bachelor's Degree in Computer Science, a Master degree in Computer Information Systems, and a Master in Business Administration (MBA). He holds the following IT **Security Certifications: CISSP, CISA, CRISC, C|CISO, CEH, PCIP, PCI QSA, PCI PFI and EnCe, CNDA, CDPSE, and ISO27001 Auditor.**

Akash Desai

Director of Information Security Consulting Services. Akash has worked at ERMProtect for 17 years. As a cybersecurity expert, he has extensive experience in all types of ethical hacking, performance of IT and\or cybersecurity audits, performance of security implementations, performance of all types of cybersecurity risk assessments using all types of NIST cybersecurity standards, ISO27001 standards, state and federal laws and regulations, and cybersecurity frameworks. Akash has also been involved in many large PCI Cybersecurity audits, compliance, and remediation projects for all the largest and most complex clients of ERMProtect. Akash has developed, enhanced, and tested many business continuity plans and security incident response plans as well as security strategies, plans, policies and procedures. He developed ERMProtect's security awareness training practice which offers off-the-shelf and customized training for employees using animations, games, mini lectures, etc. Akash as developed and delivered different types of cybersecurity trainings, assist many large clients with on-going consultation, publish cybersecurity articles and is frequently interviewed by magazines, newspapers, and television networks to share his security expertise.

Prior to working for ERMProtect, Akash worked for CERT for two years specializing in security incident response. Akash holds a Bachelor's degree in Computer Science and a Master degree in Information Networking with a Cybersecurity specialization from Carnegie Mellon University and the following IT **Security Certifications: CISSP, CISA, CEH, PCI QSA and PCIP**.

Pooja Kotian

Manager, Information Security Consulting Services. Pooja has worked at ERMProtect for 9 years, and has more than 12 years of experience as a Senior Systems Engineer and as an Information Security Consultant overseeing many types of cyber security projects. As a cybersecurity expert, she has

extensive experience in all types of ethical hacking, performance of IT and\or cybersecurity audits, performance of security implementations, performance of all types of cybersecurity risk assessments using all types of NIST cybersecurity standards, ISO27001 standards, state and federal laws and regulations, and cybersecurity frameworks. Pooja has also been involved in many large PCI Cybersecurity audits, compliance, and remediation projects for all the largest and most complex clients of ERMPROTECT. Pooja has developed, enhanced, and tested many business continuity plans, security incident response plans as well as security strategies, plans, policies and procedures.

She began her career as a Systems Engineer for Infosys before joining ERMProtect in 2015 where she was a mobile and web application developer with significant experience testing applications for issues and vulnerabilities so they can be corrected. She has a Bachelor's degree in Engineering, Information Technology. Pooja holds the following **security certifications**: **Infosys Quality Foundation, Dotnet Technology 101 and STAR Certification** (internal to Infosys).

Divyansh Arora

Manager, Information Security Consulting Services. With three years of experience at ERMProtect, Divyansh has been involved in a wide range of activities, including ethical hacking, IT and cybersecurity audits, security implementations, and various cybersecurity risk assessments using NIST cybersecurity standards, ISO27001 standards, and cybersecurity frameworks. He has also contributed to PCI Cybersecurity audits, compliance, and remediation projects for some of ERMProtect's largest clients. Additionally, Divyansh has participated in digital forensics projects, investigating security breaches, credit card breaches, fraud cases, internal misconduct, and litigation support.

Before earning his master's degree in Information Technology- Information Security from Carnegie Mellon University, Divyansh obtained a bachelor's degree in Computer and Communications.
Prior to joining ERMProtect, he served as a Senior Cybersecurity Analyst at PricewaterhouseCoopers for nearly two years. During his time at PwC, Divyansh conducted numerous vulnerability assessments and penetration tests for web applications, networks, Android & iOS mobile applications, and IoT devices such as CCTV and C&C displays for both government and private clients. He also gained experience as an intern at McKinsey Investment Office, focusing on cloud security research.
Security certifications: OSCP, CMWAPT

Collin Connors

Senior Information Security Consultant. Collin has worked for 5 years at ERMProtect. He has extensive experience in performing all types of penetration and phishing testing, as well as, cybersecurity audits, various types of cybersecurity risk assessments using all types of NIST cybersecurity standards, ISO 27001 standards and cybersecurity frameworks. Additionally, he has provided services surrounding various federal and state cybersecurity laws (e.g. GLBA, FACTA, HIPAA). Collin also has extensive knowledge and experience in cryptocurrency investigations and has participated in several Digital Forensics projects. Some of these cryptocurrency investigations have also resulted in people's conviction to prison. He has developed various automated system products for ERMProtect including an automated phishing tool, a phishing email analysis tool, and an automated system that performs SOC2 Assessments.

Collin also oversees the company's internal IT and security. He has a lot of experience in conducting cybersecurity trainings for external clients as well as ERMProtect's internal staff. His on-going consultations and customized trainings are very highly regarded and impactful. He is frequently

interviewed by television networks to share his research and knowledge regarding cryptocurrency, blockchains and cybersecurity.

Apart from working at ERMProtect, Collin is also a part-time teacher at the University of Miami where he teaches cybersecurity and computer programming to undergraduate students. He holds a bachelor's degree in computer science and mathematics and is expected to complete his PhD Degree in May 2025. His PhD research includes the use of artificial intelligence to detect malware and various novel implementations of blockchain technology. **Security certifications: CISc**

Aviral Sharma

Information Security Consultant. Aviral worked as a student intern for ERMProtect during the summer of 2022, and he became a full-time employee in February 2023. During his time at ERMProtect he has performed security risk assessments, data compliance assessments, IT audits and various types of penetration testing.

Aviral has a Bachelor's degree in Computer Science and Engineering with a specialization in Information Security, and received his master's degree in Information Technology – Information Security from the prestigious Carnegie Mellon University. At CMU he underwent advanced training in code reviews, digital forensics, and vulnerability assessments for mobile applications.

Vibha Puthran

Information Security Consultant. Vibha worked as a student intern for ERMProtect during the summer of 2023 and started her full-time job with us as an Information Security Consultant in February of this year. She performs incident response cases and digital forensic investigations for the firm's diverse client base. She specializes in incident response investigations like ransomware, tabletop exercises, incident planning and management and security awareness training. She has also participated in IT audits.

Prior to joining ERMProtect, she worked as a Cybersecurity Consultant for PwC in India for one and a half years. Vibha has a bachelor's degree in Computer Science-Engineering, a postgraduate Diploma in Cyber Law and Cyber Forensics from the National Law School of India University, and a Master's degree in Information Security from Carnegie Mellon University. **Security Certifications: EC Council Incident Handler, Microsoft Azure Fundamentals, CyberArk Certified Trustee, Splunk 7. X Fundamentals Part 1, Autopsy and Cyber Triage DFIR, ICSI CNSS and AWS Cloud Practitioner.**

To see each of our consultant's resumes please refer to the **Appendix: ERMProtect's Team resumes.**

Project Approach and Methodologies

ERMProtect understands that West Virginia Lottery aims to evaluate its cybersecurity posture and is seeking external expertise to perform network penetration testing and cybersecurity assessments. ERMProtect's assessments will follow the Center for Internet Security methodology and employ techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide. ERMProtect's services will thoroughly assess and evaluate West Virginia Lottery's infrastructure to identify areas that present an exploitable vulnerability available to attackers using a combination of automated tools and manual techniques.

Based on ERMProtect's understanding the following assessments/reviews will be required as part of the scope of work that West Virginia Lottery requires:

1. External Network Vulnerability Assessment and Penetration Test
2. Internal Network Vulnerability Assessment and Penetration Test
3. Web Application Penetration Test
4. Wireless Network Penetration Test
5. Social Engineering Assessment

ERMProtect's project approach along with the detailed technical methodologies for each of the project tasks above has been provided below.

Project Management

ERMProtect's project team will be led by a project manager. The project manager will direct, supervise, and manage a team of cybersecurity experts. This team will include all staff levels including Directors, Managers, Senior Consultants, and Consultants.

Our project management methodology is a time-tested one that incorporates compliance with all requirements that our clients require of us. Our extensive history in providing cybersecurity support to our clients results in our staff being comprised of seasoned, certified, and experienced professionals. We ensure that each contract or task order is well managed and staffed by a certified lead, hands-on and performs the support on-site as required. We utilize PMBOK and other proven processes and best practices to ensure our contracts and tasks comply with client requirements. For all our clients, we ensure we understand and incorporate existing and evolving regulations into our processes and deliverables.

Lines of Responsibility, Authority and Communication

ERMProtect executives are accomplished and seasoned program managers. The Founder and President, Silka Gonzalez, has managed ERMProtect from its inception. This project has the highest levels of corporate commitment to success and Ms. Gonzalez will ensure the project is on schedule, on budget, with the right resources and that the performance represents our excellent history of client satisfaction.

Mr. Esteban Farao, Director of Consulting Services at ERMProtect and our proposed Project Manager for this project will provide the project level day to day oversight to this project. Mr. Farao possesses a strong project and program management background and several years of information security experience with several projects of this nature. He will submit the weekly status reports, deliverables on schedule, and reviews invoices sent to the client as required by contract terms. The report covers all current and planned activities the various teams perform across the tasks and identifies any potential risk or issue areas. Mr.

Farao will ensure full compliance and program level management of personnel and is fully able to commit for the company as appropriate to avoid delays. ERMProtect's plan for this project involves several facilitated meetings and discussion sessions. The Project Manager will be the main coordinator and facilitator for all meetings and discussion sessions throughout the project performance period. Mr. Farao will provide project planning and leadership to the entire team. He reports directly to Ms. Gonzalez, has her full support, and is empowered to make decisions regarding day-to-day operations.

Our Operations team will provide the corporate contracts management and administration function for this contract and any resultant task orders. We will ensure full compliance, contract level reporting as needed, and oversee invoice submissions and task management financial functions.

ERMProtect fully recognizes the importance of effective personnel and project management, and we carefully select project managers for key assignments to ensure they have the requisite skills for the job at hand.

Management Methodology

The nature of our business is multi-year relationships with clients whereby multiple tasks are issued to address various security issues. Our client retention rate is approximately 90% which illustrates our success in delivering and managing our projects and deliverables with excellent results. Clients return to us time after time, and we are able to respond within often short timeframes to address urgent situations. We also have long term contracts with multiple task orders where we adhere to monthly project deliverables and provide performance metrics and quality control.

ERMProtect brings a strong, yet flexible program management approach to multi-year projects. Our experience working with clients on intense and rapidly evolving projects has resulted in the development of a scalable project management methodology encompassing the full life cycle of a project including project initiation, planning, executing, monitoring and controlling, and closing out activities and/or programs. In meeting the requirements of this project, our program management strategy will emphasize project planning, quality control, accurate invoicing and reporting, and workload balance throughout project execution.

Our management approach provides cohesive management to all project tasks with staffing occurring both on and off site, avoiding any perception of personal services. It also provides appropriate levels of task management for day-to-day operations.

We will attend task kick-off meetings meeting contract requirements award in person or telephonically as desired by the client. Additionally, we will attend project and task level meetings as needed with appropriate resources attending as necessary. We will meet all task level deliverables and schedules and reporting requirements and submit all required security forms for each employee. We will notify the client immediately when an employee leaves and return their identification card within five (5) days of departure.

ERMProtect
Cybersecurity Solutions

ERMProtect Management Methodology

DEFINED	TIME-TESTED	ROBUST	THOROUGH
CHAIN OF COMMAND	**PROJECT MANAGEMENT METHODOLOGY**	**TOOLS AND REPORTING**	**BACKGROUND CHECKS AND SECURITY**
Clear lines of responsibility, chain of command, and escalation pathways for seamless project movement.	Incorporates compliance, allows flexibility and adaptability to evolving requirements, ensures quality and accuracy.	Enables work breakdown structures, goal-focused project tracking, timely status reporting, and precise issue mitigation.	Employees' credit and backgrounds checked – ongoing as well as random. Secure information exchange with client over sFTP and encrypted emails. Reliable and tested service continuity management processes.

Reporting, Escalation, and Problem Resolution

Mr. Farao will assume full responsibility for preparing meeting agendas, facilitation of sessions, creation and distribution of meeting minutes, and coordination of action items. This will include notifications to meeting attendees, arrangement of meeting facilities, and coordination of any other requisite resources for these meetings and discussion sessions and resultant reports.

The Project Manager will proactively identify risk and when issues materialize will implement agreed upon mitigating strategies to reduce program impact. Mr. Farao will provide the day-to-day management of all tasks, functioning as the lead interface with the client point of contact.

Mr. Farao has complete access to the ERMProtect executive team and corporate resources as needed and is fully empowered to perform assigned duties. Any issues arising during the performance of the contract will be brought to the attention of the PM. Within 24 hours, if there is no resolution, it will be escalated to Ms. Gonzalez. We have never had an issue arise that could not be handled at this level to resolve any issues and ensure total and complete customer satisfaction. ERMProtect understands it is our full responsibility to ensure excellent performance, rapid response to issues, and continued work under the contract.

Tools/Reporting

ERMProtect utilizes a work breakdown structure, tools, and time-management/reporting tools to manage and account for contract, task order, and financial tracking and reporting. This allows us to have visibility into task spending levels based on established staffing and schedules. The status of the project and each task will be a topic of each monthly status report. Additionally, weekly status reports addressing each task will be provided and any issues will be presented, and a mitigation plan presented for any involving our tasks. Other deliverables will be defined by final Task Order and provided in the agreed upon format.

Employee Background Checks

It is ERMProtect's policy that all employees will be required to undergo a criminal background check and a credit history check prior to joining the organization. At the time of joining, an employee is screened based on the following procedures –

- Collection of photographs
- Verification of aliases

- Criminal history check
- Credit report check
- Comparison of fingerprints with National and Florida State databases

Additionally, employee backgrounds and credit reports are checked on an ongoing basis as and when required, including, but not limited to, random checks from time to time.

Service Continuity Management

ERMProtect fully recognizes and supports the need for service continuity to its clients in the face of natural disasters/calamities, electrical faults, pandemic outbreaks, non-availability of resources, and/or other such interruptions that threaten the course of normal service provision to our clients.

ERMProtect employs robust data protection strategies in the form of regular backups. Employees backup all data on a central data repository on an ongoing basis. The Security Officer performs a weekly backup of the central repository on a storage drive which is then taken off-site and maintained at a safe contingency location. Full back-up recovery testing is performed on a regular basis to ensure that backups are fully restorable. These tests are performed in a test environment that is fully segregated from the production environment. In addition, ERMProtect infrastructural components are protected physically using surge protectors, uninterruptible power supply, multi-level electronic/manual locking, burglar alarms, and fire alarms/extinguishers.

In the event of a natural disaster, ERMProtect will relocate its operations to a safe alternate site. Upon receiving an alert for a natural disaster, ERMProtect management will initiate contingency procedures. The safety of ERMProtect personnel is given foremost importance. All personnel are contacted either physically (if on-site) or by phone to indicate the initiation of contingency procedures. ERMProtect then uses emergency evacuation procedures (if necessary) to evacuate the office premises. In the event that the threat is known in advance, the relocation to the alternate site is done well in advance. An emergency chain of command is followed at all times.

In the event that ERMProtect personnel cannot physically travel (owing to either pandemic or even natural disaster like situations), personnel will work from their home premises and maintain contact over the phone on a regular basis. In such situations, it is likely that clients will not be able to travel as well and hence any information needed shall be coordinated over electronic mediums (such as the Internet or telephonic means).

ERMProtect will transparently communicate and coordinate with all clients during a contingency situation. Collective and cooperative decisions shall be taken on all issues encountered during the course of the contingency.

ERMProtect is available to begin the project almost immediately upon your request. Our project management methods ensure that we keep good with our commitments as far as project milestones are concerned. We have proven past experience in working within client expected timelines and have exceeded client expectations as far as deadlines and project completion milestones are concerned. We also maintain a robust network and coalition with staffing firms and independent consultants who are carefully vetted by us. In the unlikely event that we need to tap into this talent pool, ERMProtect will do so to ensure that project delivery and related schedules are not adversely impacted at any time.

Security

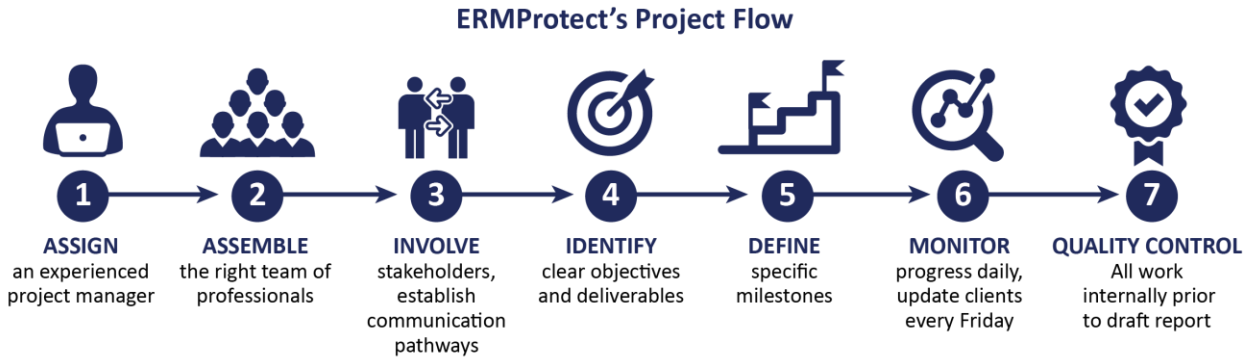
ERMProtect will apply strict security measures to all information provided by the client. All Information that can be evaluated internally at the client's locations will be performed on-site at the client and ERMProtect will return all documents (manual and electronic) to the client organization's staff. Final reports and supporting evidence that ERMProtect maintains will be stored in an encrypted format. Moreover, e-mails that contain sensitive information and attachments will be transferred in an encrypted manner.

ERMProtect has implemented robust logical and physical security measures at our site. All client reports and supporting evidence are stored in a secure server and separated by client. Only a limited number of ERMProtect authorized employees have access to the server and clients' resources. Client resources are encrypted while in storage and when they are transmitted to and from clients.

ERMProtect will also use a secure FTP (sFTP) server to exchange sensitive information with the client. The server employs robust security controls including intrusion detection protection, logging, monitoring, and alerting. The sFTP server undergoes ongoing information security testing and reviews to ensure that it complies with industry best practices and leading standards.

Project Flow

ERMProtect will reach out to key personnel and points of contact at the West Virginia Lottery to introduce our project manager. The project manager will then introduce the project team and provide information on the overall project flow.



ERMProtect's project manager will reach out to key client personnel to discuss the project scope, understand the project expectations, objectives, and goals as well as to confirm logistics arrangements, discuss and understand in detail the organization's risk tolerance and culture, and agree upon a communication strategy and plan with escalation channels and specific key individuals identified.

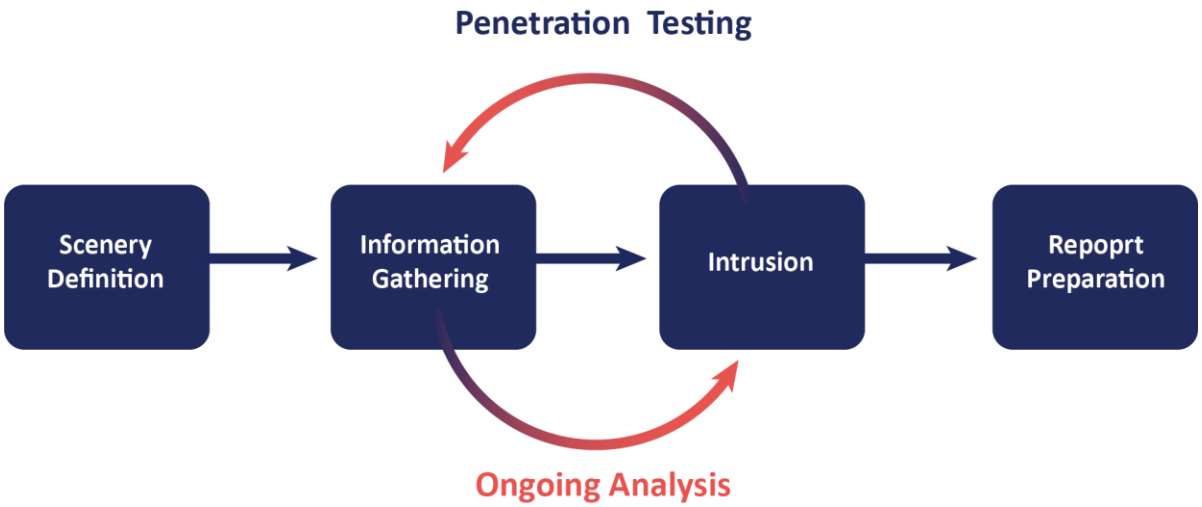
ERMProtect's project manager will then prepare a comprehensive project plan (Work Plan) that covers project timelines, schedules, key individuals involved, rules of engagement, methodology for testing systems, priority ranking of systems, safe/non-production testing time windows, tasks that will be performed as part of the project, listings of information requirements, and deliverables. ERMProtect will then seek West Virginia Lottery's review and approval of the project plan before proceeding forward.

When performing penetration testing tasks, ERMProtect will work closely with the organization's key

personnel to keep them constantly posted on any critical vulnerabilities identified and potential implications both in terms of the information asset risks it poses as well as the overall business and legal impact. For instance, if a potential or confirmed data breach is identified, ERMProtect will leverage its deep knowledge of regulatory compliance requirements to advise the organization on regulatory items such as data breach notifications, associated timelines, potential options, and so on. ERMProtect's advice, however, will be from a technical and regulatory compliance standpoint. ERMProtect is not a legal expert and does not offer legal advice. During penetration testing, any added network traffic resulting from the various scans and/or assessments will be roughly pre-determined to ensure that no unexpected network bandwidth congestion or denial of service results.

Detailed Technical Methodologies

The following sections of the proposal will delve into details of each phase of this project and the specific types of penetration tests/assessments that will be conducted therein. At a high-level though, our penetration testing methodology is depicted below:



After ERMProtect has completed all the phases of the project, we will perform:

- A comprehensive clean-up of all test-related aspects such as:
  - Removal of accounts created by ERMProtect as part of the assessment.
  - Removal of tools installed by the ERMProtect tester on client systems.
  - Confidential data about the client obtained as a result of the assessment will be identified and electronically shredded to the satisfaction of the client.
- Once testing is complete, ERMProtect will not store/retain any data obtained during the test/assessment.

1. External Network Vulnerability Assessment and Penetration Test

The goal of this phase is to perform an external network vulnerability assessment and penetration test. ERMProtect's technical methodology will be covered in detail in this section. Our methodology combines in key elements of significant testing methodologies and cybersecurity standards/frameworks such as the

Penetration Testing Execution Standard (PTES), NIST Cybersecurity Framework (CSF), Open-Source Security Testing Methodology Manual (OSSTMM), and Information System Security Assessment Framework (ISSAF), as well as Open Web Application Security Project (OWASP) for web-related testing.

As part of this phase of the project, ERMProtect will evaluate the efficiency and security of the network perimeter and firewall. The goal of this assessment is to determine if an outside attacker can gain access to the client's IT infrastructure assets remotely (over the internet) and whether the client's IT department can detect such activity. We will assess the overall network security including the network perimeter devices residing on network segments (DMZ) and the Internet for potential vulnerabilities that could expose critical organizational systems and applications; customer information; organization information, and financial assets. This assessment will be conducted combining the tools and techniques used by malicious "hackers" with disciplined scientific procedures to provide unique insight into the state of security in the information systems environment of the organization. The security assessment will provide the organization with a diagnosis of network vulnerabilities from an external perspective (from the Internet into the organization's internal network). Networked devices including firewalls, routers, switches, servers, printers, remote-access devices, mainframes, middleware, and backend services connected to the Internet will all be assessed.

The engagement will provide the organization with an overall external security assessment of the organization that addresses risk exposures noted during the evaluation. The results of this review will help strengthen the established security controls, standards, and procedures to prevent unauthorized access to the organizational systems, applications, and critical resources. As a result of our tests, we will prepare detailed work papers documenting the tests performed, a report of our findings including recommendations for external access security controls.

Rules of Engagement

The network penetration assessments will follow the following rules of engagement:

- No denial of service attacks will be used
- No un-trusted tools and techniques will be used
- No active backdoor or Trojans will be installed
- No sensitive data will be copied, modified or destroyed
- The specific tasks of the tests performed will be documented
- The operational impact to the networks will be maintained to the minimum

Scope

The following section summarizes the phases that will be executed during the engagement:

Phase 1: Footprinting - This is primarily an information gathering phase. The purpose of this phase is to gather information about the organization on public resources. During this phase, ERMProtect will create a complete profile of the organization's security environment. Information related to the organization's Internet, intranet, remote access, and extranet will be identified. During this phase ERMProtect will identify all relevant network targets, domain names, network blocks, and individual IP addresses of the entity's systems that are directly connected to the Internet. Every new finding in this phase will be used to identify more opportunities to exploit.

Phase 2: Enumeration and Network Reconnaissance (OSINT) - During this phase of the assessment, ERMProtect will gather more specific information about the organization's network topology, live hosts,

potential access paths into the networks, running services, access control mechanisms, any publicly viewable interactions between systems and infrastructure components, and the type of traffic that moves through the organization's networks. The main objective in this phase is to gather as much information as possible about the target networks and interconnected systems to start exploiting potential vulnerabilities. Specifically, during this phase, ERMProtect will perform DNS interrogation, NIC querying, and ICMP ping-swiping.

Phase 3: Network Scanning - Once ERMProtect completes gathering information about the organization's networks and related systems, ERMProtect will focus their attempts on specific servers at known IP addresses and specific openings on those servers such as unprotected shares and ports. During this phase, ERMProtect will conduct both generic and specific vulnerability testing and identify the specific operating systems and applications used by various hosts as well as services that can be exploited. These running services include, but are not limited to, HTTP, HTTPS, DNS, SMTP, remote access, SNMP, Telnet, SSH, FTP, sFTP, TFTP, and others. To accomplish this task, ERMProtect will use a variety of methods and tools to scan the networks and related hosts.

Phase 4: Risk and Vulnerability Assessment - During this phase, ERMProtect will consolidate, document, and analyze all the information gathered to develop an approach for focused attacks. At this stage, ERMProtect will also embark on the process of weeding out false positives by analyzing platform discrepancies, hacker return on investment and feasibility, potential vulnerabilities that have most likely been addressed in the latest patches, manual vulnerability identification and confirmation, etc. Specifically, once ERMProtect finishes analyzing all the information gathered during prior phases and potential vulnerabilities have been identified, we will determine the level of risks related to all the found vulnerabilities.

Phase 5: Exploitation - During this phase, ERMProtect will examine the documented vulnerabilities and potential security deficiencies on the various target hosts and determine which are more likely to be successful. Our penetration testing team manually exploits as many findings as are possible to exploit and documents them with artifacts/screenshots in what we call an “Exploitation Report”. This report essentially contains proofs of exploitation and in creating this report a lot of the false positives are identified by our testing team. This exploitation report is also one of our deliverables to you. Our experience tells us that manual testing outperforms automated testing and so a significant number of our tests are highly technical, specifically crafted, manual tests. Roughly, there is a 25-75 split in terms of percentage work performed automated versus manual (with 75% of the core testing work being manual). At this point, ERMProtect will start exploiting a select number of the found vulnerabilities starting with the one with the highest level of risk to the one with the lowest level of risk. During this phase, ERMProtect will load a set of different tools that will assist them in the process of compromising the targeted systems. As the tools are loaded into the hosts, ERMProtect will keep track of the tools loaded to ensure that organizational systems can be returned to their normal state prior to the testing. While penetration testing in the context of network security is, and has always been, a moving target to which cybersecurity experts and ethical hackers constantly adapt, the following tests/exploits will provide a high-level idea of what ERMProtect will look to exploit:

- Spoofing of IPs and other network/application level identifiers.
- Null or Default Passwords.
- Protocol vulnerabilities including IP options, fragmentation testing, exploitation of trust relationships, protocol encapsulation, misguided and misdirected routing, and man-in-the-middle attack testing.

- Configuration-level attacks and tests on servers hosting web applications.
- Obtaining escalated privileges in an unauthorized manner by leveraging existing vulnerabilities, leveraging the accesses currently available or obtained, stepping across user boundaries, URL-based manipulation, and/or creating a completely new (unauthorized) account with the desired privileges.
- Default shared keys.
- Eavesdropping.
- Service-specific vulnerabilities.
- Application-specific vulnerabilities and tampering such as SQL injection, Cross-Site Scripting, Parameter Pollution, XML misconfigurations, and so on.
- Repudiation-based manipulation/tampering and identity forging attacks, e.g. forcing wrong log data, manipulating authoring information of a specific user, causing misleading data references/inferences, and so on.
- Misconfigurations in firewalls, routers, switches, operating systems, security software, and other network infrastructure components.
- Broken authentication, security policy misdirection and authentication/access specific man-in-the-middle attacks.
- Information disclosure and data leakage/breach exploitation various potential methods including cookie spoofing, session hijacking, brute force attacks, backdoor initiation, and other potential vulnerabilities in key generation, protocol deployment, and/or database management.

Phase 6: Documentation of Findings, Presentation to Management and Final Report - ERMProtect will document the work using a detailed documentation methodology followed by standard industry practitioners. ERMProtect will provide the detailed vulnerabilities prioritized by risk exposure. Additionally, ERMProtect will prepare a formal report summarizing our findings and recommendations to enhance the security of the external and internal networks. Furthermore, the results of our findings will be summarized for the local management with a formal presentation. The section of this proposal titled "KEY DELIVERABLE: ERMProtect's Reports" describes in great detail the precise format and content of the reports that will be delivered.

Important Notes

- Our review of the areas mentioned above assumes that internal personnel will help with the coordination efforts. The help required, though, will be minimal.
- ERMProtect shall use various proprietary and in-house tools and scripts for the purpose of this project.
- ERMProtect fully understands that the organization require "near zero downtime". In this light, all tests shall be planned and scheduled to be conducted in night or early morning time windows to minimize the risk of downtime.
- All external scanning and testing will be done using ERMProtect facilities, hardware, software, and concerned resources. No additional facilities or resources need to be provided by the client.
- In addition to U.S. facilities, ERMProtect has facilities to perform scans and tests from outside the U.S. as well to enable more "realistic" attack scenarios.

2. Internal Network Vulnerability Assessment and Penetration Test

The goal of this phase is to perform an internal network vulnerability assessment and penetration test. ERMProtect's technical methodology will be covered in detail in this section. Our methodology combines

in key elements of significant testing methodologies and cybersecurity standards/frameworks such as the Penetration Testing Execution Standard (PTES), NIST Cybersecurity Framework (CSF), Open-Source Security Testing Methodology Manual (OSSTMM), and Information System Security Assessment Framework (ISSAF), as well as Open Web Application Security Project (OWASP) for web-related testing.

As required by the West Virginia Lottery, this will be a two-part testing to assess the security of all network assets, including servers, desktops, firewalls, network devices, and network monitoring and management. Note that wireless testing is covered as a separate test and a separate detailed methodology has been provided for it. In part one of testing, ERMProtect will simulate an attack by an untrusted outsider or unauthenticated user without the working knowledge of West Virginia Lottery's network. In part two of testing, ERMProtect will perform testing with low-level credentials of an authenticated user.

As part of this phase of the project, ERMProtect will evaluate the efficiency and security of the internal network and firewall from the perspective of someone who has access from the inside, such as an employee or contractor. The goal of this assessment is to determine if an internal attacker can escalate privileges to assets, applications or devices within any network and if detection can occur. We will assess the overall network security including the network perimeter devices residing on internal network segments for potential vulnerabilities that could expose critical organizational systems and applications; customer information; organization information, and financial assets. This assessment will be conducted combining the tools and techniques used by malicious "hackers" with disciplined scientific procedures to provide unique insight into the state of security in the information systems environment of the organization. The security assessment will provide the organization with a diagnosis of network vulnerabilities from an internal perspective (from the internal network to the Internet). The assessment will essentially look to cover every device/system that can connect to a network and obtain an IP address – networked devices including firewalls, routers, switches, servers, endpoints (desktops, laptops, mobile devices, printers), VoIP equipment, security cameras, remote-access devices, cloud accesses and directory services, third party connections, WAN/MAN connections, mainframes, middleware, and backend services connected to the Internet will all be assessed.

The engagement will provide the organization with an overall internal security assessment of the organization that addresses risk exposures noted during the evaluation. The results of this review will help strengthen the established security controls, standards, and procedures to prevent unauthorized access to the organizational systems, applications, and critical resources. As a result of our tests, we will prepare detailed work papers documenting the tests performed, a report of our findings including recommendations for external access security controls.

Rules of Engagement

The network penetration assessments will follow the following rules of engagement:

- No denial of service attacks will be used
- No un-trusted tools and techniques will be used
- No active backdoor or Trojans will be installed
- No sensitive data will be copied, modified or destroyed
- The specific tasks of the tests performed will be documented
- The operational impact to the networks will be maintained to the minimum

Scope

The following section summarizes the phases that will be executed during the engagement:

Phase 1: Footprinting - This is primarily an information gathering phase. The purpose of this phase is to gather information about the organization on freely accessible resources (including public resources). During this phase, ERMProtect will create a complete profile of the organization's security environment. Information related to the organization's Internet, intranet, remote access, and extranet will be identified. During this phase ERMProtect will identify all relevant network targets, domain names, network blocks, and individual IP addresses of the entity's systems that are directly connected to the Internet. Every new finding in this phase will be used to identify more opportunities to exploit.

Phase 2: Enumeration and Network Reconnaissance - During this phase of the assessment, ERMProtect will gather more specific information about the organization's network topology, live hosts, potential access paths into the networks, running services, access control mechanisms, any publicly viewable interactions between systems and infrastructure components, and the type of traffic that moves through the organization's networks. The main objective in this phase is to gather as much information as possible about the target networks and interconnected systems to start exploiting potential vulnerabilities. Specifically, during this phase, ERMProtect will perform DNS interrogation, NIC querying, and ICMP ping-swiping.

Phase 3: Network Scanning - Once ERMProtect completes gathering information about the organization's networks and related systems, ERMProtect will focus their attempts on specific servers at known IP addresses and specific openings on those servers such as unprotected shares and ports. During this phase, ERMProtect will conduct both generic and specific vulnerability testing and identify the specific operating systems and applications used by various hosts as well as services that can be exploited. These running services include, but are not limited to, HTTP, HTTPS, SMB, ARP, DNS, SMTP, printsharing, remote access, SNMP, Telnet, SSH, FTP, sFTP, TFTP, and others. To accomplish this task, ERMProtect will use a variety of methods and tools to scan the networks and related hosts.

Phase 4: Risk and Vulnerability Assessment - During this phase, ERMProtect will consolidate, document, and analyze all the information gathered to develop an approach for focused attacks. At this stage, ERMProtect will also embark on the process of weeding out false positives by analyzing platform discrepancies, hacker return on investment and feasibility, potential vulnerabilities that have most likely been addressed in the latest patches, manual vulnerability identification and confirmation, etc. Specifically, once ERMProtect finishes analyzing all the information gathered during prior phases and potential vulnerabilities have been identified, we will determine the level of risks related to all the found vulnerabilities.

Phase 5: Exploitation - During this phase, ERMProtect will examine the documented vulnerabilities and potential security deficiencies on the various target hosts and determine which are more likely to be successful. Our penetration testing team manually exploits as many findings as are possible to exploit and documents them with artifacts/screenshots in what we call an "Exploitation Report". This report essentially contains proofs of exploitation and in creating this report a lot of the false positives are identified by our testing team. This exploitation report is also one of our deliverables to you. Our experience tells us that manual testing outperforms automated testing and so a significant number of our tests are highly technical, specifically crafted, manual tests. Roughly, there is a 25-75 split in terms of percentage work performed automated versus manual (with 75% of the core testing work being manual). At this point, ERMProtect will start exploiting a select number of the found vulnerabilities starting with the one with the highest level of risk to the one with the lowest level of risk. During this phase, ERMProtect

will load a set of different tools that will assist them in the process of compromising the targeted systems. As the tools are loaded into the hosts, ERMProtect will keep track of the tools loaded to ensure that organizational systems can be returned to their normal state prior to the testing. While penetration testing in the context of network security is, and has always been, a moving target to which cybersecurity experts and ethical hackers constantly adapt, the following tests/exploits will provide a high-level idea of what ERMProtect will look to exploit:

- Spoofing of IPs and other network/application level identifiers.
- Null or Default Passwords.
- Weak passwords targeted with the help of bruteforce and dictionary attacks as well as identification of poor password policy implementation covering reused passwords, expired passwords, and so on.
- Configuration-level attacks and tests on servers hosting web applications.
- Poorly/inadequately configured settings that could promote social engineering link-based attacks such as phishing.
- Protocol vulnerabilities including IP options, fragmentation testing, exploitation of trust relationships, protocol encapsulation, misguided and misdirected routing, and man-in-the-middle attack testing.
- Obtaining escalated privileges in an unauthorized manner by leveraging existing vulnerabilities, leveraging the accesses currently available or obtained, stepping across user boundaries, URL-based manipulation, and/or creating a completely new (unauthorized) account with the desired privileges.
- Default shared keys.
- Eavesdropping.
- Service-specific vulnerabilities.
- Application-specific vulnerabilities such as SQL injection, Cross-Site Scripting, Parameter Pollution, XML misconfigurations, and so on.
- Repudiation-based manipulation/tampering and identity forging attacks, e.g. forcing wrong log data, manipulating authoring information of a specific user, causing misleading data references/inferences, and so on.
- Misconfigurations in firewalls, routers, switches, operating systems, security software, and other network infrastructure components.
- Broken authentication, security policy misdirection and authentication/access specific man-in-the-middle attacks.
- Information disclosure and data leakage/breach exploitation various potential methods including cookie spoofing, session hijacking, brute force attacks, backdoor initiation, and other potential vulnerabilities in key generation, protocol deployment, and/or database management.
- Overall data security control weakness exploitation specifically targeting compliance-critical data such as PII, PHI, ePHI, and other data relevant to compliance with regulations/standards such as CJIS, HIPAA, PCI DSS, etc.
- Exploit and test the effectiveness of SIEM controls deployed.

Phase 6: Documentation of Findings, Presentation to Management and Final Report - ERMProtect will document the work using a detailed documentation methodology followed by standard industry practitioners. ERMProtect will provide the detailed vulnerabilities prioritized by risk exposure. Additionally, ERMProtect will prepare a formal report summarizing our findings and recommendations to enhance the security of the external and internal networks. Furthermore, the results of our findings will be summarized for the local management with a formal presentation. The section of this proposal titled

"KEY DELIVERABLE: ERMProtect's Reports" describes in great detail the precise format and content of the reports that will be delivered.

Important Notes

- Our review of the areas mentioned above assumes that internal personnel will help with the coordination efforts. The help required, though, will be minimal.
- ERMProtect shall use various proprietary and in-house tools and scripts for the purpose of this project.
- ERMProtect fully understands that the organization require "near zero downtime". In this light, all tests shall be planned and scheduled to be conducted in night or early morning time windows to minimize the risk of downtime.
- For internal testing, ERMProtect professionals will require the organization to help connect a virtual scanner appliance internally in a way that the appliance can obtain an internal IP address with access to the scope IPs and segments. The client will be expected to provide minor assistance in terms of guiding where such connection points are located. Additionally, in the case of remote testing, VPN access will need to be facilitated with access to the internal scope IPs and segments.

3. Web Application Penetration Test

ERMProtect's application penetration testing methodology is directly based on OWASP. ERMProtect will gather and analyze general information related to the web application to obtain a deep understanding of the scope and functionality of the application. The following areas will then be assessed based on this understanding and knowledge of the target:

Authentication: ERMProtect will evaluate the adequacy of the application's authentication control mechanism as it processes the identity of individuals or entities. Among the tests that will be conducted during this phase are:

- Find possible brute force password guessing access points in the application.
- Find valid login credentials with password grinding.
- Bypass authentication system with replay authentication information.
- Determine the application logic to maintain the authentication.
- Verification testing to confirm the digital identity of a communication sender and attempts to subvert/side-step such confirmatory checks.
- Attacks and tests directed at the authorization process once a user is authenticated.
- Attempt to gain unauthorized access without proper credentials by leveraging/masquerading as legitimate users in the application and/or non-existent users and further attempt to gain access to user data using browser and framework-based exploits.
- Attempt to gain unauthorized access via the front-end such that data of legitimate users can be stolen and/or modified.
- Attempt to gain unauthorized access via the front-end and bulk extract legitimate user data from the backend database.
- Attempt to masquerade a malicious internal user and try to steal data of other users by leveraging application layer vulnerabilities.

Session Management: ERMProtect will evaluate the adequacy of the application's session management control mechanism as it traces the activities performed by authenticated application users. Among the tests that will be conducted during this phase are:

- Identify the possibility to establish concurrent sessions from different computers.
- Determine if the session ID is maintained with IP address information.
- Replay gathered information to fool the application from different computers.
- Identify is appropriate session timeouts are in place.
- Attacks and tests directed at user roles, including privilege escalation attacks between roles, and verifying levels of access and authorizations.
- Attacks and tests directed at the user registration/enrolment process and pages to check the possibility of registering a fake/malicious account.
- Deep-dive testing and attacks related to controls that confine and create boundaries around interactions between users and software applications with active attempts to bypass such control mechanisms.

Input Manipulation: ERMProtect will evaluate the adequacy of the application's input controls as the application processes inputs received from different interfaces and\or entry points. Among the tests that will be conducted during this phase are:

- Testing, fiddling, and fuzzing of all inputs that are possible to the web server and application from the client-side and the client environment.
- Use exceptionally long character-strings to find buffer overflow vulnerabilities.
- Concatenate commands in the input strings of the application.
- Inject SQL language in the input strings of database-tired web application – will involve manual attack methods wherein injection technique will be adapted based on the target database in question.
- Examine "Cross-Site Scripting" in the web application of the system – will involve manual attack methods wherein all parameters both direct (e.g. form-based fields) as well as indirect (e.g. target, destination, etc.) will be attacked.
- Perform code execution attacks on the client-side as well as the server-side.
- Use specific URL-encoded strings to bypass input validation mechanisms.
- Examine unauthorized directory/file access with path/directory.
- Manipulate cookies to modify the logic in the server-side web application. Additionally test the business logic of the application by forcing errors and race conditions.
- Use illogical/illegal input to test the application error-handling routines and force the application to reveal additional/sensitive information via errors, error codes, and/or stack trace leakages.

Output Manipulation: The purpose of this is to determine if it is possible to get information from the temporary Internet files, cookies and other application objects. Among the tests that will be conducted during this phase are:

- Retrieve valuable information stored in cookies or temp files.
- Retrieve valuable information from the client application cache.
- Retrieve valuable information stored in the temporary files and objects.

Information Leakage: The purpose of this area is to determine the type of information that is transferred back to the user or stored in the client's machine. Among the tests that will be conducted during this phase are:

- Find useful information in hidden field variables (e.g. viewstate), temp files and comments.
- Examine the information contained in the application banners.
- Examine contents of headers of automated e-mails generated by the application to see if internal IP address information is being leaked.

- Intercept and/or steal data during rest and transit over networks connected to the application.

Other Tests: ERMProtect will assess the application based on other attacks, tampering methods, and manipulations commonly used by hackers. Among the tests that will be conducted during this phase are:

- Identify if the cookies used by the application are appropriately protected (i.e. marked secure, HTTPOnly, etc.).
- Identify if appropriate encryption is being used by the application with tests involving the robustness and adequacy of the ciphers employed by the application.
- Identify if auto-email features in the application can be used as a potential spam gateway.
- Identify if valid user IDs can be ascertained based on the behavior of the application and the kind of error messages and exceptions it generates (e.g. the "Forgot Password" link can sometimes be misused as a function to identify if a user ID is valid based on the error message it generates).
- Identify if employed encryption is validly deployed throughout the application and if there is a possibility for unencrypted versions of the internal pages to be forced out.
- Identify if auto-generated e-mails containing any sort of application-specific information are being sent in cleartext.
- Identify if another user's account can be hijacked from another valid user account and force the application to display the other user's account information and details.
- Identify and assess the auto-complete feature in all significant application parameters.
- Identify if logged-in user privileges can be escalated by tricking the application.
- Web server configuration manipulation, fiddling, and misdirection in order to identify if secure configurations are able to protect the web server adequately.

4. Wireless Network Penetration Test

ERMProtect will evaluate the security of the key wireless networks at the organization using a series of 802.1X exploits. ERMProtect's wireless hacking and audit team shall perform a comprehensive wireless network assessment and penetration testing, attempting to:

- Identify all access points on the network using manual and automated tools to include information such as the MAC address, SSID, Channel, Vendor, Name, and Location (using a GPS or approximately locating the access point(s) on the physical map).
- Pinpointing valid and rogue access points with the help of the organization's documentation of valid access points.
- Attempt user access and access privilege escalation where possible.
- Ensure that all access points use adequate and appropriate frequencies so as to minimize interferences with other access points and other known frequencies.
- Ensure that default settings and parameters are not used in any access points, including default SSIDs.
- Ensure that wireless access points use strong levels of encryption for any sensitive data or internal (non-guest) networks.
- Ensure that wireless access points use strong administrator passwords.
- Ensure that these passwords are changed on a periodic basis and that the password usage, change, and storage policies and practices are adequate and appropriate.
- Ensure that usernames and passwords transmitted for administrative access are encrypted appropriately and free from unauthorized access or malicious use.
- Ensure that logging is appropriately enabled to include all successful and failed administrator access attempts, and that these logs have an appropriate and adequate retention policy.

- Ensure that administrative credentials are not shared to access wireless networks and access points.
- Ensure that a centralized authentication protocol is appropriately in place so that administrators need to authenticate to the access point via this protocol.
- Ensure that logging is appropriately enabled to include all changed made to wireless access point configurations, and that these logs have an appropriate and adequate retention policy.
- Determine if a centralized management technology is instated for better security.

ERMProtect will further evaluate the adequacy of the security controls surrounding the wireless infrastructure. The technical review will address the following critical issues related to the deployment of secure wireless access points:

- Access Point Location
- Network Design
- Access Point Configuration
- Authentication Controls
- Encryption Controls
- VPN Implementations
- Wireless Routing
- Client Configuration
- Administrative Controls
- Logging and Monitoring Controls

The assessment will involve ERMProtect professionals attempting to hack into the wireless networks using wardriving and other such wireless hacking techniques. Manual as well as automated tools shall be used during this section of the engagement. The section of this proposal titled “KEY DELIVERABLE: ERMProtect’s Reports” describes in great detail the precise format and content of the reports that will be delivered.

5. Social Engineering Assessment

ERMProtect will conduct a targeted social engineering assessment as a baseline test to fully understand the level of security awareness at the organization.

During this assessment, ERMProtect professionals with the approval of the client will use non-technical social engineering techniques to obtain physical access and escalate privileges in the technical environment. ERMProtect shall use Social Engineering methods to coerce or dupe Help Desk, network/system administrators, and other personnel as ERMProtect deems appropriate.

Social Engineering assessments use coercion and manipulation via a variety of attack scenarios. One or more of the following attack scenarios may be used. The precise assessment and scenario(s) will be determined jointly upon discussions with the client organization.

For this assessment ERMProtect will send emails to the organization’s employees trying to get the employees to reveal sensitive information.

ERMProtect has developed our own Phishing assessment tool, Stingray. This tool is developed, maintained, and upgraded by ERMProtect. Stingray allows for fast, flexible, and data-driven phishing campaigns.

Stingray phishing campaigns happen in two phases. First, targets are sent the initial phishing email. This email can be customized to any scenario. Including changing the sender's name, sender's email address, the subject, and the content of the email. The email will also include a link to a webpage leading to the phishing attack's second phase. After the initial email is sent, Stingray will record which users open the email.

In the second phase of the phishing attack, users are brought to a fake webpage asking for sensitive information. Again, this is highly customizable, allowing ERMProtect and the organization to determine the web page's content, the sensitive information requested, and flexibility with the webpage's domain. Stingray will record which users click on the link to the webpage. Likewise, Stingray will register which users filled out the form on the webpage. Users who submit the form can be brought directly to the training material.

An advantage to this tool is that it provides a graphical representation of all the statistics and details of how the users interact with phishing emails. This would help detect gaps in understanding amongst the users and can be used as motivation for the next security awareness training.

Since Stingray allows for a high level of flexibility, ERMProtect will work with the organization to determine a scenario that works best for its goals.

Scenario 1: Fake Employee (Email)
In this scenario, the attacker sends an email to a generic email address of the organization and pretends to be a member of the organization who forgot the password for accessing a secure online system or requests additional information that is sensitive in nature. The attacker requests personal information or the password to be reset and sent back to him in the reply.

Scenario 2: Employee Seminar
In this scenario, the attacker sends an email to all employees inviting them to attend a free stress management seminar sponsored by the organization. In the email, the attacker will encourage employees to sign up for the seminar by replying to the email and providing personal information such as names, department names, job titles, home addresses, telephone numbers, social security numbers, etc.

Scenario 3: Spear Phishing
In this scenario, the attacker sends an email to all organizational employees/users using a valid internal email address. The email invites employees to participate in a survey where management asks for their opinion about the organization's culture and treatment of employees. To answer the survey, the employees must click on a web link that leads them to a false website that the attacker had prepared. Then, employees are required to enter their user ID, password, and other information to complete the survey. In addition to this sample survey scenario, there are several other scenarios that ERMProtect crafts for clients in a customized manner. Some examples of these include:

- Work from-home survey purportedly from the Department of Health.
- Fake Windows updates with a sense of urgency.
- Fake Glassdoor review email where the target is lured with a gift certificate as bait.
- Fake data breach investigation where the target is told that their machine has caused a data breach.

Scenario 4: Customized Scenario
The above scenarios are only representative samples to provide you with an idea of the various possibilities that we can implement as part of phishing scenarios. The exact scenario can be discussed with you at length and then implemented accordingly. Our consultants would sit down with appropriate personnel to discuss specific needs of the Lottery department and customize a unique scenario tailored to your needs.

The results of ERMProtect's tests and reviews will be summarized for management in a formal report and presentation.

Deliverables

KEY DELIVERABLE - ERMProtect's Reports
For each of the areas identified above, ERMProtect's project team will document all project findings in a final report. This report will provide visibility into specific weaknesses and deficiencies in the security controls employed or inherited by the technical infrastructure and/or assessment area in scope. The report will make comprehensive recommendations on each finding along with precise instructions and action items on how findings can be best remediated.

Before finalizing a report, ERMProtect will meet with key client personnel to discuss a draft version of the report. System managers and key technical client staff will then have the opportunity to review and discuss information gathered, findings, and/or recommendations in order to avoid any misunderstanding in identified report items. ERMProtect will obtain and incorporate all draft report feedback to then document the final reports. All final reports will be provided to the client in both physical and electronic forms. The electronic form can be made available in a specific format the client wishes (e.g. spreadsheet of findings, editable document, etc.).

The final report shall be divided into various sections. Each section is described below:
Executive Summary

- **Executive Summary:** An executive-level summary free of jargon and buzz-words directed at senior management. It will cover the objective, scope, approach, overall assessment results, and risk/severity levels.
- **Summary of Findings and Recommendations:** ERMProtect will describe the environment and high-level findings and root causes and make recommendations based on risk to the client. For scans/penetration tests, in as non-technical manner as possible, ERMProtect will also provide a summary of exploited vulnerabilities, discovered hosts, and list the most exploited vulnerabilities (both overall and by operating system). All sensitive information (such as PII, SSN, PHI, etc.) that could be found during the assessment will be identified, annotated, and specific artefacts/evidences related to these will be provided as appendices (as applicable).

Technical Matrix
This report can be considered a detailed findings matrix targeted to technical staff that will provide more granular detail:

- **Summary:** ERMProtect will provide details specific to the engagement methodology as well as positive security aspects identified. It will also include the number of compromised hosts

identified, the services and applications identified on each host, and the average number of exploited vulnerabilities on these hosts.

- **Detailed Findings and Recommendations:** ERMProtect will document the details of all findings, as well as detailed recommendations for remediation per finding/system and include evidence of controls and information sufficient to replicate the findings. ERMProtect will base recommendations on these root causes and prioritize for a risk-based remediation with an estimation of relative work effort. In cases where a specific vulnerability cannot be confirmed, ERMProtect will still include the finding in the reports with a note indicating the same.

  For scans/penetration tests, ERMProtect will also provide vulnerability categories, risk ratings, CVE and other industry reference details such as Bugtraq ID, Microsoft advisory ID, Remote Code Execution Industry standard vulnerability identifier, information disclosure configuration, IP address of targeted host along with any operating system information identified, information on each device tested along with a profile per device, security risks identified and their potential impacts on systems, as well as a summary risk score on CVSS2/3 baselines. For all systems that ERMProtect was able to compromise, we will provide detailed instructions on how to uninstall any agents installed from our end in compromised systems. All findings will also be provided as a sortable Excel spreadsheet.

- **Artifacts:** ERMProtect will provide details and specific examples, including screenshots, technical details, code excerpts and other relevant observations and also provide documents or data that are relevant but do not fit in other categories. All potential “flags”/”trophies” (e.g. passwords, SSNs, PII, etc.) will be redacted. These will be included in ERMProtect’s exploitation report or as an appendix to the same report (as applicable).

KEY DELIVERABLE: Findings Presentation

ERMProtect will not only deliver the reports, but will also present findings and allocate up to four hours for transfer of knowledge to the personnel al the West Virginia Lottery to help them improve the security controls and in turn the security posture of the entity.

ERMProtect will facilitate and deliver a formal findings presentation to:

- Key Organizational Personnel
- Senior/Top Management

The presentation will summarize the results of each phase of the project, research, evaluation, findings, risk assessment, remediation strategies, and recommendations for remediation and improvement. ERMProtect will cover the full methodology followed during the project as well as advise the organization on how to use the deliverables that ERMProtect will be handing over. This presentation will also serve as an opportunity for the client organization to ask questions. In addition, ERMProtect’s team members will always be available both during the project as well as after the project to answer any questions that may arise at any time.

PROJECT LEVEL DELIVERABLE: Meetings, Coordination, and Updates

As part of the project management level deliverables for this project, ERMProtect will conduct weekly/biweekly status meetings with key stakeholders at the client organization and:

1. Introduce key project team members and define roles and responsibilities

2. Review timelines, meetings, and additional requirements
3. Schedule status meeting and other recurring touchpoints, as required
4. Review engagement progress
5. Identify engagement risks
6. Identify upcoming tasks
7. Request any additional involvement from stakeholders
8. Escalate issues or roadblocks to successful project completion

As a result, ERMProtect will provide the client organization with weekly status update reports highlighting key task area actions, owners, estimated completion dates/times, and overall project status delivered after each meeting.

PROJECT LEVEL DELIVERABLE: Knowledge Transfer Session and Value-Added Services
Besides delivering the abovementioned reports/deliverables, ERMProtect will provide a session of up to four (4) hours for the transfer of knowledge and training to West Virginia Lottery personnel.

We also offer the West Virginia Lottery the following value-added service:

- ✓ One month of free access to ERMProtect Security Awareness Training platform (19 cybersecurity training modules in both English and Spanish).

Pricing Page

Please find the completed Pricing Page below. As per instructions and clarifications in Addendum No. 1, we understand the pricing page uses an estimated consumption of two (2) assessment of each of the four (4) types per year. Also, we understand that each assessment involves eight (8) sites.

The pricing presented below assumes that we will be allowed to perform testing on all eight (8) locations together in one go as part of each assessment.

In summary, the total price presented represents the cost of:

- ✓ Two (2) full assessments of each or the four (4) types per year.
- ✓ Each of the yearly assessments will encompass eight (8) locations.
- ✓ Testing for each assessment will be performed in “one-go”

EXHIBIT A - Pricing Page

Item #	Section	Description of Service	*Estimated Number of Assesments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	$ 1,485 -	$ 11,880 -
2	4.2	Website Penetration Testing	8	$ 895 -	$ 7,160 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	$ 3,191.25 -	$ 25,530 -
4	4.4	Wireless Penetration Testing	8	$ 3,985 -	$ 31,880 -
				TOTAL BID AMOUNT	$ 76,450 -

Please note the following information is being captured for auditing purposes and is an estimate for evaluation only

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

Any product or service not on the Agency provided Pricing Page will not be allowable.

The state cannot accept alternate pricing pages, failure to use Exhibit A Pricing Page could lead to disqualification of vendors bid.

Vendor Name:	Enterprise Risk Management, Inc. (dba ERMProtect)
Vendor Address:	800 S Douglas Rd. Suite 940 N, Coral Gables, FL 33134
Email Address:	sgonzalez@ermprotect.com
Phone Number:	305-447-6750 / 305-335-7610
Fax Number:	305 447 6752
Signature and Date:	March 27, 2024

ERMProtect
Cybersecurity Solutions

Appendix: ERMProtect Team Resumes

Please see resumes starting on the next page.

ESTEBAN FARAO

Director, IT Consulting Services

efarao@ermprotect.com
305-447-6750

EDUCATION

Bachelor's degree in Information Systems, Universidad be Belgrano.

Master's degree in Management Information Systems, Universidad de Salvador

Master's degree in International Business, Florida International University

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Chief Information Security Officer (C | CISO)
- Certified Ethical Hacker (CEH)
- Payment Card Industry Professional (PCIP)
- PCI-Qualified Security Assessor (PCI-QSA)
- EnCase Certified Examiner (EnCe)
- Certified Network Defense Architect (CNDA).
- Certified Data Privacy Solutions Engineer (CDPSE)
- PCI Forensic Investigator (PFI)

ERMProtect
Cybersecurity Solutions

Summary

Esteban Farao is a Director of IT Consulting Services. He performs computer forensics and incident response during major security breaches. As an expert certified ethical hacker, he knows the routes malicious actors use to penetrate organizations and puts this knowledge to use to protect clients. His deep knowledge of computer forensics has helped him break open major cases related to fraud, embezzlement, IP theft and other misdeeds. He is also an expert in assisting organizations to prepare, plan and respond to data breaches.

Experience

With two master's degrees and 25+ years in information security, Esteban has led >10k projects related to general data breaches, PCI DSS-related data breaches and investigative forensics. He has served as the court-appointed "neutral" in disputes, testified in both U.S. and Latin American courts, and provided evidence to the United States Secret Service and other enforcement agencies. He has performed thousands of gap assessments for clients related to data compliance, including for PCI DSS, GLBA, SEC, NIST, FISM, HIPAA, HITECH, etc.

Prior to joining ERMProtect, Esteban led attack and penetration testing assignments for PwC in London and set up and managed the company's IT security practice in Argentina. He holds 11 high-level IT Security certifications.

Case Highlights

- **Security Training and Table-Top Exercises –** Prepared and delivered table-top exercise training for institutions such as Helm Bank USA and the State of Kansas, Office of the Bank Commissioner.
- **Digital Forensics -** Extracted information from various mobile phones to provide evidence for a large sports investigation case related to use of illegal substances.
- **Law Firm Support –** Extracted information from various servers, computers, mobile devices, and mobile phones to provide evidence that executives committed corporate fraud.
- **Data Breach –** Determined that a bank employee copied a database to run a large identity theft operation.
- **PCI Data Breach –** As PCI PFI, investigated multiple large breaches of credit card data affecting all major payment cards brands and retailers processing from $1.5M-$17M monthly.
- **Forensic Investigation –** Determined who processed $2 million dollars of unauthorized wire transfer transactions via an on-line banking system by installing a malicious program in the administrator's machine.

AKASH DESAI

Director, Information Security Consulting Services

adesai@ermprotect.com
305-447-6750

EDUCATION

Master's degree in Information Networking with a Cybersecurity specialization from Carnegie Mellon University

Bachelor's degree in Computer Science from Sardar Patel University

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Ethical Hacker (CEH)
- PCI Qualified Security Assessor (PCI-QSA)
- Payment Card Industry Professional (PCIP)

ERMProtect
Cybersecurity Solutions

Summary

Akash Desai is a Director of Information Security Consulting Services for ERMProtect. For more than 20 years, he has combined technical expertise with creativity and problem-solving acumen to create solutions that address challenging cybersecurity problems. He leads penetration tests, comprehensive security assessments, gap analyses, and incident response tests and reviews to identify and fix vulnerabilities. To address human vulnerabilities, he developed ERMProtect's security awareness training practice which offers off-the-shelf and customized training for employees using animations, games, mini lectures, etc. His customized training for large federal agencies helped improve security of the military supply chain and of U.S. immigration and citizenship records worldwide and at U.S. embassies. Prior to joining ERMProtect, Akash worked for two years with the Computer Emergency Response Team Coordination Center (CERT®/CC) where he evaluated security attacks on U.S. private enterprise and provided solutions to prevent them.

Relevant Experience

- **Security Awareness Training –** Mr. Desai is the brain behind ERMProtect's security awareness training. He developed scripts for a 75+ library of animations, games, videos, and mini-videos available on our LMS or in SCROM-compliant modules. He has developed highly customized training for:
  - **NAVAIR** – Personnel involved in the supply chain to enable them to securely purchase weaponry, jets, ships, vehicles, and critical parts to supply the U.S. military.
  - **USCIS** – Personnel with access to sensitive citizenship and immigration data of the U.S. government and embassies.
  - **The Gap** – Employees of a global retail company to help protect the company's infrastructure systems and data.
  - **Penn State University** – 100,000 users to teach them to spot attacks and adhere to information security policies.
  - **Norwegian Cruise Lines** – Employees to protect data on and offshore and to ensure compliance with regulations.

- **Penetration Testing –** Developed and led penetration testing in complex environments, followed by remediation. For banks, compromised accounts, wire transfer systems, and physical cameras. *Sample clients: Telecommunications giant, many banks, large hospital, global insurance company, states of New Hampshire and West Virginia.*

- **Security Incident Response & Data Breach** – Developed, tested, and improved security incident response plans for many clients. Helped a City ward off a developing cybersecurity incident that involved a takeover of servers, workstations, devices, and key systems to mine bitcoin.

POOJA KOTIAN

Manager, Information Security Consulting Services

pkotian@ermprotect.com
305-447-6750

EDUCATION

Bachelor's degree in Engineering, Information Technology - Sardar Patel University

CERTIFICATIONS

- Infosys Quality Foundation (Internal to Infosys)
- Dotnet Technology 101 (Internal to Infosys)
- STAR Certification (Internal to Infosys)

ERMProtect
Cybersecurity Solutions

Summary

Pooja Kotian is a Senior Information Security Consultant at ERMProtect. She has more than 12 years of experience as a Senior Systems Engineer and as an Information Security Consultant overseeing penetration testing and vulnerability assessments, performing regulatory compliance assessments, reviewing policies and procedures related to IT security, and developing comprehensive security training content. She began her career as a Systems Engineer for Infosys before joining ERMProtect in 2015. She is highly experienced at conducting penetration tests of various kinds of web applications, internal and external networks, mobile applications, and social engineering. She performs vulnerability assessments on systems, applications, and infrastructures to identify, classify and prioritize vulnerabilities. She performs audits to ensure adherence to best practices and applicable laws, standards, and regulations.

Relevant Experience

- **Penetration Testing –** Found difficult-to-identify vulnerabilities in web applications, mobile applications, APIs, and network infrastructures. *Sample Clients: Assurant Solutions, State of New Hampshire, Safra National Bank of New York, City of Boynton Beach, and Metropolitan Washington Airport Authority.*
- **Vulnerability Assessments:** Identified highly technical security weaknesses with the help of scans, manual tests, as well as deep-dive source code reviews. Provided detailed remediation recommendations to clients and helped follow-through efforts. *Sample Clients: Segpay, Banco do Brasil, City of Coral Gables, CSID – Experian, and City of Lake Worth Beach.*
- **Security Assessments –** Performed comprehensive security assessments that helped clients comply with various regulations and regulatory requirements including PCI DSS, GLBA, FACTA, GDPR, FedRAMP, FISMA, ISO 27001, FFIEC, etc. *Sample Clients: itelBPO, Outplex, Helm Bank, Bancredito, SlimCD.*
- **Security Training –** Developed innovative information security training content used to train client employees on a vast array of cybersecurity awareness topics. *Sample Clients: CentralReach, Bancredito, Axiomatic, Banco de Credito del Peru, and Norwegian Cruise Line.*
- **Social Engineering –** Performed several social engineering assessments including phishing, spear phishing, impersonation, etc. to help clients test the cybersecurity awareness levels of their employees. Provided recommendations for improvement. *Sample Clients: Baer's Furniture, Safrapay, Welligent, and City of Lake Worth Beach.*

DIVYANSH ARORA

Manager, Information Security Consulting Services

darora@ermprotect.com
412-708-6331

EDUCATION

Bachelor's degree in Technology, Computer and Communication, Manipal Institute of Technology

Master's degree in Information Technology – Information Security, Carnegie Mellon University

CERTIFICATIONS

- Offensive Security Certified Professional

AWARDS

- EPT Leaderboard – 20+ machines vs. 5 teams
- CMU Academic Scholarship, 2019
- 2You Rock – Awarded for organizing PwC One Cyber Bootcamp, 2018

ERMProtect
Cybersecurity Solutions

Summary

Divyansh Arora is a Consultant, Information Security Services for ERMProtect. Prior to receiving his master's degree in Information Technology at the prestigious Carnegie Mellon University, Divyansh worked as a Senior Cybersecurity Analyst at PricewaterhouseCoopers. At PwC, he conducted hundreds of vulnerability assessments of web applications, IPs in the network, Android & iOS mobile applications and IoT devices such as CCTV and Central Command displays, for multiple government and private clients. He also assessed various phases in the SDLC and performed static and dynamic source code reviews. Subsequently, while working on his master's degree, he worked as an intern at McKinsey & Company, researching cloud security. After graduating with a 3.79 GPA, he joined ERMProtect to provide a wide variety of IT security services.

Relevant Experience

- **Vulnerability Assessment & Penetration Testing –** Conducted vulnerability assessment and penetration testing of 100+ web applications, millions of IPs in the network, over 20 Android & iOS mobile applications and IoT devices such as Spy Cameras, Baby Monitors, CCTV, Central Command Displays, for multiple government and private clients to ensure the security of critical infrastructure from various threat actors. Discovered possibility of fraud payments in payment gateway applications and prevented significant monetary losses to the client.

- **Security Awareness Training –** Delivered social engineering attack prevention training to 1500+ employees of the client by executing official phishing campaign, achieving a 65% success rate by developing a fake website to obtain sensitive information.

- **Secure Code Review –** Performed static and dynamic secure code review of various web, desktop and mobile applications developed in multiple languages, using a number of tools such as AppScan, Fortify, Coverity.

- **Built Cloud-Native SIEM tool –** Built a Scalable Cloud-Native SIEM (Security Information & Event Management) System based on AWS to help collect and aggregate logs, detect incidents, and respond to security threats.

- **Security Training and Table-Top Exercises –** Participated in preparing and delivering table-top exercise training for institutions such as Helm Bank USA and the State of Kansas, Office of the Bank Commissioner.

COLLIN CONNORS

Consultant, Information Security Consulting Services

cconnors@ermprotect.com
305-447-6750

EDUCATION

Bachelor's degree in Mathematics and Computer Science, University of Miami

Ph.D. in Computer Science, University of Miami (May 2025)

GPA: 3.80

ERMProtect
Cybersecurity Solutions

Summary

Collin Connors is an ERMProtect Information Security Consultant. He develops the company's proprietary tools, such as our automated phishing and phishing-detection tools. He oversees the company's internal security to prevent attacks on our networks, utilizing penetration testing, monitoring logs and security software, including vendor software that analyzes our metadata to assess potential compromises. A Ph.D. candidate at the University of Miami, he is researching the use of AI to detect malware, implementation of blockchain at banks, and prevention of attacks in a shared cloud environment.

Relevant Experience

- **Penetration Tests** - Performed Internal, External, Wireless and Web application penetration tests for clients and for ERMProtect to secure infrastructure, systems, and data. Created automated tools to improve test performance.
- **Security Incident Response** – Participated on a team of security directors to create, implement, and test a plan to prevent attacks on ERMProtect's internal networks, including monitoring for malware, adding security measures, and performing simulated attacks.
- **Security Monitoring** – Created an internal security program to monitor logs for security threats. Researched multiple security tools and implemented the tools into the ERMProtect security architecture. Supervised the continued monitoring of security logs and response to detected threats.
- **Policies and Procedures** – Designed and wrote all internal security policies and procedures based on industry best practices. Oversaw testing and implementation of these policies and procedures.

Research

- **Blockchain Architecture -** Designed a novel blockchain architecture for use in general applications. The architecture was designed to be highly module and easy for a user to implement. Implemented our novel architecture to show the efficacy of our architecture.
- **A Deep Learning Approach to Malware Detection -** Created over 20 deep learning models to analyze Portable Executable Files and classify them as malicious or benign**.** Compared the various architectures to find the most efficient and most accurate model, and then looked at the information measure of each model to validate of our findings.

AVIRAL SHARMA

Consultant, Information Security Consulting Services

asharma@ermprotect.com
(206)513-9143

EDUCATION

Bachelor's degree in Technology, Computer Science and Engineering - Specialization in Information Security, Vellore Institute of Technology

Master's degree in Information Technology – Information Security – Applied Advanced Study, Carnegie Mellon University

Summary

Aviral Sharma is a Consultant, Information Security Services, for ERMProtect. He performs risk assessments, data compliance assessments, and penetration testing for the company. Aviral received his master's degree in information technology from the prestigious Carnegie Mellon University, where he underwent advanced training in code reviews, digital forensics, and vulnerability assessments for mobile applications. He is experienced in web development, image processing, and machine learning as a software developer. He graduated from Carnegie Mellon with a 3.6 GPA, and during his time at Carnegie, worked as an intern at various startups such as Intros.ai and TreeMama Organization as a web developer and an information security analyst. At ERMProtect, in addition to providing a wide variety of IT security services to clients, he is also pursuing certifications in digital forensics and cryptocurrency tracing to further enhance his cybersecurity investigation skills.

Relevant Experience

- **Risk Assessments –** Conducted risk assessments such as GLBA, FACTA for multiple clients. Participated in various vulnerability assessments and penetration tests conducted by ERMProtect. Discovered and proved the lack of security awareness among the non-technical employees of a client's staff, paving the way for training that prevented significant potential monetary losses to the client.

- **Cyber Forensics investigations –** As part of the capstone project for Cyber Forensics Specialization, Aviral had the opportunity to be trained in Cyber forensics and participate in mock investigations that mirrored real-world security incidents. These team investigations were conducted in conjunction with industry experts including but not limited to professionals from cyber forensics teams at police departments, law firms, and private investigation companies, etc.

- **Vulnerability Assessments –** Performed static and dynamic secure code reviews as well as vulnerability assessments of web and mobile applications developed in multiple languages, using a number of tools such as AppScan, Fortify, Coverity.

- **Research Experience –** Published a thesis exploring the feasibility of using Digital Twins concept to reinforce the security, availability, and privacy of an IT infrastructure with meaningful returns.

- **Web Development & Security –** Working on development of a SOC2 automation tool as a full-stack developer at ERMProtect. Has experience in using various tools such python, Java, JavaScript, php, MySQL, etc.

VIBHA DHIRAJ PUTHRAN

Information Security Consultant

vputhran@ermprotect.com
305-447-6750

EDUCATION

Bachelor in Technology (Computer Science Engineering), PES University

Postgraduate Diploma in Cyber Law and Cyber Forensics, National Law School of India University

Master of Science in Information Technology – Information Security, Carnegie Mellon University

CERTIFICATIONS

- EC Council Certified Incident Handler
- Microsoft Azure Fundamentals
- CyberArk Certified Trustee
- Splunk 7. X Fundamentals Part 1
- Autopsy and Cyber Triage DFIR
- ICSI Certified Network Security Specialist (CNSS)

ERMProtect
Cybersecurity Solutions

Summary

Vibha Dhiraj Puthran is an Information Security Consultant. She performs digital forensic investigations and data breach investigations for the firm's diverse client base. Her training in incident response and advanced digital forensics equips her to battle data breaches in a technically and legally-sound manner. She has assisted multiple organizations to identify system vulnerabilities, harden security, and close gaps that could lead to breaches and regulatory fines. Prior to joining ERMProtect, she worked as a Cybersecurity Consultant for PwC in India. She has a master's degree in information technology from Carnegie Mellon University.

Relevant Experience

- **Digital Forensic & Incident Response** – Led investigations involving data manipulation by an insider, ATM intrusions, ransomware, business email compromises, and other types of data breaches.
- **Tabletop Exercises** – Led tabletop drills for multinational clients to test and improve their incident response plans. Created an Incident Response Playbook and facilitated training.
- **Cyber Crime** – Working as an intern for a State Police department, gained an understanding of the methodology of investigation of cybercrimes reported to the Government of India. Learned the digital forensics methodology, including acquiring hard drive images and analysis of call detail records. Also, co-led training for police officers regarding cybercrimes.

Publications

- **Data Privacy and User Consent** – An Experimental Study on Various Smartphones (2021) International Journal of Digital Society (IJDS), Volume 12, Issue 1
- **Detecting Data Exfiltration on Android Phones (2020)** – Presented the paper at the World Congress on Internet Security (WorldCIS) 2020 Conference held in London.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: LOT2400000009

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

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

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

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

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

Enterprise Risk Management, Inc. (dba ERMProtect)
Company

Authorized Signature

March 26, 2024
Date

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

10.2. The following remedies shall be available to Agency upon default.

10.2.1. Immediate cancellation of the Contract.

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

10.2.3. Any other remedies available in law or equity.

11. MISCELLANEOUS:

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

Contract Manager: Silka M. Gonzalez
Telephone Number: 305-447-6750 / 305-335-7610
Fax Number: 305-447-6752
Email Address: sgonzalez@ermprotect.com

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Silka M. Gonzalez

(Address) 800 S Douglas Rd. Suite 940 N, Coral Gables, FL 33134

(Phone Number) / (Fax Number) 305-447-6750 305 447 6752

(email address) sgonzalez@ermprotect.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through *wv*OASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Enterprise Risk Management, Inc. (dba ERMProtect)
(Company)

(Signature of Authorized Representative)

Silka M. Gonzalez President
(Printed Name and Title of Authorized Representative) (Date)

305-335-7610
(Phone Number) (Fax Number)

sgonzalez@ermprotect.com
(Email Address)

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

State of West Virginia
Centralized Request for Quote
Service - Prof

Proc Folder: 1369290			**Reason for Modification:**
Doc Description: Network Penetration Testing and Cybersecurity Assessments			
Proc Type: Central Master Agreement			
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2024-03-08	2024-03-28 13:30	CRFQ 0705 LOT2400000009	1

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:

Vendor Name :

Address :

Street :

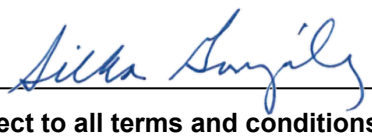
City :

State : **Country :** **Zip :**

Principal Contact :

Vendor Contact Phone: **Extension:**

FOR INFORMATION CONTACT THE BUYER
Brandon L Barr
304-558-2652
brandon.l.barr@wv.gov

Vendor Signature X  **FEIN#** 65-0827427 **DATE** March 26, 2024

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

EXHIBIT A - Pricing Page

Item #	Section	Description of Service	*Estimated Number of Assesments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	$ 1,485 -	$ 11,880 -
2	4.2	Website Penetration Testing	8	$ 895 -	$ 7,160 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	$ 3,191.25 -	$ 25,530 -
4	4.4	Wireless Penetration Testing	8	$ 3,985 -	$ 31,880 -
				TOTAL BID AMOUNT	$ 76,450 -

Please note the following information is being captured for auditing purposes and is an estimate for evaluation only

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

Any product or service not on the Agency provided Pricing Page will not be allowable.

The state cannot accept alternate pricing pages, failure to use Exhibit A Pricing Page could lead to disqualification of vendors bid.

Vendor Name:	Enterprise Risk Management, Inc. (dba ERMProtect)
Vendor Address:	800 S Douglas Rd. Suite 940 N, Coral Gables, FL 33134
Email Address:	sgonzalez@ermprotect.com
Phone Number:	305-447-6750 / 305-335-7610
Fax Number:	305 447 6752
Signature and Date:	March 27, 2024