Rethinking Your Cybersecurity

RSI Security Response to

Region 14 Education Service Center
for
IT Security Products and Data Protection Solutions
National Cooperative Purchasing Alliance
RFP # 40-22

Submitted By:
John Shin
RSI Systems, Inc. dba RSI Security
10531 4S Commons Drive, Suite 527, San Diego, CA 92127
bids@rsisecurity.com
www.rsisecurity.com
858.999.3030

November 167, 2022

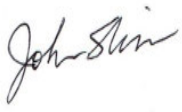
Region 14 ESC and NCPA

RSI Security is pleased to present this proposal to Region 14 ESC ("the Region") and the National Cooperative Purchasing Alliance (NCPA) for the provision of IT data protection services.

RSI Security is committed to excellence in the provision of compliance advisory and managed IT and security services. We have performed thousands of engagements for clients in a variety of industries, including state and local governments and educational institutions.

If you have any questions regarding the contents of this proposal, please do not hesitate to contact us. I confirm that the contents of this proposal, all attachments, and corresponding pricing are valid for no less than (120) calendar days from the date of bid opening and that RSI Security takes no exceptions or deviations from the terms, conditions, and specifications of the solicitation as written. We look forward to helping you meet your cybersecurity needs.

Best regards,



John Shin
Managing Director

Tab 1 – Master Agreement / Signature Form 3

Tab 2 – NCPA Administration Agreement 4

Tab 3 – Vendor Questionnaire 5

Tab 4 – Vendor Profile 6

Tab 5 – Products and Services / Scope 14

PCI DSS Consulting and Assessment 14

Risk Assessment 15

Vulnerability Assessment and Penetration Testing 16

Incident Response, Continuity of Operations, and Disaster Recovery Planning 18

Tab 6 – References 21

Tab 7 – Pricing 29

Tab 8 – Value Added Products and Services 30

Security Awareness Training 31

Tab 9 – Required Documents 35

REFERENCES 36

SYSTEM and ADDITIONAL REQUIREMENTS 36

ATTACHMENTS 44

Tab 1 – Master Agreement / Signature Form

TAB 1
MASTER AGREEMENT - GENERAL TERMS AND CONDITIONS

Customer Support
The vendor shall provide timely and accurate technical advice and sales support. The vendor shall respond to such requests within one (1) working day after receipt of the request.

Disclosures
Respondent affirms that he/she has not given, offered to give, nor intends to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor or service to a public servant in connection with this contract.

The respondent affirms that, to the best of his/her knowledge, the offer has been arrived at independently, and is submitted without collusion with anyone to obtain information or gain any favoritism that would in any way limit competition or give an unfair advantage over other vendors in the award of this contract.

Renewal of Contract
Unless otherwise stated, all contracts are for a period of three (3) years with an option to renew for up to two (2) additional one-year terms or any combination of time equally not more than 2 years if agreed to by Region 14 ESC and the vendor.

Funding Out Clause
Any/all contracts exceeding one (1) year shall include a standard “funding out” clause. A contract for the acquisition, including lease, of real or personal property is a commitment of the entity’s current revenue only, provided the contract contains either or both of the following provisions:

Retains to the entity the continuing right to terminate the contract at the expiration of each budget period during the term of the contract and is conditioned on a best efforts attempt by the entity to obtain appropriate funds for payment of the contract.

Shipments (if applicable)
The awarded vendor shall ship ordered products within seven (7) working days for goods available and within four (4) to six (6) weeks for specialty items after the receipt of the order unless modified. If a product cannot be shipped within that time, the awarded vendor shall notify the entity placing the order as to why the product has not shipped and shall provide an estimated shipping date. At this point the participating entity may cancel the order if estimated shipping time is not acceptable.

Tax Exempt Status
Since this is a national contract, knowing the tax laws in each state is the sole responsibility of the vendor.

Payments
The entity using the contract will make payments directly to the awarded vendor or their affiliates (distributors/business partners/resellers) as long as written request and approval by NCPA is provided to the awarded vendor.

Adding Authorized Distributors/Dealers
Awarded vendors may submit a list of distributors/partners/resellers to sell under their contract throughout the life of the contract. Vendor must receive written approval from NCPA before such distributors/partners/resellers considered authorized.

Purchase orders and payment can only be made to awarded vendor or distributors/ business partners/resellers previously approved by NCPA.

Pricing provided to members by added distributors or dealers must also be less than or equal to the pricing offered by the awarded contract holder.

All distributors/partners/resellers are required to abide by the Terms and Conditions of the vendor's agreement with NCPA.

Pricing
All pricing submitted shall include the administrative fee to be remitted to NCPA by the awarded vendor. It is the awarded vendor's responsibility to keep all pricing up to date and on file with NCPA.

All deliveries shall be freight prepaid, F.O.B. destination and shall be included in all pricing offered unless otherwise clearly stated in writing

Warranty
Proposal should address the following warranty information:

- Applicable warranty and/or guarantees of equipment and installations including any conditions and response time for repair and/or replacement of any components during the warranty period.
- Availability of replacement parts
- Life expectancy of equipment under normal use
- Detailed information as to proposed return policy on all equipment

Products: Vendor shall provide equipment, materials and products that are new unless otherwise specified, of good quality and free of defects
Construction: Vendor shall perform services in a good and workmanlike manner and in accordance with industry standards for the service provided.

Safety
Vendors performing services shall comply with occupational safety and health rules and regulations. Also all vendors and subcontractors shall be held responsible for the safety of their employees and any conditions that may cause injury or damage to persons or property.

Permits
Since this is a national contract, knowing the permit laws in each state is the sole responsibility of the vendor.

Indemnity
The awarded vendor shall protect, indemnify, and hold harmless Region 14 ESC and its participants, administrators, employees and agents against all claims, damages, losses and expenses arising out of or resulting from the actions of the vendor, vendor employees or vendor subcontractors in the preparation of the solicitation and the later execution of the contract.

Franchise Tax
The respondent hereby certifies that he/she is not currently delinquent in the payment of any franchise taxes.

Supplemental Agreements
The entity participating in this contract and awarded vendor may enter into a separate supplemental agreement to further define the level of service requirements over and above the minimum defined in this contract i.e. invoice requirements, ordering requirements, specialized delivery, etc. Any supplemental agreement developed as a result of this contract is exclusively between the participating entity and awarded vendor.

Certificates of Insurance
Certificates of insurance shall be delivered to the Public Agency prior to commencement of work. The insurance company shall be licensed in the applicable state in which work is being conducted. The awarded vendor shall give the participating entity a minimum of ten (10) days notice prior to any modifications or cancellation of policies. The awarded vendor shall require all subcontractors performing any work to maintain coverage as specified.

Legal Obligations
It is the Respondent's responsibility to be aware of and comply with all local, state, and federal laws governing the sale of products/services identified in this RFP and any awarded contract and shall comply with all while fulfilling the RFP. Applicable laws and regulation must be followed even if not specifically identified herein.

Protest
A protest of an award or proposed award must be filed in writing within ten (10) days from the date of the official award notification and must be received by 5:00 pm CST. Protests shall be filed with Region 14 ESC and shall include the following:

- Name, address and telephone number of protester
- Original signature of protester or its representative
- Identification of the solicitation by RFP number
- Detailed statement of legal and factual grounds including copies of relevant documents and the form of relief requested

Any protest review and action shall be considered final with no further formalities being considered.

Force Majeure
If by reason of Force Majeure, either party hereto shall be rendered unable wholly or in part to carry out its obligations under this Agreement then such party shall give notice and full particulars of Force Majeure in writing to the other party within a reasonable time after occurrence of the event or cause relied upon, and the obligation of the party giving such notice, so far as it is affected by such Force Majeure, shall be suspended during the continuance of the inability then claimed, except as hereinafter provided, but for no longer period, and such party shall endeavor to remove or overcome such inability with all reasonable dispatch.

The term Force Majeure as employed herein, shall mean acts of God, strikes, lockouts, or other industrial disturbances, act of public enemy, orders and regulation of any kind of government of the United States or any civil or military authority; insurrections; riots; epidemics; pandemic; landslides; lighting; earthquake; fires; hurricanes; storms; floods; washouts; droughts; arrests; restraint of government and people; civil disturbances; explosions, breakage or accidents to machinery, pipelines or canals, or other causes not reasonably within the control of the party claiming such inability. It is understood and agreed that the settlement of strikes and lockouts shall be entirely within the discretion of the party having the difficulty, and that the above requirement that any Force Majeure shall be remedied with all reasonable dispatch shall not require the settlement of strikes and lockouts by acceding to the demands of the opposing party or parties when such settlement is unfavorable in the judgment of the party having the difficulty

Prevailing Wage
It shall be the responsibility of the Vendor to comply, when applicable, with the prevailing wage legislation in effect in the jurisdiction of the purchaser. It shall further be the responsibility of the Vendor to monitor the prevailing wage rates as established by the appropriate department of labor for any increase in rates during the term of this contract and adjust wage rates accordingly.

Termination
Either party may cancel this contract in whole or in part by providing written notice. The cancellation will take effect 30 business days after the other party receives the notice of cancellation. After the 30th business day all work will cease following completion of final purchase order.

Open Records Policy
Because Region 14 ESC is a governmental entity responses submitted are subject to release as public information after contracts are executed. If a vendor believes that its response, or parts of its response, may be exempted from disclosure, the vendor must specify page-by-page and line-by-line the parts of the response, which it believes, are exempt. In addition, the respondent must specify which exception(s) are applicable and provide detailed reasons to substantiate the exception(s).

The determination of whether information is confidential and not subject to disclosure is the duty of the Office of Attorney General (OAG). Region 14 ESC must provide the OAG sufficient

information to render an opinion and therefore, vague and general claims to confidentiality by the respondent are not acceptable. Region 14 ESC must comply with the opinions of the OAG. Region14 ESC assumes no responsibility for asserting legal arguments on behalf of any vendor. Respondent are advised to consult with their legal counsel concerning disclosure issues resulting from this procurement process and to take precautions to safeguard trade secrets and other proprietary information.

PROCESS

Region 14 ESC will evaluate proposals in accordance with, and subject to, the relevant statutes, ordinances, rules, and regulations that govern its procurement practices. NCPA will assist Region 14 ESC in evaluating proposals. Award(s) will be made to the prospective vendor whose response is determined to be the most advantageous to Region 14 ESC, NCPA, and its participating agencies. To qualify for evaluation, response must have been submitted on time, and satisfy all mandatory requirements identified in this document.

Contract Administration
The contract will be administered by Region 14 ESC. The National Program will be administered by NCPA on behalf of Region 14 ESC.

Contract Term
The contract term will be for three (3) year starting from the date of the award. The contract may be renewed for up to two (2) additional one-year terms or any combination of time equally not more than 2 years.

It should be noted that maintenance/service agreements may be issued for up to (5) years under this contract even if the contract only lasts for the initial term of the contract. NCPA will monitor any maintenance agreements for the term of the agreement provided they are signed prior to the termination or expiration of this contract.

Contract Waiver
Any waiver of any provision of this contract shall be in writing and shall be signed by the duly authorized agent of Region 14 ESC. The waiver by either party of any term or condition of this contract shall not be deemed to constitute waiver thereof nor a waiver of any further or additional right that such party may hold under this contract.

Price Increases
Should it become necessary, price increase requests may be submitted at any point during the term of the contract by written amendment. Included with the request must be documentation and/or formal cost justification for these changes. Requests will be formally reviewed, and if justified, the amendment will be approved.

Products and Services Additions
New Products and/or Services may be added to the resulting contract at any time during the term by written amendment, to the extent that those products and/or services are within the scope of this RFP.

Competitive Range
It may be necessary for Region 14 ESC to establish a competitive range. Responses not in the competitive range are unacceptable and do not receive further award consideration.

Deviations and Exceptions
Deviations or exceptions stipulated in response may result in disqualification. It is the intent of Region 14 ESC to award a vendor's complete line of products and/or services, when possible.

Estimated Quantities
While no minimum volume is guaranteed, the estimated (but not limited to) annual volume for Products and Services purchased under the proposed Master Agreement is $50 million dollars annually. This estimate is based on the anticipated volume of Region 14 ESC and current sales within the NCPA program.

Evaluation
Region 14 ESC will review and evaluate all responses in accordance with, and subject to, the relevant statutes, ordinances, rules and regulations that govern its procurement practices. NCPA will assist the lead agency in evaluating proposals. Recommendations for contract awards will be based on multiple factors, each factor being assigned a point value based on its importance.

Formation of Contract
A response to this solicitation is an offer to contract with Region 14 ESC based upon the terms, conditions, scope of work, and specifications contained in this request. A solicitation does not become a contract until it is accepted by Region 14 ESC. The prospective vendor must submit a signed Signature Form with the response thus, eliminating the need for a formal signing process. Contract award letter issued by Region 14 ESC is the counter-signature document establishing acceptance of the contract.

NCPA Administrative Agreement
The vendor will be required to enter and execute the National Cooperative Purchasing Alliance Administration Agreement with NCPA upon award with Region 14 ESC. The agreement establishes the requirements of the vendor with respect to a nationwide contract effort.

Clarifications/Discussions
Region 14 ESC may request additional information or clarification from any of the respondents after review of the proposals received for the sole purpose of elimination minor irregularities, informalities, or apparent clerical mistakes in the proposal. Clarification does not give respondent an opportunity to revise or modify its proposal, except to the extent that correction of apparent clerical mistakes results in a revision. After the initial receipt of proposals, Region 14 ESC reserves the right to conduct discussions with those respondent's whose proposals are determined to be reasonably susceptible of being selected for award. Discussions occur when oral or written communications between Region 14 ESC and respondent's are conducted for the purpose clarifications involving information essential for determining the acceptability of a proposal or that provides respondent an opportunity to revise or modify its proposal. Region 14 ESC will not assist respondent bring its proposal up to the level of other proposals through discussions. Region 14 ESC will not indicate to respondent a cost or price that it must meet to neither obtain further consideration nor will it provide any information about other respondents' proposals or prices.

Multiple Awards
Multiple Contracts may be awarded as a result of the solicitation. Multiple Awards will ensure that any ensuing contracts fulfill current and future requirements of the diverse and large number of participating public agencies.

Past Performance
Past performance is relevant information regarding a vendor's actions under previously awarded contracts; including the administrative aspects of performance; the vendor's history of reasonable and cooperative behavior and commitment to customer satisfaction; and generally, the vendor's businesslike concern for the interests of the customer.

EVALUATION CRITERIA

Pricing (40 points)
Electronic Price Lists

- Products, Services, Warranties, etc. price list
- Prices listed will be used to establish both the extent of a vendor's product lines, services, warranties, etc. available from a particular bidder and the pricing per item.

Ability to Provide and Perform the Required Services for the Contract (25 points)

- Product Delivery within participating entities specified parameters
- Number of line items delivered complete within the normal delivery time as a percentage of line items ordered.
- Vendor's ability to perform towards above requirements and desired specifications.
- Past Cooperative Program Performance
- Quantity of line items available that are commonly purchased by the entity.
- Quality of line items available compared to normal participating entity standards.

References and Experience (20 points)

- A minimum of ten (10) customer references for product and/or services of similar scope dating within past 3 years
- Respondent Reputation in marketplace
- Past Experience working with public sector.
- Exhibited understanding of cooperative purchasing

Value Added Products/Services Description, (8 points)

- Additional Products/Services related to the scope of RFP
- Marketing and Training
- Minority and Women Business Enterprise (MWBE) and (HUB) Participation
- Customer Service

Technology for Supporting the Program (7 points)

- Electronic on-line catalog, order entry use by and suitability for the entity's needs
- Quality of vendor's on-line resources for NCPA members.
- Specifications and features offered by respondent's products and/or services

SIGNATURE FORM

The undersigned hereby proposes and agrees to furnish goods and/or services in strict compliance with the terms, specifications and conditions at the prices proposed within response unless noted in writing. The undersigned further certifies that he/she is an officer of the company and has authority to negotiate and bind the company named below and has not prepared this bid in collusion with any other Respondent and that the contents of this proposal as to prices, terms or conditions of said bid have not been communicated by the undersigned nor by any employee or agent to any person engaged in this type of business prior to the official opening of this proposal.

Prices are guaranteed: **120 days**

RSI Systems, Inc. dba RSI Security

Company Name

10531 4S Commons Drive, Suite 527

Address

San Diego, CA 92127

City State Zip

858.999.3030

Telephone Number

858.999.6714

Fax Number

bids@rsisecurity.com

Email Address

John Shin

Printed Name

Managing Director

Position

Authorized Signature

Tab 2 – NCPA Administration Agreement

RSI Security has reviewed and acknowledges the provided Administration Agreement and will sign this Agreement upon award as requested.

TAB 2
NCPA ADMINISTRATION AGREEMENT

This Administration Agreement is made as of December 1, 2022, by and between National Cooperative Purchasing Alliance ("NCPA") and RSI Systems, Inc. dba RSI Security ("Vendor").

Recitals

WHEREAS, Region 14 ESC has entered into a certain Master Agreement dated December 1, 2022, referenced as Contract Number 01-157, by and between Region 14 ESC and Vendor, as may be amended from time to time in accordance with the terms thereof (the "Master Agreement"), for the purchase of IT Security Products and Data Protection Solutions;

WHEREAS, said Master Agreement provides that any state, city, special district, local government, school district, private K-12 school, technical or vocational school, higher education institution, other government agency or nonprofit organization (hereinafter referred to as "public agency" or collectively, "public agencies") may purchase products and services at the prices indicated in the Master Agreement;

WHEREAS, NCPA has the administrative and legal capacity to administer purchases under the Master Agreement to public agencies;

WHEREAS, NCPA serves as the administrative agent for Region 14 ESC in connection with other master agreements offered by NCPA

WHEREAS, Region 14 ESC desires NCPA to proceed with administration of the Master Agreement;

WHEREAS, NCPA and Vendor desire to enter into this Agreement to make available the Master Agreement to public agencies on a national basis;

NOW, THEREFORE, in consideration of the payments to be made hereunder and the mutual covenants contained in this Agreement, NCPA and Vendor hereby agree as follows:

General Terms and Conditions

- The Master Agreement, attached hereto as Exhibit 1 and incorporated herein by reference as though fully set forth herein, and the terms and conditions contained therein shall apply to this Administration Agreement except as expressly changed or modified by this Administration Agreement.
- NCPA shall be afforded all of the rights, privileges and indemnifications afforded to Region 14 ESC under the Master Agreement, and such rights, privileges and indemnifications shall accrue and apply with equal effect to NCPA under this Administration Agreement including, but not limited to, Contractor's obligation to provide appropriate insurance and certain indemnifications to Region 14 ESC.

- Contractor shall perform all duties, responsibilities and obligations required under the Master Agreement in the time and manner specified by the Master Agreement.
- NCPA shall perform all of its duties, responsibilities, and obligations as administrator of purchases under the Master Agreement as set forth herein, and Contractor acknowledges that NCPA shall act in the capacity of administrator of purchases under the Master Agreement.
- With respect to any purchases made by Region 14 ESC or any Participating Agency pursuant to the Master Agreement, NCPA (a) shall not be construed as a dealer, re-marketer, representative, partner, or agent of any type of Contractor, Region 14 ESC, or such Participating Agency, (b) shall not be obligated, liable or responsible (i) for any orders made by Region 14 ESC, any Participating Agency or any employee of Region 14 ESC or Participating Agency under the Master Agreement, or (ii) for any payments required to be made with respect to such order, and (c) shall not be obligated, liable or responsible for any failure by the Participating Agency to (i) comply with procedures or requirements of applicable law, or (ii) obtain the due authorization and approval necessary to purchase under the Master Agreement. NCPA makes no representations or guaranties with respect to any minimum purchases required to be made by Region 14 ESC, any Participating Agency, or any employee of Region 14 ESC or Participating Agency under this Administration Agreement or the Master Agreement.
- With respect to any supplemental agreement entered into between a Participating Agency and Contractor pursuant to the Master Agreement, NCPA, its agents, members and employees shall not be made party to any claim for breach of such agreement.
- This Administration Agreement supersedes any and all other agreements, either oral or in writing, between the parties hereto with respect to the subject matter hereof, and no other agreement, statement, or promise relating to the subject matter of this Administrative Agreement which is not contained herein shall be valid or binding.
- Contractor agrees to allow NCPA to use their name and logo within website, marketing materials and advertisement. Any use of NCPA name and logo or any form of publicity regarding this Administration Agreement or the Master Agreement by Contractor must have prior approval from NCPA.
- If any action at law or in equity is brought to enforce or interpret the provisions of this Administration Agreement or to recover any administrative fee and accrued interest, the prevailing party shall be entitled to reasonable attorney's fees and costs in addition to any other relief to which such party may be entitled.
- Neither this Administration Agreement nor any rights or obligations hereunder shall be assignable by Contractor without prior written consent of NCPA, provided, however, that the Contractor may, without such written consent, assign this Administration Agreement and its rights and delegate its obligations hereunder in connection with the transfer or sale of all or substantially all of its assets or business related to this Administration Agreement, or in the event of its merger, consolidation, change in control or similar transaction. Any permitted assignee shall assume all assigned obligations of its assignor under this Administration Agreement.
- This Administration Agreement and NCPA's rights and obligations hereunder may be assigned at NCPA's sole discretion, to an existing or newly established legal entity that has the authority and capacity to perform NCPA's obligations hereunder.

Term of Agreement

This Agreement shall be in effect so long as the Master Agreement remains in effect, provided, however, that the obligation to pay all amounts owed by Vendor to NCPA through the

termination of this Agreement and all indemnifications afforded by Vendor to NCPA shall survive the term of this Agreement.

Fees and Reporting

The awarded vendor shall electronically provide NCPA with a detailed quarterly report showing the dollar volume of all sales under the contract for the previous quarter. Reports are due on the fifteenth (15th) day after the close of the previous quarter. It is the responsibility of the awarded vendor to collect and compile all sales under the contract from participating members and submit one (1) report. The report shall include at least the following information as listed in the example below:

Entity Name	Zip Code	State	PO or Job #	Sale Amount

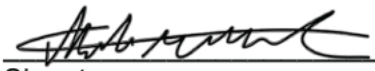
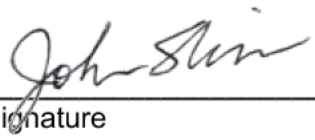
Total _____

Each quarter NCPA will invoice the vendor based on the total of sale amount(s) reported. From the invoice the vendor shall pay to NCPA an administrative fee based upon the tiered fee schedule below. Vendor's annual sales shall be measured on a calendar year basis. Deadline for term of payment will be included in the invoice NCPA provides.

Annual Sales Through Contract	Administrative Fee
0 - $30,000,000	2%
$30,000,001 - $50,000,000	1.5%
$50,000,001+	1%

Supplier shall maintain an accounting of all purchases made by Public Agencies under the Master Agreement. NCPA and Region 14 ESC reserve the right to audit the accounting for a period of four (4) years from the date NCPA receives the accounting. In the event of such an audit, the requested materials shall be provided at the location designated by Region 14 ESC or NCPA. In the event such audit reveals an under reporting of Contract Sales and a resulting underpayment of administrative fees, Vendor shall promptly pay NCPA the amount of such underpayment, together with interest on such amount and shall be obligated to reimburse NCPA's costs and expenses for such audit.

ACKNOWLEDGMENT OF CONTRACTOR REQUIREMENTS

National Cooperative Purchasing Alliance	**RSI Systems, Inc dba RSI Security**
Organization	Vendor Name
Matthew Mackel	**John Shin**
Name	Name
Director, Business Development	**Managing Director**
Title	Title
PO Box 701273	**10531 4S Commons Drive, Suite 527**
Address	Address
Houston, TX 77270	**San Diego, CA 92127**
Address	Address
	
Signature	Signature
December 1, 2022	December 1, 2022
Date	Date

Tab 3 – Vendor Questionnaire

TAB 3
VENDOR QUESTIONAIRE

Please provide responses to the following questions that address your company's operations, organization, structure, and processes for providing products and services.

Locations Covered

- Bidder must indicate any and all locations where products and services can be offered.
- Please indicate the price co-efficient for each location if it varies.

☒ **All 50 States & District of Columbia** (Selecting this box is equal to checking all boxes below)			
☐ Alabama	☐ Illinois	☐ Montana	☐ Rhode Island
☐ Alaska	☐ Indiana	☐ Nebraska	☐ South Carolina
☐ Arizona	☐ Iowa	☐ Nevada	☐ South Dakota
☐ Arkansas	☐ Kansas	☐ New Hampshire	☐ Tennessee
☐ California	☐ Massachusetts	☐ New Jersey	☐ Texas
☐ Colorado	☐ Michigan	☐ New Mexico	☐ Utah
☐ Connecticut	☐ Minnesota	☐ New York	☐ Vermont
☐ Delaware	☐ Mississippi	☐ North Carolina	☐ Virginia
☐ D.C.	☐ Missouri	☐ North Dakota	☐ Washington
☐ Florida	☐ Kentucky	☐ Ohio	☐ West Virginia
☐ Georgia	☐ Louisiana	☐ Oklahoma	☐ Wisconsin
☐ Hawaii	☐ Maine	☐ Oregon	☐ Wyoming
☐ Idaho	☐ Maryland	☐ Pennsylvania	

☒ **All U.S. Territories and Outlying Areas** (Selecting this box is equal to checking all boxes below)	
☐ American Somoa	☐ Northern Marina Island
☐ Federated States of Micrones	☐ Puerto Rico
☐ Guam	☐ U.S. Virgin Islands
☐ Midway Islands	

☒ **All Canada Provinces and Territories** (Selecting this box is equal to checking all boxes below)	
☐ Alberta	☐ Prince Edward Island
☐ British Columbia	☐ Quebec
☐ Manitoba	☐ Saskatchewan
☐ New Brunswick	☐ Northwest Territories
☐ Newfoundland and Labrador	☐ Nunavut
☐ Nova Scotia	☐ Yukon
☐ Ontario	

If awarded a Master Agreement, will your company extend the terms offered in your Proposal to public agencies in Canada? If no or maybe, please explain.

☒ Yes ☐ Maybe ☐ No

If awarded a Master Agreement, will your company extend the terms offered in your Proposal to private sector customers?

☐ Yes ☒ Maybe ☐ No

Minority and Women Business Enterprise (MWBE) and (HUB) Participation
It is the policy of some entities participating in NCPA to involve minority and women business enterprises (MWBE) and historically underutilized businesses (HUB) in the purchase of goods and services. Respondents shall indicate below whether or not they are an M/WBE or HUB certified.

☒ Minority/Women Business Enterprise
Respondent Certifies that this firm a Minority / Women Business Enterprise

☐ Historically Underutilized Business
Respondent Certifies that this firm is a Historically Underutilized Business

Small Business, MWBE and HUB Growth
If Proposer is a Large, National or Multinational Organization/Corporation, what programs are in place that partners or supports the growth of small and MWEB and HUB business? If yes, please describe.

☒ N/A, we are a recognized small, MWEB or HUB organization

☐ No, we do not have any programs in place.

☐ Yes, we have programs in place.

Residency
Responding Company's principal place of business is in the city of San Diego, State of California.

Felony Conviction Notice
Please Check Applicable Box (If the 3rd box is checked, a detailed explanation of the names and convictions must be attached):

☐ A publicly held corporation; therefore, this reporting requirement is not applicable.

☒ Is not owned or operated by anyone who has been convicted of a felony.

☐ Is owned or operated by the following individual(s) who has/have been convicted of a felony

Distribution Channel
Which best describes your company's position in the distribution channel:

☐ Manufacturer Direct ☐ Certified education/government reseller

☐ Authorized Distributor ☐ Manufacturer marketing through reseller

☒ Value-added reseller ☒ Other: IT Services provider

Processing Contact Information

Contact Person	John Shin
Title	Managing Director
Company	RSI Systems Inc., DBA RSI Security
Address	10531 4S Commons Drive, Suite 527
City/State/Zip	San Diego, CA 92127
Phone	858.999.3030
Email	bids@rsisecurity.com

Pricing Information
In addition to the current typical unit pricing furnished herein, the Vendor agrees to offer all future product introductions at prices that are proportionate to Contract Pricing. If answer is no, attach a statement detailing how pricing for NCPA participants would be calculated for future product introductions.

☒ Yes ☐ No

Pricing submitted includes the required NCPA administrative fee. The NCPA fee is calculated based on the invoice price to the customer.

☒ ☐

Tab 4 – Vendor Profile

Founded in San Diego as a California S Corporation in 2013, RSI Systems, Inc. DBA RSI Security is a cybersecurity firm working exclusively to defend the cyber environments of American and transnational organizations. Since our inception, we've taken great pride in providing unparalleled cybersecurity services for clients in nearly every industry, including the government sector. In the nine years that we have been incorporated, we have performed thousands of assessments and have provided IT security consulting for over 250 clients.

In accordance with the solicitation we have provided the following information:

DUNS Number	079971681	
Standard Payment Terms	Upon receipt of invoice	
Marketplace Competition	Small business IT cybersecurity service providers nationwide	
Number of employees	35 full-time employees, numerous consultants and 1099 contractor employees	
Anticipated Revenue	RSI Security consistently earns between $5-7 million per year across all engagements. We anticipate this will continue over the next 3 years.	

What differentiates your company from competitors?

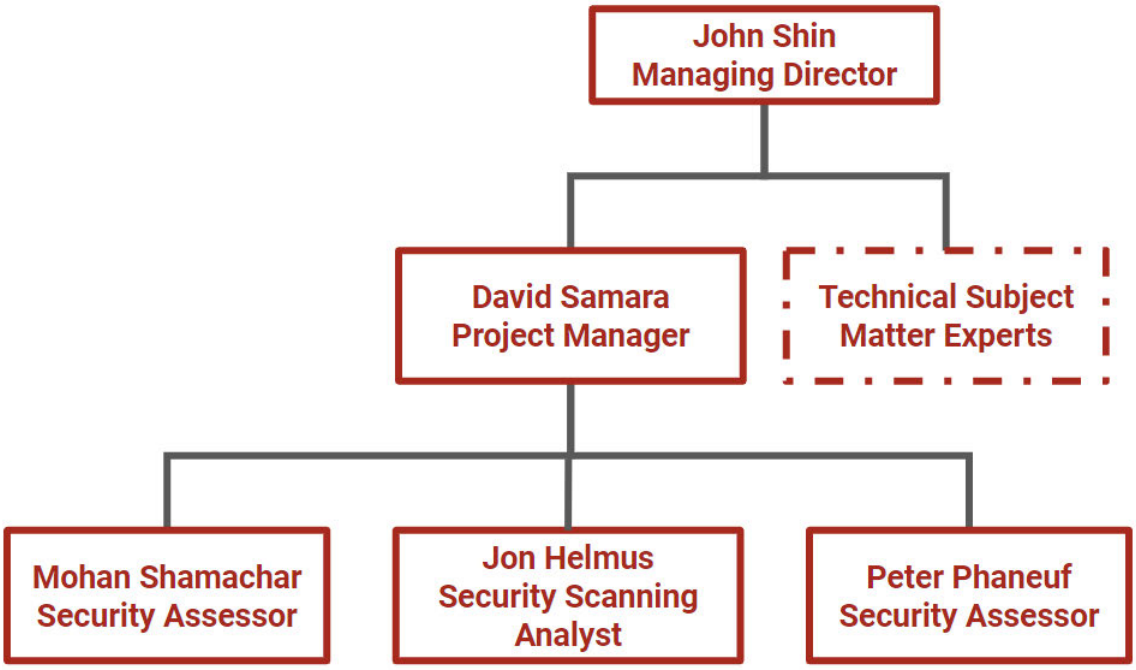
RSI Security is certified as an SB(Micro) business. We are also a 100% minority-owned and 50% woman-owned firm. We are proud of our client relationships and retention rate, which is 92% over the year.

Key Personnel Organizational Chart and Bios

Our internal structure consists of the following teams:

- Technical Advisory & Consulting (TAC)
- Project Management Office (PMO)
- Sales
- Marketing
- Human Resources & Operations (HR/Ops)
- Technical Operations (TechOps)
- Finance

For each specific engagement, we identify, propose, and provide qualified assessors and cybersecurity engineers most appropriate to the needs of the client we are serving. All engagements are overseen by a technical project manager and supervised by our managing director to ensure consistency in the quality of services provided. The following biographies summarize the experience and qualifications of our proposed key personnel for NCPA engagements.



John Shin, Managing Director – *QSA, CISSP, CISM, CISA, PMP, ASV, CHQP, CCSFP*
John@rsisecurity.com
22 Years Experience
John H. Shin is a principal author on multiple Internet privacy and security technology papers, such as "Dominant Cyber Offensive Engagement and Supporting Technology" and "Reconnaissance and Data Exfiltration" for the U.S. Air Force Research Laboratory. Mr. Shin has over two decades of leadership, management and information technology experience. His area of expertise is IT security and technology management. He was responsible for external customer information systems as well as the global infrastructure operations at Abraxas Corporation, a risk mitigation technology company solely focused on the National Security Community. Mr. Shin also worked in several management positions for Genoptix, Inc. (Nasdaq: GXDX) in the IT/Bioinformatics division. During his tenure at SunGard, Mr. Shin performed as an operations engineer responsible for mission-critical infrastructure and ISO-compliance system processes.

David Samara, Senior Technical Project Manager – *CISSP, PMP, CSM, CQIA, CCP, CMMC-RP*
Davids@rsisecurity.com
18 Years Experience
David Samara is a skilled technical project manager able to define and deliver project scope, timelines, budget, and quality expectations utilizing operational policies, processes, and project management best-practice methodologies. With over 18 years installing, operating, managing, and shaping IT/OT mechanical systems, Mr. Samara is adept at leading and contributing to

multiple projects simultaneously. He effectively manages risks, delivers requirements that meet and exceed clients' expectations, and cultivates relationships with executives, vendors, and internal/external stakeholders. Mr. Samara has an active DoD security clearance.

Mohan Shamachar, Senior Assessor – *CIPP/US, QSA, CISM, CISA, CISSP, CCSFP, CMMC RP*
Mohan@rsisecurity.com
17 Years Experience
Mohan Shamachar is a skilled and experienced QSA, Certified Information Systems Security Professional, Certified Auditor and Business Management Professional with over 17 years of leadership, management and Information Technology experience. Mohan's professional responsibilities include projects and program management, compliance audits, assessments and security consulting and architecting technology solutions.

Senior Assessor - QSA - Peter Phaneuf – *QSA, CISSP, CISA, CISM, CMMC-RP*
Peter@rsisecurity.com
Peter Phaneuf is a CMMC RP, skilled and experienced PCI DSS QSA, CCPA and GDPR technical subject matter expert with 35 years of leadership, management and information technology experience. Peter's professional responsibilities include projects and program management, compliance audits, assessments and security consulting. In the last 15 years, Peter has focused on consulting services in highly regulated industries and delivering cybersecurity-related solutions ranging from information security program management, security audits, PCI, PII and CCPA/GDPR assessments. He is also well versed in CMMC and NIST regulations and assessment techniques and general audit readiness practices.

Jon Helmus, Senior Penetration Tester – *CEH, Security+, PenTest+, CVNP*
Jonh@rsisecurity.com
10 Years Experience
Jon Helmus has over 10 years of professional experience in vulnerability assessments, penetration testing, and related consulting and mentoring, as well as a masters degree in cybersecurity. In addition to his active role as a senior penetration tester and subject matter expert for RSI Security, he also serves as an adjunct professor on the topic for the University of Seattle, National University, and Metropolitan State University.

Describe how your company will market this contract if awarded. Describe how you intend to introduce NCPA to your company.

RSI Security will make every effort to market, promote, and communicate the benefits of a contract award to current and future potential NCPA members nationwide.

RSI Security client partnerships are featured prominently on the RSI Security website, and any contract award with NCPA, would be similarly promoted to advertise our client partnership. In addition, all applicable contract terms and conditions, services offered, and ordering information for NCPA members will be displayed prominently on the RSI Security website.

Because of the nature of the cooperative agreement, RSI Security would also provide information for NCPA members specific to the services provided as part of this agreement and instructions for reaching the appropriate RSI and NCPA members to pursue task order award. The RSI Security website is designed using search engine optimization principles to help ensure effective advertisement of the contract and client-provider relationship as well as to highlight RSI Security as a viable source of the desired services.

Following the contract award, RSI Security will issue a press release and customer outreach mailing announcing the award and advertising the services provided to NCPA members to our existing mailing list, as well as to a standard nationwide mailing list of NCPA professionals. Regular outreach email blasts to NCPA members that highlight services provided and capabilities covered within the cooperative agreement will also be generated and distributed at a frequency agreeable to NCPA. In addition, we will feature this new partnership on our RSI Security blog, which has over 40,000 visitors per month.

RSI Security is capable of producing full-color advertisements in electronic format that are tailored to content specifically appropriate for NCPA members. Advertisements will include company and NCPA logos, as well as current contact information for ordering.

Describe your firm's capabilities and functionality of your on-line catalog / ordering website.
Not Applicable
RSI Security is proposing the provision of IT security services only.

Describe your company's Customer Service Department (hours of operation, number of service centers, etc.)
Once a member accepts a proposal, the onboarding process begins by issuing a welcome email to the client. If not already provided upon signature, a purchase order will be requested in order to schedule the engagement start date. Once payment is received, a project manager will schedule a kickoff call with the client and or client's team to introduce the project team and review the overall engagement. A request for information will follow which typically includes technical diagrams and network details. The project manager sets a series of weekly or bi-weekly meetings for the length of the project term.

Our client services are provided by the Technical Operations team for managed service clients and the Technical Advisory and Consulting team for professional service clients. Both teams are equipped with technologies, processes and people to respond and resolve all client service issues. All issues can be submitted to support to meet the 24-hour response time and appropriate resolution time depending on SLA and the nature of the issue. Both teams track lagging and leading indicators of client satisfaction to stay proactive and improve continuously. If RSI receives a complaint, it is immediately escalated to upper management for resolution.

Green Initiatives (if applicable)

RSI Security is committed to increasing its efforts toward a sustainable, low-waste future. We are striving to continually improve our environmental sustainability and waste reduction and to initiate additional projects and activities that will further our goal of reducing our overall impact.

Our commitment to the environment extends to our customers, our staff, and the community in which we operate. We are committed to the following:

- Complying with all applicable environmental regulations;
- Preventing pollution whenever possible, and recycling everything possible;
- Training all of our staff on our sustainability program and encouraging them to contribute and participate;
- Communicating our environmental commitment and efforts to our customers, staff, and our community; and
- Continually improving over time by striving to measure our environmental impacts and by setting goals to reduce these impacts each year.

Anti-Discrimination Policy (if applicable)

RSI Security is an equal opportunity employer and makes employment decisions on the basis of merit. We want to have the best available persons in every job. Company policy prohibits unlawful discrimination based on: race, color, religion, religious creed (all aspects of religious beliefs, observance or practice, including religious dress and grooming practices), national origin, ancestry, citizenship, physical or mental disability, medical condition (including cancer and genetic characteristics), genetic information, marital status, sex (including pregnancy, childbirth, breastfeeding, or related medical conditions), gender, gender identity, gender expression, age (40 years and over), sexual orientation, veteran and/or military status (including members or veterans of the United States Armed Forces, United States Armed Forces Reserve, the United States National Guard, and the California National Guard), protected medical leaves (requesting or approved for leave under the Family and Medical Leave Act or the California Family Rights Act), domestic violence victim status, political affiliation, and any other status protected by local, state or federal law. It also prohibits unlawful discrimination based on the perception that anyone has any of those characteristics, or is associated with a person who has or is perceived as having any of those characteristics. Discrimination can also include failing to reasonably accommodate religious practices or qualified individuals with disabilities where the accommodation does not pose an undue hardship. All such discrimination is unlawful.

Equal Employment Opportunity applies to all personnel practices, including but not limited to recruitment, hiring, training, promotion, compensation, benefits, transfers, educational assistance, and social and recreational activities. RSI Security is committed to compliance with all applicable laws providing equal employment opportunities. This commitment applies to all persons involved in Company operations and prohibits unlawful discrimination by any employee, including supervisors, managers, and coworkers. If you wish to report discrimination on any of the protected classes above, please reach out to the Human Resources team.

Vendor Certifications (if applicable)

In addition to our business certificates provided on the following pages, our personnel maintain certifications and expertise in regulatory frameworks with fundamental certifications, including:

POST IN CONSPICUOUS PLACE OR KEEP ON PERSON

CITY OF SAN DIEGO * CERTIFICATE OF PAYMENT OF BUSINESS TAX

RSI SECURITY
10531 4S COMMONS DR #527
SAN DIEGO CA 92127-3517

Certificate Number: B2015016565

Business Name: RSI SECURITY
Business Owner: RAYNA KIM
Business Address: 10531 4S COMMONS DR #527
SAN DIEGO CA 92127-3517

Primary
Business Activity: INFORMATION & DATA PROCESSING SERVICES

Secondary
Business Activity: MANAGEMENT OF COMPANIES & ENTERPRISES

Effective Date: 01/01/2020
Expiration Date: 12/31/2020

PLEASE NOTIFY THE CITY TREASURER'S OFFICE IN WRITING OF ANY CHANGE IN OWNERSHIP OR ADDRESS – PLEASE SEE REVERSE SIDE FOR ADDITIONAL INFORMATION

BUSINESS FILE COPY

CITY OF SAN DIEGO
CERTIFICATE OF PAYMENT OF BUSINESS TAX
PO BOX 122289, SAN DIEGO, CA 92112-2289
1200 3RD AVENUE, MS 51T, SAN DIEGO, CA 92101
(619) 615-1500; FAX (619) 533-3272
www.sandiego.gov/treasurer

RSI SECURITY
10531 4S COMMONS DR # 527
SAN DIEGO, CA 92127-3517

000614

Certificate Number: B2015016565 PIN: GDL4V

Business Name: RSI SECURITY
Business Owner: RAYNA KIM
Business Address: 10531 4S COMMONS DR #527
SAN DIEGO CA 92127-3517

Primary
Business Activity: INFORMATION & DATA PROCESSING SERVICES

Secondary
Business Activity: MANAGEMENT OF COMPANIES & ENTERPRISES

Effective Date: 01/01/2020
Expiration Date: 12/31/2020

Mailing Address: RSI SECURITY
10531 4S COMMONS DR #527
SAN DIEGO CA 92127-3517

This certificate acknowledges payment of business taxes pursuant to the San Diego Municipal Code. This **is not** a License to do business within the City of San Diego in violation of any section of the Municipal Code or regulation adopted by the City Council including, but not limited to: Zoning restrictions; Land Use specifications as defined in Planned Districts, Redevelopment areas, Historical Districts, or Revitalization areas; Business Tax Regulations; Police Department Regulations; and Fire, Health or Sanitation Permits and Regulations.

This document is issued without verification that the payer is subject to or exempt from licensing by the State of California.

Payment of the required tax at the time or times due is for the term and purpose stated and is pursuant to City Ordinance. Please refer to delinquency information under "Notice".

NOTICE: It is the responsibility of the certificate holder to renew this certificate of payment of business tax within the proper time limits. Failure to do so, even if you have not received a renewal notice, will result in the assessment of a penalty. Please note your expiration date on this certificate above. The certificate holder is requested to notify the City Treasurer's Office upon sale or closure of the business, change of location, or change of business activity.

The tax or fees collected are **Not Refundable** unless collected as a direct result of an error by the City of San Diego.

This certificate is NOT transferable for a change in business ownership.

See reverse side.

State of California
Secretary of State

CERTIFICATE OF STATUS

ENTITY NAME:

RSI SYSTEMS INC.

FILE NUMBER:	C3589345
FORMATION DATE:	07/19/2013
TYPE:	DOMESTIC CORPORATION
JURISDICTION:	CALIFORNIA
STATUS:	ACTIVE (GOOD STANDING)

I, ALEX PADILLA, Secretary of State of the State of California, hereby certify:

The records of this office indicate the entity is authorized to exercise all of its powers, rights and privileges in the State of California.

No information is available from this office regarding the financial condition, business activities or practices of the entity.

IN WITNESS WHEREOF, I execute this certificate and affix the Great Seal of the State of California this day of May 03, 2018.

ALEX PADILLA
Secretary of State

Tab 5 – Products and Services / Scope

RSI Security is pleased to offer a broad ranging suite of IT security and compliance consulting services.

Cyber Security Services

- Cybersecurity Posture Analysis
- Gap analysis & remediation based on Cybersecurity standards
- Incident Management
- Incident response
- Risk Assessment
- IT Security & Cyber awareness training
- Policy Documentation

Testing Services

- Penetration Testing
- Threat Management
- Vulnerability Management
- PII Scanning & Identification
- CC Scanning & Identification
- Incident Response Readiness

Compliance & Advisory

- PCI DSS / PCI ASV
- HIPAA / HITECH
- HITRUST
- SOC 2
- NERC CIP
- FISMA / NIST 800-171 / CMMC
- CCPA / GDPR
- SEC / FINRA
- 3rd Party Risk Management

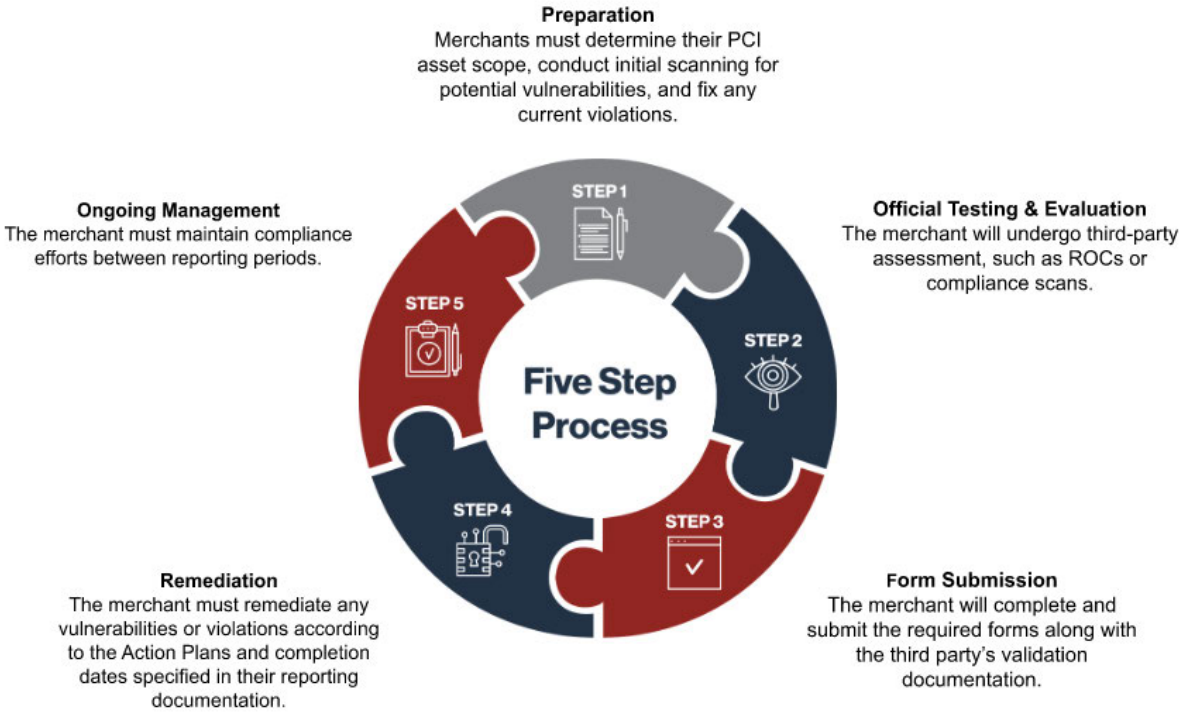
PCI DSS Consulting and Assessment

Our compliance advisory services operate on a collaborative model. We work closely with your team to prepare for a clean, smooth audit. That includes full-scale implementation and top-down initiatives like program design and staff training. The goal is to achieve PCI compliance swiftly and seamlessly, protect cardholder data from unauthorized access, and prevent credit card fraud.

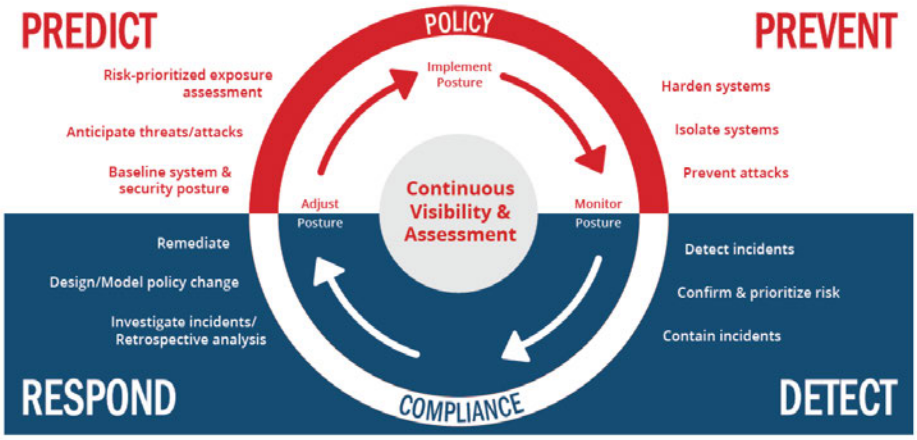
RSI Security will determine NCPA's merchant level and PCI DSS goals and requirements, then will hone the scope of risk | vulnerability assessment and management services and technical solutions to suit the NCPA.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder date 2. Remove vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel



Risk Assessment



RSI Security's assessment service includes cybersecurity measures based on NIST CSF:

- Inventory of authorized and unauthorized devices and software
- Secure configurations for hardware and software
- Continuous vulnerability assessment and remediation
- Controlled use of administrative privileges
- Maintenance, monitoring, and analysis of audit logs
- Email and web browser protections
- Malware defenses
- Limitation and control of network ports
- Data recovery capability
- Secure configurations for network devices
- Boundary defense
- Controlled access based on the need to know
- Account monitoring and control
- Security skills assessment and training / phishing simulations with feedback to admins
- Application software security
- Incident response and management

RSI Security's methodology is based on the interviews and practical evaluation with the key stakeholders and reviewing technical documentation. All the findings are mapped on the NIST CSF standard.

The following activities occur during the engagement:

- **Interviews:** RSI Security will interview key personnel to gain an understanding of how key business drivers are impacted by cybersecurity concerns. Interviews will also be conducted to set expectations and document process baselines for comparison with provided policies, procedures, and assessment results.
- **Documentation Review:** RSI Security's team will evaluate the NCPA's security-related policies and procedures. We will first review to ensure that policies and procedures clearly

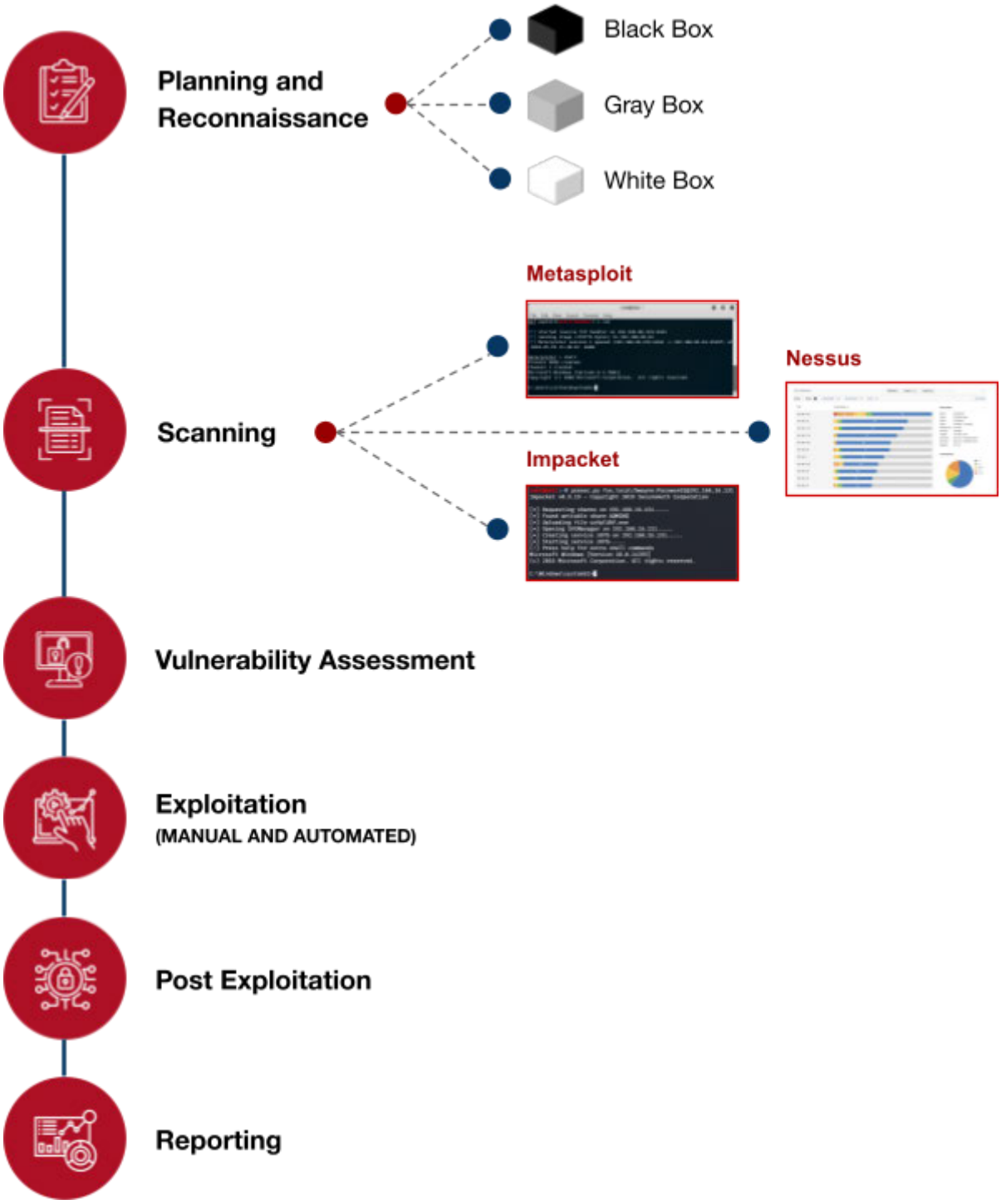
define roles and responsibilities for information security and event management. We will also assess related policies and procedures to ensure they are current, consistent, and reflect the operating environment.

- **Process Review:** RSI Security will evaluate the NCPA's security-related processes to determine overall cybersecurity posture and program maturity. We will then make recommendations on how to improve those processes based on current operational procedures.
- **Evidence Collection:** As directed by RSI Security, the NCPA will provide evidence that shows implementation and maturity of NIST CSF requirements. Evidence will be assessed against the Capability Maturity Model (CMM) to determine the NCPA's process and implementation maturity.
- **Creation of Current-State and Target-State Profiles:** RSI Security will identify the requirements that define the current state of the NCPA's cybersecurity program through the establishment of a current-state profile. The current-state profile will include an evidence-based evaluation of maturity and will be used to inform a risk-based target-state profile. The target-state profile focuses on the assessment of the framework categories and subcategories describing the NCPA's desired cybersecurity outcomes.

Vulnerability Assessment and Penetration Testing

RSI Security regularly performs mid- and large-scale security assessments and penetration testing for clients in the private and public sectors, including several NCPA entities. Our penetration testing that aligns with standards, regulatory frameworks, and best practices, including CIS Critical Security Control 18, NIST SP 800-115, MITRE ATT&CK, and the Cyber Kill Chain.

We employ a suite of proprietary knowledge and private and publicly available tools. Our process runs deep and comprehensive:



RSI Security penetration testers employ a client-tailored blend of automated and manual tools to ethically exploit networks. They will:

Risks and vulnerabilities will be logged, ranked, and scored. First-class reporting will include recommendations for budget-sensitive remediations.

In addition to the above processes and procedures, vulnerability assessments associated with this engagement will specifically result in the following deliverables:

- A listing of IPs and devices assessed
- A gap analysis of each device/IP versus best practices
- Recommended steps to cure gaps found
- A comparison with previous year assessments to record progress

Incident Response, Continuity of Operations, and Disaster Recovery Planning

In the confirmed event of an incident, RSI Security will support and advise the NCPA through the incident response lifecycle. If the incident is complex and requires additional services (ad hoc services), RSI Security will provide the NCPA with our base support and guidance services and provide the NCPA with an incident response plan (IRP). These services are available to all RSI Security clients regardless of size. Our base services cover triaging and handling of an incident.

Responding to reported incidents quickly and efficiently is paramount in containing incident effects to users, limiting exposure, stemming losses, and preserving evidence. An incident can

lead to data loss and costly fines, as well as damage to an organization's brand and reputation. RSI Security has many years of incident response expertise and seasoned experience responding to hundreds of data security incidents.

RSI Security incident response includes:

- General systems outage incident troubleshooting and diagnosis
- Network and application intrusion analysis
- Incident response readiness training
- Incident response plan development
- Retained forensics services
- Emergency breach response
- Network and application intrusion analysis
- Documentation summarizing the incident and resolutions taken
- Associated technical reports documenting incidents, technical findings, recommendations, and mitigation implementation progress

Our disaster recovery, incident response planning, and management process consists of the following:

- **Incident Identification**
  RSI Security's incident management team will bring the right technology and expertise to clearly identify any breaches or incidents.
- **Incident Logging**
  Once an incident has been detected, RSI Security will help audit the NCPA's critical systems to ensure proper logging and tracking.
- **Investigation and Diagnosis**
  We then investigate how the incident took place and what was affected. This stage diagnoses exactly what went wrong.
- **Assignment or Escalation**
  Depending on the incident, tasks and responsibilities will be allocated or escalated to solve the problem efficiently.
- **Resolution and Closure**
  Once the incident has been responded to and remediated, we help close out the case and implement preventative measures.
- **Customer Satisfaction**
  Incidents can have a massive impact on customer satisfaction and brand image. We help minimize negative impacts.

Incident, Threat, and Vulnerability Management
RSI Security works with clients to ensure that all incident management program best practices are being applied and followed. Whether it's on-premise or cloud-based incident management, we help implement core incident management best practices:

- **Incident Lifecycle Management**
  Determine the nature and status of the incident, determine the problem priority and manage the issue until resolution
- **Enforcement of Standardized Processes**
  Hold each stakeholder in the incident management program accountable with standardized processes for optimal problem management
- **Classification and Prioritization**
  Detect what systems or services are impacted and determine whether the effects are strictly internal or customer facing
- **Automation and Escalation**
  Work with our clients' service desk incident management teams to ensure that the most current technology is used and enable staff to escalate identified issues to the right people as quickly as possible.

Security Awareness Training

No matter how much you spend, no matter how complex the technology, no matter how rigorous or punitive the compliance requirements are, investments in technical cybersecurity mitigation measures by themselves will never be enough.

Even if your cybersecurity defenses in place stop 99.9% of all attempted data breaches, it can take just a single click on a malicious link by a distracted employee, such as through phishing emails, to lock up your entire system or to introduce damaging viruses.

As much faith as we have in our employees to be vigilant against cyber threats, responsible companies must plan for lapses and put in place rigorous and ongoing training and awareness programs.

One-Time Training Isn't Enough

It's not enough to put new and existing employees through a one-hour security training session (perhaps mingled with company history videos, performance expectations, harassment training, etc.) and expect perfect execution to counter potential hacks or damaging security incidents. In the course of a busy work day, a very official-looking email could come in from a spoofed executive account, "authorizing" the release of funds, or requesting a password or special phrase.

Continuous Security Awareness Training

Data breach tactics evolve in sophistication every day, so we all need to be kept aware of threats in general as well as how threats might present themselves. To help keep our clients informed of the threats of today (and tomorrow), RSI offers comprehensive web-based security awareness training that integrates formal training programs with mock phishing attacks that simulate the look and feel of a real social engineering attack.

Given the potential damage of a breach, security concerns need to stay top of mind for everyone in your organization, our mock attacks are deployed at random, in various forms. If the employee falls for one of these simulated attacks, an administrator is informed, setting up an opportunity for further training and to understand the broader context of why the breach was made possible.

Was the employee simply distracted? Was the attack messaging type new and unique? Was it guised in official-looking documents such as a Microsoft Word file? Was it a link hidden in a FedEx tracking email? Our training programs provide valuable metrics to company administrators to understand their specific threat attack surface, and can provide insights on how to proactively counter future breach attempts and keep sensitive data away from those with unauthorized access.

Our Training Program includes the following services:

- Unlimited Phishing Security Tests
- Automated Security Awareness Program
- Security “Hints & Tips”
- Training Access Level I
- Automated Training Campaigns
- Crypto-Ransom Guarantee
- Phish Alert Button
- Phishing Reply Tracking
- Active Directory Integration
- Training Access Level II
- Monthly Email Exposure Check
- Vishing Security Test
- Smart Groups
- Social Engineering Indicators
- EZXploit™ - “Automated Human Pentesting”
- USB Drive Test
- Vulnerable Browser Plugin Detection
- Priority Level Support
- Training Access Level III
- AIDA™ Artificial Intelligence-driven Agent BETA

Security Software

All of the services and software below are included in the total proposed pricing.

Solutions	Services/Software/Third-Party Agreement
Penetration Testing	
External Network Internal Network Web App Social Engineering	Rapid7 Qualys Groundlabs Darktrace Redwood (internal GRC tool) - https://redwood.rsisecurity.com TCT Kali Linux Netcat, Hydra Burp Suite Professional Dirbuster ZAP proxy Armitage Kali Linux operating system Wireshark SSLSCAN Nmap Nessus Metasploit framework Acunetix SQL tools Paros proxy KnowBe4
Vulnerability Assessment	
External	Qualys
Internal	Qualys
Virtual Appliance for Internal VA Scan	Qualys
Assessment Report	
Policies, Procedures and Standards	Nipper Apptega Connectwise Automate
Network Device Configurations (core, edge)	
Network Architecture	

Wireless Infrastructure and Configuration	Sophos TCT portal Redwood portal Qualys Cloud Agent
Firewall Configuration	
VPN Configuration	
DMZ Configuration	
Server Environment and Configurations	
VMware Virtual Environment	
Data and Information Security	
VoIP Environment and Configuration	
Mobile Devices	
Desktop and Laptop Configurations	
Physical Security	
Cyber Resilience Program Documentation	
Project Management Systems	RSI Mavenlink (https://rsi.mavenlink.com) Google Drive
Implementation Plan	
Project Management Systems	RSI Mavenlink (https://rsi.mavenlink.com) Google Drive
Project Management	
Project Management Systems	RSI Mavenlink (https://rsi.mavenlink.com) Google Drive
Security Awareness Training	
Training Software	KnowBe4

Tab 8 – Value Added Products and Services

Technical Documentation Services

RSI Security's technical writing services | streamline all your internal cybersecurity documentation needs. Unlike many of our competitiors, RSI Security provides deep domain expertise in all facets of cybersecurity defense, compliance, and certifications. We'll work closely with your team to determine what kind of technical writing you require and produce clear, accurate documentation when you need it.

Our technical writing and online proofreading services are staffed by a technical writing team who is accustomed to researching, supporting, and writing documentation to support a wide array of cybersecurity initiatives. Our team will talk with your subject matter experts, business leaders, and IT staff during the preparation stage. We'll ask the right questions, get clarity on what your exact needs are, and produce a quality finished product that speaks to the right audience.

Whether it's a breach response plan, training materials, or operating manuals, RSI Security's business technical writing services help make sure your entire organization is on the same page with the right documentation. When it comes to cybersecurity, communication and coordination are key, and that's what our technical writing services are designed to enable. Our technical writing services include:

Audit Report Writing

RSI Security's professional audit report writing services will ensure clear, professional communications with the necessary regulatory bodies and agencies. Whether it's regulations and compliance in finance, healthcare, or military contracting, audit report writing is simply a fact of life. Let our experienced, professional technical writing staff execute your audit report writing quickly and painlessly.

Documentation Writing

Writing technical documentation for software and cybersecurity is one of the core capabilities of RSI Security's technical writing team. Take documentation writing off your plate by partnering with RSI Security, and get your entire team on the same page with a single source of documentation to reference.

Policy Writing

Every company needs internal policies written and documented in a clear, concise, professional fashion. This is especially true in cybersecurity, where internal policies can often determine whether or not your critical data and systems are vulnerable to hackers and cybercriminals. Use RSI Security's compliance policy writing services to not only ensure your internal staff takes the

right security measures, but to also rest easy knowing that you have the proper documentation to show regulatory agencies, should the need arise.

Business Technical Writing

Business and technical writing can be a challenge for many organizations without proper internal expertise, experience, and resources. Whether it's marketing materials explaining your highly technical service offerings or communications with regulatory bodies, every organization needs the capaNCPA to convey highly technical concepts in a business-friendly manner. RSI Security's business writing services will help you distill even the most complex topics and concepts into clear, powerful communications.

Online Proofreading Services

When it comes to any sort of technical writing or documentation, it's always good to have a second pair of eyes to review the content. RSI Security's online proofreading services can review all of your technical writing and documentation for accuracy, clarity, and conciseness. We'll assign you the right remote technical writer who will ensure all of your documentation is correct and as powerful as possible.

IT Architecture

RSI Security can help your organization by augmenting your IT department with qualified and skilled team members to handle your next cloud architecture implementation or setting up a secure network with the most up-to-date best practices.

RSI Security's IT architecture services are designed to create a flexible, secure IT environment that meets the needs of each individual business. Our IT architecture services:

- Enhance cybersecurity risk management
- Improve overall cyber defense posture
- Increase ease of regulatory compliance
- Help achieve strategic business goals
- Create a secure BYOD work environment
- Boost system performance and reliability

Our team is broadly skilled and can help you even in the most complex of environments and support your organization in any technology it uses.

Our IT Architecture Implementation Services include:

- **Cloud Architecture**
  Our cloud architecture implementation services will help you protect critical information, even when it's not in your hands. Whether it's data at rest or in motion to or from the cloud, RSI Security will help you implement a secure architecture.

- **Network Architecture**
  RSI Security's network architecture implementation services will work hand-in-hand with your IT team to secure your network. We'll assess the security of your network at present, and come up with an improved architecture to meet your needs.
- **Endpoint Security**
  By choosing RSI Security's endpoint security implementation services, you'll seal off any potential entry points that hackers might seek to exploit. We'll conduct penetration testing, help erect firewalls and seal off endpoints from cybercriminals.
- **Mobile Security**
  Mobile Security Architecture implementation services from RSI Security will allow your business to safely function in a mobile environment. Whether it's field service workers or work from home, we'll help secure your entire enterprise mobile ecosystem.
- **Enterprise Architecture**
  Enlist our enterprise architecture services if you're a large company, business or organization. Even small and medium businesses that plan to scale need to consider how their cybersecurity posture will change as their business grows and scales.
- **Application Development**
  Web and other applications are often a target for cybercriminals. RSI Security's team will assist you in application development that's in alignment with a robust cybersecurity posture. Create applications that are both safe and effective.

Cloud Computing Security Services

From restricting physical systems access to bolstering third-party security, at RSI Security we'll work with you to develop a flexible, scalable approach to ensuring your data is secure in the cloud. Our suite of Cloud-Based Security Services includes:

- Protection against Internal and External Threats Comprehensive Threat Monitoring and Analytics
- Timely Threat Detection, Response, and Remediation
- AWS
- Azure
- Office365 Google Cloud Platform
- Cost-effective, Flexible, and Scalable Protection
- Cloud Architecture Assessment and Build
- Security Governance Strategy and Audits
- Identity and Access Management
- Vulnerability Assessments and Management
- Patch Management
- Web Application Security

Tab 9 – Required Documents

RSI Security acknowledges receipt and acceptance of all required documents incorporated into this solicitation. Our required signature forms are on the following pages.

FEDERAL REQUIRED SIGNATURES

Offeror certifies compliance with all provisions, laws, acts, regulations, etc. as specifically noted in the pages above. It is further acknowledged that offeror agrees to comply with all federal, state, and local laws, rules, regulations and ordinances as applicable.

Offeror	RSI Systems Inc., DBA RSI Security
Address	10531 4S Commons Drive, Suite 527
City/State/Zip	San Diego, CA 92127
Authorized Signature	
Date	11/16/2022

ANTITRUST CERTIFICATION STATEMENTS
TEXAS GOVERNMENT CODE § 2155.005

I affirm under penalty of perjury of the laws of the State of Texas that:

(1) I am duly authorized to execute this contract on my own behalf or on behalf of the company, corporation, firm, partnership or individual (Company) listed below;

(2) In connection with this bid, neither I nor any representative of the Company has violated any provision of the Texas Free Enterprise and Antitrust Act, Tex. Bus. & Comm. Code Chapter 15;

(3) In connection with this bid, neither I nor any representative of the Company has violated any federal antitrust law; and

(4) Neither I nor any representative of the Company has directly or indirectly communicated any of the contents of this bid to a competitor of the Company or any other company, corporation, firm, partnership or individual engaged in the same line of business as the Company.

Company Name	RSI Systems Inc., DBA RSI Security
Address	10531 4S Commons Drive, Suite 527
City/State/Zip	San Diego, CA 92127
Telephone Number	858.999.3030
Fax Number	858.225.6190
Email Address	bids@rsisecurity.com
Printed Name	John Shin
Title	Managing DIrector
Authorized Signature