Proposal to NCPA

Cyber-Security Solutions, Malware, Ransomware Protection, Other Related Products and Services

Solicitation Number: RFP #34-21

November 18, 2021

Empower Results®

November 18, 2021

To whom it may concern:

Thank you for giving Aon Cyber Solutions the opportunity to share its capabilities and discuss how those would be put to work for NCPA members interested in our enterprise focused cyber risk management program. In this material, we have intentionally focused on Aon Cyber Solution's unique ability to provide an integrated, superior cyber risk management program to NCPA members.

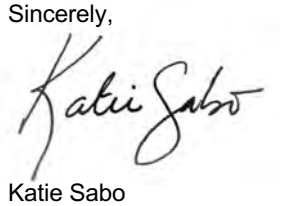
Aon is not just an insurance broker of cyber. We realized years ago that cyber was an unusually complex and growing risk for our clients and that they needed more than traditional broking. In 2016, Aon acquired a leading incident response/forensic cyber firm: Stroz Friedberg. Staffed with leading cyber experts from federal law enforcement and experts in emerging technology vulnerabilities, Stroz Friedberg could have easily continued to grow its business without being part of Aon. However, their leaders and ours saw a bigger opportunity: the chance to use cyber expertise to help clients deeply identify their vulnerabilities, quantify associated financial and reputational risk, protect against attacks and support successful incident response and recovery needs.

The success of this approach has been tremendous. As the world faces more threat actors and greater exposure, Aon Cyber Solutions is engaged to help public and private sector organizations manage cyber risk with greater certainty and better outcomes.

We welcome the chance to introduce our team and have you speak with our references about the results we deliver. Most of all, we look forward to learning more about NCPA programs.

Again, we appreciate this opportunity to respond to NCPA's request and look forward to growing our relationship with you.

Sincerely,



Katie Sabo

State and Local Leader
Aon Public Sector Partnership

Table of Contents

Executive Summary

The National Cooperative Purchasing Alliance (NCPA) is a leading national government purchasing cooperative working to reduce the cost of goods and services by leveraging the purchasing power of public agencies in all 50 states. NCPA utilizes state of the art procurement resources and solutions that result in cooperative purchasing contracts that ensure all public agencies are receiving products and services of the highest quality at the lowest prices.

Aon is a leading global professional services firm providing advice and solutions in Risk, Wealth (Retirement and Investments) and Health to both public and private sectors clients. Aon develops insights that reduce the risks our public sector clients face.

Aon Cyber Solutions was created in 2016, redefining the cyber security services market by joining forces with the industry's leading providers, Stroz Friedberg, LLC and Gotham Digital Science (GDS). Aon acquired Stroz Friedberg November 2016, who acquired GDS in April 2016. Together, Aon Cyber Solutions is a global leader in the field of cybersecurity, with leading experts in incident response, security science, investigations, eDiscovery, digital forensics, and due diligence.

Aon's National Public Sector practice has been working with the public sector since 1979, providing risk management services to public sector clients nationwide. Among them are more than 30 state governments, and thousands of local municipalities (including hundreds of counties and cities). Our group is one of the largest public sector risk management service providers locally and worldwide. Initiated over 25 years ago, our specialized practice serves thousands of municipal, governmental, and quasigovernmental authorities and other organizational groups.

Together, we the only firm that can manage cyber risks proactively and reactively across the entire cyber ecosystem and through the insurance lifecycle for public sector governments and agencies.

We understand that NCPA utilizes state of the art procurement resources and solutions that result in cooperative purchasing contracts that ensure all public agencies are receiving products and services of the highest quality at the lowest prices.

Mindful of these imperatives Aon brings an approach that will enable NCPA members to engage with a firm that provides enterprise-wide cyber identification, protection, detection, recovery and response activities to create the best protections for taxpayers.

In the following pages, we will present our integrated offerings. The key elements will include:

Seek – Identify

We applied our deep experience handling some of the largest, most difficult cyber investigations to create a framework that includes tooling and scanning to help identify and assess an entities attack vector, attacker techniques and indicators, and provide ongoing visibility into risk exposure.

Aon's modeling is proprietary and leverages leading industry knowledge and data — not out-of-the-box - that can be tailored to the Trust's unique needs. Our work product will include cyber aggregation risk, identification, and quantification the exposure to cyber risk and model probable risk scenarios, delivering data to effectively manage your financial and operational risk from a cyber event.

Shield – Protect

Aon Cyber Security protection products and services are designed to holistically address the critical controls that help protect and mitigate ransomware attack vectors. Aon's Cyber Solutions specializes in performing a range of

security testing services including network penetration testing, application security testing, source code review, social engineering assessments e.g., phishing & vishing campaigns, and physical penetration testing.

Core to Aon's Cyber Solutions security testing approach are test cases and testing techniques that require execution by highly skilled security engineers. Automated assessment techniques, proprietary Security Directives, and the use of premier proprietary, commercial, and open-source assessment tools in a consistent and repeatable process supplement manual testing. This approach ensures every Aon assessment maximizes depth and breadth of vulnerability coverage.

Solve – Detect, Respond and Recover

Aon is ready to help when a cyber-attack occurs. Our experts are poised to help limit business/service interruption, ensure recovery, and expedite claims preparation. In addition, we can preserve digital evidence required for reporting purposes or in the event of legal action, and we can act as expert witnesses during regulatory proceedings or litigation.

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

- Proposals should address each of the following:
  - 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

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 of any kind of government of the United States or any civil or military authority; insurrections; riots; epidemics; 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.

Miscellaneous

- 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.

Products and Services additions

- Products and Services may be added to the resulting contract during the term of the contract by written amendment, to the extent that those products and 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

- The estimated dollar volume of 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. There is no guarantee or commitment of any kind regarding usage of any contracts resulting from this solicitation.

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.

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.
- Provide both On-premise solutions as well as Cloud based solutions.

References (15 points)

- A minimum of ten (10) customer references for product and/or services of similar scope dating within past 3 years

Technology for Supporting the Program (10 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

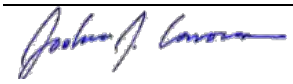
Value Added Services Description, Products and/or Services (10 points)

- Marketing and Training
- Minority and Women Business Enterprise (MWBE) and (HUB) Participation
- Customer Service

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

Company Name	Stroz Friedberg, LLC (Aon Cyber Solutions)
Address	One Liberty Plaza; 165 Broadway
City/State/Zip	New York, NY 10006
Telephone No.	212-903-2813
Fax No.	
Email Address	Joshua.Larocca@aon.com
Printed Name	Joshua J. Larocca
Position with company	Senior Managing Director
Authorized Signature	

Stroz Friedberg LLC has incorporated its standard terms and conditions in the Appendix of this proposal.

Tab 2. NCPA Administration Agreement

As required by the RFP, Stroz Friedberg, LLC agrees to execute the required Administration Agreement at time of award.

This Administration Agreement is made as of **December 13, 2021** by and between National Cooperative Purchasing Alliance ("NCPA") and **Aon Cyber Solutions (Stroz Friedberg, LLC.)** ("Vendor").

Recitals

WHEREAS, Region 14 ESC has entered into a certain Master Agreement dated **December 13, 2021**, referenced as Contract Number 01-129, 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 Cyber-Security Solutions, Malware, Ransomware Protection, Other Related Products and Services ;

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 Tab 1 and incorporated herein by reference as though fully set forth herein, and the terms and conditions contained therein shall apply to this Agreement except as expressly changed or modified by this 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 Agreement including, but not limited to, the Vendor's obligation to provide appropriate insurance and certain indemnifications to Region 14 ESC.
- Vendor 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 Vendor 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 Public 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 Vendor, Region 14 ESC, or such Public Agency, (b) shall not be obligated, liable or responsible (i) for any orders made by Region 14 ESC, any Public Agency or any employee of Region 14 ESC or Public 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 Public 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 Public Agency, or any employee of Region 14 ESC or Public Agency under this Agreement or the Master Agreement.

- The Public Agency participating in the NCPA contract and 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 Public Agency and Vendor. NCPA, its agents, members and employees shall not be made party to any claim for breach of such agreement.

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.

General Provisions

- This 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 Agreement which is not contained herein shall be valid or binding.
- Awarded vendor 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 contract by awarded vendor must have prior approval from NCPA.
- If any action at law or in equity is brought to enforce or interpret the provisions of this 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 Agreement nor any rights or obligations hereunder shall be assignable by Vendor without prior written consent of NCPA, provided, however, that the Vendor may, without such written consent, assign this 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 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 Agreement.
- This 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
- All written communications given hereunder shall be delivered to the addresses as set forth below.

National Cooperative Purchasing Alliance:		**Vendor:**	Stroz Friedberg LLC
Name:	Matthew Mackel	Name	Thomas J. Hibarger
Title:	Director, Business Development	Title:	Senior Managing Director
Address:	PO Box 701273	Address:	2001 K Street, NW, Suite 625
	Houston, TX 77270		Washington, DC 20006
Signature:		Signature:	
Date:	December 13, 2021	Date:	January 5, 2022

Tab 3. Vendor Questionnaire

1. States Covered

Bidder must indicate any and all states where products and services can be offered.

Please indicate the price co-efficient for each state if it varies.

State Matrix *(x indicates where we are able to sell our services a blank indicates where we are unable to sell our services)*	Products & Solutions					
	Cyber Assessments	Cyber Security Testing	Due Diligence & Background Investigations	Simulations, Protection Planning and Development Tools	Aon Cyber Solutions Detect, Response and Recovery Solutions EXCLUDING Incident Response and Digital Forensics	Aon Cyber Solutions Detect, Response and Recovery Solutions INCLUDING Incident Response and Digital Forensics
Alabama	X	X	X	X	X	
Alaska	X	X	X	X	X	
Arizona	X	X	X	X	X	X
Arkansas	X	X	X	X	X	
California	X	X	X	X	X	X
Colorado	X	X	X	X	X	X
Connecticut	X	X	X	X	X	X
Delaware	X	X	X	X	X	X
District of Columbia	X	X	X	X	X	X
Florida	X	X	X	X	X	X
Georgia	X	X	X	X	X	
Hawaii	X	X	X	X	X	
Idaho	X	X	X	X	X	X
Illinois	X	X	X	X	X	X
Indiana	X	X	X	X	X	X
Iowa	X	X	X	X	X	
Kansas	X	X	X	X	X	X
Kentucky	X	X	X	X	X	X
Louisiana	X	X	X	X	X	
Maine	X	X	X	X	X	X
Maryland	X	X	X	X	X	X
Massachusetts	X	X	X	X	X	X
Michigan	X	X	X	X	X	X
Minnesota	X	X	X	X	X	X
Mississippi	X	X	X	X	X	X
Missouri	X	X	X	X	X	
Montana	X	X	X	X	X	X
Nebraska	X	X	X	X	X	
Nevada	X	X	X	X	X	X
New Hampshire	X	X	X	X	X	X
New Jersey	X	X	X	X	X	X
New Mexico	X	X	X	X	X	
New York	X	X	X	X	X	X
North Carolina	X	X	X	X	X	X
North Dakota	X	X	X	X	X	
Ohio	X	X	X	X	X	X
Oklahoma	X	X	X	X	X	
Pennsylvania	X	X	X	X	X	X
Rhode Island	X	X	X	X	X	X
South Carolina	X	X	X	X	X	
South Dakota	X	X	X	X	X	X
Tennessee	X	X	X	X	X	X
Texas	X	X	X	X	X	X
Utah	X	X	X	X	X	
Vermont	X	X	X	X	X	
Virginia	X	X	X	X	X	X
Washington	X	X	X	X	X	X
West Virginia	X	X	X	X	X	
Wisconsin	X	X	X	X	X	X
Wyoming	X	X	X	X	X	X
Territories						
American Samoa	X	X	X	X	X	
Federated States of Micronesia	X	X	X	X	X	
Guam	X	X	X	X	X	
Midway Islands	X	X	X	X	X	
Northern Marina Islands	X	X	X	X	X	
Puerto Rico	X	X	X	X	X	
U.S. Virgin Islands	X	X	X	X	X	

Please indicate the price co-efficient for each state if it varies.

No co-efficient used

2. 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 is a M/WBE ☐

Historically Underutilized Business

Respondent Certifies that this firm is a HUB ☐

3. Residency

Responding Company's principal place of business is in the city of New York City, State of New York.

Aon Cyber Solutions
Stroz Friedberg, LLC.
One Liberty Plaza
165 Broadway, #3201
New York, NY 10006

4. Felony Conviction Notice

If the 3rd box is checked, a detailed explanation of the names and convictions must be attached.

Please Check Applicable Box;

X	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.

5. 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

[X] Other: Consultant, professional services

6. Processing Information

Provide company contact information for the following:

Sales Reports/Accounts Payable, Purchase Orders, Sales and Marketing

Sales Reports/Accounts Payable

Contact Person: Anita White
Title: Operations Manager – Public Sector Partnership
Company: Aon c/o Aon Cyber Solutions
Address: 200 East Randolph
City: Chicago
State: IL
Zip: 60601
Phone: 312-381-5321
Email: anita.white@aon.com

Purchase Orders

Contact Person: Anita White
Title: Operations Manager – Public Sector Partnership
Company: Aon c/o Aon Cyber Solutions
Address: 200 East Randolph
City: Chicago
State: IL
Zip: 60601
Phone: 312 381 5321
Email: anita.white@aon.com

Sales and Marketing

Contact Person: Katie Sabo
Title: State and Local Leader – Public Sector Partnership
Company: Aon
Address: 200 East Randolph
City: Chicago
State: IL
Zip: 60654
Phone: 312-381-1058
Email: katie.sabo@aon.com

7. 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.

    [X] Yes [ ] No

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

[X] Yes [ ] No

- Vendor will provide additional discounts for purchase of a guaranteed

  [X] Yes [ ] No

8. Cooperatives

List any other cooperative or state contracts currently held or in the process of securing.

Cooperative/ State Agency	Discount Offered	Expires	Annual Sales Volume
None.			

We do not currently have any cooperative and/or statewide contracts for our cyber services

Tab 4. Vendor Profile

Please provide the following information about your company:

Company's official registered name

Stroz Friedberg, LLC. (Aon Cyber Solutions)

Brief history of your company, including the year it was established.

Aon is the leading global professional services firm providing advice and solutions in Risk, Wealth (Retirement and Investments) and Health. Aon develops insights that reduce the volatility our clients face and help them maximize their performance.

Aon Cyber Solutions was created in 2016, redefining the cyber security services market by joining forces with the industry's leading providers, Stroz Friedberg, LLC and Gotham Digital Science (GDS). Aon acquired Stroz Friedberg November 2016, who acquired GDS in April 2016. Together, Aon Cyber Solutions is a global leader in the field of cybersecurity, with leading experts in incident response, security science, investigations, eDiscovery, digital forensics, and due diligence.

Founded in 2000, Stroz Friedberg is an international digital risk management firm specializing in security consulting, digital forensics, electronic discovery, data breach and cybercrime response, due diligence, and investigations. Stroz Friedberg's team includes former federal and state prosecutors and former law enforcement officers with both government and private-sector experience in traditional and cyber-based investigations, digital forensics, data preservation and analysis, infrastructure protection, and electronic discovery. Many of our security consultants, digital forensic examiners, malware analysts, electronic discovery specialists, and private investigators joined Stroz Friedberg following careers in law enforcement, the intelligence community, consulting, and academia.

Aon Cyber Solutions (ACS) brings the following experience and qualifications to NCPA:

Unmatched Experience. We have handled many of the most sensitive and large incident response matters in the US. Based on multiple public listings, we have worked a material portion of the largest public incident response matters in history.

Deep Bench of Expertise. ACS has over 126 technical forensic investigators worldwide,

which we believe to be the largest, most expansive team in the world. We also have 12 technical labs worldwide whereas many competitors have only a handful, or even just one location. ACS has technical labs, not just office addresses, in the U.S., Canada, Europe, the U.K., and Asia. Our Incident Response team is complemented by 246 cyber, investigative, and risk consulting consultants, including Advisory, Testing, Intelligence, Investigations, eDiscovery, Brokerage, and Forensic Accounting, professionals. Having these complimentary services allows us to offer our clients unparalleled vertically integrated cyber risk mitigation solutions, including the ability to resource from these teams for incident response matters.

Training, Certifications, and Awards. Our cyber professionals hold 100+ professional certifications – at least 2 per practitioner. We consistently win team SANS NetWars competitions. Our practitioners include those that train law enforcement e.g., our team include leaders of The International Association of Computer Investigative Specialists (IACIS), including its current President.

Testifying Experience & Board Advisory. Our Cyber team has a deep bench of technical leads and forensic investigators with testifying experience in state and federal courts, along with regulatory and arbitration proceedings. We routinely assist with or provide briefings to executives and Boards related to current cyber security threats, risk assessments findings, and risk maturation.

Company's Dun & Bradstreet (D&B) number

DUNS is 01-761-5464.

Company's organizational chart of those individuals that would be involved in the contract.

A key differentiator for Aon versus others in this space is our "Best in Front" services and industry focused operating model. We believe that assembling the most specialized team together regardless of geography will drive the best results for you and your objectives. This contract will have executive support from Aon Cyber Solutions CEO down to our regional leaders.

Aon Cyber Solutions Leadership Team

North American Leaders:

Christian Hoffman
Chief Executive Officer

Eric Friedberg
Co-President, Stroz Friedberg

Jim Trainor
Senior Vice President

Chad Pinson
President of Engagement

Jay Stampfl
National Sales Leader

Senior Leadership:

Digital Forensics & Incident Response
Orie Hunter
Cheri Char
Sankara Shanmugam

Security Advisory
Beatrice Conner
Nitai Mandhyan

Security Testing
Adam Bixby
Denny Deaton

eDiscovery
Barbara Dunn

Investigations
Sam Willoughby
Danielle Callici
Catrina Kim

Quantification
Adam Peckman

This contract will be supported by subject matter experts from around the U.S. We are proud that every Aon Cyber solution we design, and deliver is backed by the dedication, energy, and resources of Aon Corporation. Below is an illustrative project team that reflect our blended hourly pricing rates.

See roles and descriptions below:

Role	Description	Experience
Senior Project Team Manager and Primary Point of Contact	Areas of expertise will be consulting and project management	20+ years
Senior Cyber Risk Assessor(s)	Areas of expertise include cyber assessment, Enterprise Risk Management governance, assessment, mitigation planning, forecasting and strong understanding of key financial metrics	20+ years
Senior Risk Assessor(s)	Areas of expertise include leading projects for Cyber Quantification (Cyber Impact Analysis), Cyber Security Risk Assessments, and CyQu Evaluations	20+ years
Cyber Impact Analyst(s)	Areas of expertise include leveraging best in class cybersecurity Frameworks to assess risk, maturity, and gaps. Experience in both the public and private sector. Advisor to the U.S. intelligence and special operations community and experience working as an executive consultant with top-tier professional services firms	20+ years
Security Risk Assessor(s)	Areas of expertise include IR Preparedness, Security Operation Capabilities, Crisis Management (BCP/DR), Industrial Resilience (IOT IIOT, ICS), CISO Advisory, Security Culture and Insider Threat Program development, virtual CISO (vCISO) and strategic advisory services, business development support	20+ years
Industry Threat Analyst(s)	Areas of expertise are open, deep and dark web research and analysis for due diligence and threat intelligence, company and individual threat assessments, employee insider risk assessments, data security, workplace misconduct, and financial fraud investigations	10+ years
Account Manager	Areas of expertise include account management activities including, open items, invoicing, stewardship	10+ years

Corporate Office Location
List the number of sales and services offices for states being bid in solicitation.
List the names of key contacts at each with title, address, phone and e-mail address.

Corporate Office
Aon Cyber Solutions
Stroz Friedberg, LLC.
One Liberty Plaza
165 Broadway, #3201
New York, NY 10006

Number of Sales and Services Offices:

Aon Cyber Solutions and Aon affiliates and subsidiaries have offices in nearly every state. As a result, we can provide sales and services across the country.

The key contacts for this contract will be:

Leslie Austin
Senior Director
Public Sector Partnership
2001 K Street, NW
Suite 625 North
Washington, DC 20006
Tel: 202-492-8593
E: leslie.austin@aon.com

Katie Sabo
State and Local Leader
Aon's Public Sector Partnership
200 East Randolph
Chicago, IL 60601
Tel: 312-381-1058
E: katie.Sabo@aon.com

Define your standard terms of payment.

Net 30 days.

Who is your competition in the marketplace?

Aon Cyber Solutions is the only firm that can manage cyber risks proactively and reactively across the entire cyber ecosystem and through the insurance lifecycle.

There are other firms that provide cybersecurity services however none provide the depth and breadth of services and solutions to minimize our clients' overall risks. Firms that focus solely on cybersecurity services may vary in size, and their coverage of services may vary from local, state, regional to national levels. Large firms that have comparable cybersecurity services are Artic Wolf and Paladion Networks.

What differentiates your company from competitors?

Aon Cyber Solutions (ACS) is the only firm that can manage cyber risks proactively and reactively across the entire cyber ecosystem and through the insurance lifecycle.

ACS specializes in holistic cyber risk management. We use a data-driven approach to help mitigate security risks. Our clients benefit from our security advisory, testing, intelligence and Stroz Friedberg's Incident Response teams to help maximize a client's value.

Over the last 15 years, we've responded to 90% of the highest profile breaches. Our talent, coupled with our set of proprietary tools and methodology, enables us to proactively address threats.

Our professionals are leaders in digital forensics, incident response and proactive services; cyber insurance and risk quantification; cyber investigation; and eDiscovery. Our goal is to maximize the resilience of an organization to improve its profitability, continuity, and protection in the face of enormous cyber risk. Today cyber risk is as ubiquitous as digital technology. To thrive, organizations must approach cyber risk management as rigorously as they approach digital technology development and implementation.

Our unsurpassed investigative skills and proprietary technologies help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents. Aon works to maximize the health of an organization, ensuring its longevity, protection, and resilience. Aon Cyber Solutions was founded in 2016 through the acquisition of Stroz Friedberg, which was founded in 2000

Our proprietary testing methodologies provide a consistent and repeatable process. Our testing techniques have developed from many years of enterprise security assessments completed by highly skilled Aon security engineers utilizing premier proprietary, commercial, and open-source assessment tools. We are supported by a world-class Security Research and Development Team.

Describe how your company will market this contract if awarded.

Aon's Public Sector Partnership (PSP) team is dedicated exclusively to working with US state, local, Tribal, regulated, and quasi-governmental entities on risk management, advisory and transfer solutions. Our PSP team will work with our cyber professionals to inform prospective clients within the NCPA of the vehicle and the advantages gained for new client engagements. We will work to generate leads through local outreach/marketing efforts, prospect meetings, and other engagements. We will include contract information in our capability's presentations to NCPA members.

Our marketing efforts may also include:

- Press releases(s) – if approved by NCPA, Aon will create and distribute a press release announcing the new contract award through our media contacts.

- Webinars/Virtual Events – Aon has utilized webinars and virtual events to address customer challenges and the respective solutions. Most recently we held a webinar on cybersecurity/ransomware.
- Sales collateral – We will include the NCPA contract in our public sector sell sheets that may be distributed electronically and available for download on our public sector website (aon.com/public-sector)

Describe how you intend to introduce NCPA to your company.

The PSP maintains deep relationships with key trade groups and associations and will look to introduce the National Cooperative Purchasing Alliance (NCPA) as the leading national government purchasing cooperative to our company. Introductions will take form in the following:

- Introduce the contract vehicle during our monthly call with all US public sector focused colleagues to provide timely and relevant tools and resources such as NCPA.
- Work with our teaming partners and offer the contract as a preferred vehicle for opportunities with NCPA members.

Describe your firm's capabilities and functionality of your on-line catalog / ordering website.

As a service provider, not a product reseller, we will work with each client to understand their request for services. We will develop a statement of work or engagement letter specific to each client engagement. Katie Sabo, our primary point of contact, well-being discussions regarding ordering services. Katie will coordinate among our Cyber sales and delivery teams to document the appropriate engagement agreement(s).

Is all work performed within the United States? Is work performed by employees, contractors or sub-contractors. Please indicate the percentage performed by each group.

Yes, all work will be performed in the US by Aon employees.

Indicate the level of certification and accreditation of you employees or contractor on the tools they use in the delivery of services.

Our professionals are Certified Information Systems Security Professionals and Information Privacy Professionals. We are ISO 27001 (Cyber) certified across multiple service lines (cyber resilience and digital forensics) in seven U.S. cities and the UK, where we have also obtained Cyber Essentials certification. We are certified to offer CREST (the Council of Registered Ethical Security Testers) penetration testing services in the U.S. and the UK. Aon's security testing team (Gotham Digital Science) is certified to offer industry-leading CREST STAR (Simulated Target Attack and Response) and CBEST application and penetration testing services. Our eDiscovery data centers are SSAE16 certified.

Our multidisciplinary cyber security teams are unmatched, combining technical expertise with unique experience in law enforcement. We are elite forensic analysts and computer scientists specializing in malware decryption, decoding, and reverse engineering; we are also former attorneys from the Department of Justice; internationally respected former prosecutors, litigators, and regulators; and former members of the FBI and CIA.

Where services are to be supplied – what are the choices of license model. Does the customer own the software license or the vendor? Is there a choice?

There is no appliable license model. Aon Cyber Solutions will offer this as a professional services contract based on an agreed scope of work and then priced accordingly.

Who owns the security data artifacts and where are they held? What is the process of supplying the data to the customer at termination of services?

Stroz Friedberg retains the Indicators of Compromise (IOCs) which do not identify any individuals or entities. Customer data is stored in our secure facilities in the US, including evidence rooms with limited, secured access – and on Stroz Friedberg's secure, private network. Once the engagement is complete or services have been terminated, Stroz Friedberg can either delete all customer data in a forensically sound manner and provide a certificate of destruction or return the data to the customer.

Describe your company's Customer Service Department (hours of operation, number of service centers, etc.)

During a breach, you need to act fast. Our response teams are available 24/7 and can be reached using the contact information on the right. For the services we propose providing, we will identify the appropriate points of contact for each engagement and contract. Each engagement will have an Aon Senior Project Team Manager, who will serve as the primary points of contact for clients to handle customer service questions and any contract or payment questions. We observe standard hours of operations and holidays. However, your Aon team will respond to you the same day whenever service is needed.

Additionally, **Aon's Global Emergency Operations Center (GEOC)** is a global, 24/7/365 service serving as a single point of control, coordination, and communication for protecting Aon's people, property and information. When needed, the GEOC team notifies and advises those who need to know about relevant local or national threats. The GEOC exercises the recall of all global employee semi-annually and can be reached 24/7 to find any Aon employee.

General Contract Questions can be sent to:

Leslie Austin
Senior Director
Public Sector Partnership
2001 K Street, NW
Suite 625 North
Washington, DC 20006
Tel: 202-492-8593
E: leslie.austin@aon.com

Katie Sabo
State and Local Leader
Aon's Public Sector Partnership
200 East Randolph
Chicago, IL 60601
Tel: 312-381-1058
E: katie.Sabo@aon.com

Green Initiatives

As our business grows, we want to make sure we minimize our impact on the Earth's climate. We are taking every step we can to implement innovative and responsible environmental practices throughout NCPA to reduce our carbon footprint, reduce waste, energy conservation, ensure efficient computing and much more. To that effort we ask respondents to provide their companies environmental policy and/or green initiative.

Aon is committing to net-zero emissions by 2030. We believe this is a necessary step to take as a global corporate citizen to ensure we are doing our part to reduce our carbon footprint and help mitigate the significant and catastrophic impacts of climate change. Since 2015, we have reduced our greenhouse gas emissions by 60%+, but we recognize there is much more work to be done to have a lasting impact.

In alignment with science-based targets, we will adopt achievable objectives and set action plans focusing on sustainable sourcing, energy efficiency, business travel and renewable energy. Taking these actions will make our firm more effective, efficient, and resilient. We have long been committed to best practices internally and our firm will continue to work with clients to help them identify, understand, and mitigate key environmental, social and governance risks to navigate volatility and drive innovation.

This is just a first step for us, but a significant one. We believe it is in the best interests of our colleagues, clients, and communities that we make this commitment, and we will continue to share our progress toward this goal

Vendor Certifications (if applicable)

Aon Cyber Solutions (The Stroz Friedberg team) holds advanced academic credentials **in science, mathematics, engineering and computer science** and industry leading certifications required to perform the work outlined in this statement of work.

AccessData
AccessData Certified Examiner (ACE)

Association of Certified Fraud Examiners
Certified Fraud Examiner (CFE)

Blacklight
Certified Blacklight Examiner (CBE)
Network+
Security+

Cellebrite
Certified Cellebrite UFED Mobile Device Examiner (CCUMDE)
Cellebrite Certified Operator (CCO)
Cellebrite Certified Physical Analyst (CCPA)

CompTIA
A+
Network+
Security+

EC-Council
Certified Ethical Hacker (CEH)

EnCase
EnCase Certified Examiner (EnCE)

Federal Law Enforcement Training Center
Seized Computer Evidence Recovery Specialist (SCERS)

GIAC
Advanced Smartphone Forensics (GASF)
Certified Forensic Analyst (GCFA)
Certified Forensic Examiner (GCFE)
Certified Incident Handler (GCIH)
Certified Intrusion Analyst (GCIA)
Continuous Monitoring (GMON)
Defending Advanced Threats (GDAT)
Global Industrial Cyber Security Professional (GICSP)
Mobile Device Security Analyst (GMOB)
Network Forensic Analyst (GNFA)
Penetration Testing (GPEN)
Reverse Engineering Malware (GREM)
Security Essentials (GSEC)

IACIS
Certified Forensic Computer Examiner (CFCE)
Certified Electronic Evidence Collection Specialist

(ISC)2
Certified Information Systems Security Professional (CISSP

ISFCE (International Society of Forensic Computer Examiners)
CCE, Certified Computer Examiner

Microsoft
M365 Security Administrator Associate (M365 SAA)

PCI Standards Council
PCI Qualified Security Assessor (PCI-QSA)
PCI Professional (PCIP)

Rapid7
Metasploit Pro Certified Specialist (MPCS)
PCI Professional (PCIP)

Teel Tech
Teel Tech JTAG Forensic Certification (TJFC)

Wetstone
Certified Steganography Investigator (CSI)

Other
Licensed Private Investigators
Top Secret Security Clearance

Additionally, Aons Cyber Solutions is certified by Schellman & Company, LLC to operate as an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2013.

schellman
Quality, above all.

CERTIFICATE OF REGISTRATION

Information Security Management System - ISO/IEC 27001:2013

The Certification Body of Schellman & Company, LLC hereby certifies that the following organization operates an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2013

Stroz Friedberg, LLC

for the following scope of registration

The scope of the ISO/IEC 27001:2013 certification is limited to the information security management system (ISMS) supporting the people, processes, and systems for the Stroz Friedberg Incident Response, Digital Forensics and Security Advisory Services, and in accordance with the statement of applicability version 6.1, dated November 21, 2019.

which includes the following in-scope location(s) on page 2 of 2

Certificate Number: **1731752-6**

ISO 27001 CERTIFIED by schellman

ANAB ACCREDITED ISO/IEC 17021 MANAGEMENT SYSTEMS CERTIFICATION BODY

UKAS MANAGEMENT SYSTEMS 8685

Authorized by:

Christopher L. Schellman
CEO, Schellman & Company, LLC
4010 W Boy Scout Blvd., Suite 600
Tampa, Florida 33607, United States
www.schellman.com

Issue Date	Original Registration Date	Expiration Date	Certificate Version
April 13, 2020	**February 19, 2016**	**February 17, 2022**	**Version 6**

Page 1 of 2

CONDITIONS & LIMITATIONS:

1. The aforementioned organization has a perpetual responsibility to maintain compliance with ISO/IEC 27001:2013 during the period of certification.
2. This certificate is subject to the satisfactory completion of annual surveillance audits by Schellman & Company, LLC
3. ISO/IEC 27001:2013 compliance audits are not designed to detect or prevent criminal activity or other acts that may result in an information security breach. As such, this certification should not be construed as a guarantee or assurance that an organization is unsusceptible to information security breaches.
4. The information in this document is provided "AS IS", without warranties of any kind. Schellman & Company, LLC expressly disclaims any representations and warranties, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose.
5. This certificate is the property of Schellman & Company, LLC and is bound by the conditions of contract. The authenticity of this certificate can be validated by contacting Schellman & Company, LLC

In-Scope Location(s)

Location	Function / Role
One Liberty Plaza 165 Broadway, Floor 28 New York, New York 10006 United States	Headquarters and main location of the ISMS and its owners
5005 Lyndon B. Johnson Freeway Suite 1500 Dallas, Texas 75244 United States	Office Facility
1925 Century Park East Los Angeles, California 90067 United States	Office Facility
The Leadenhall Building 122 Leadenhall Street London, EC3V 4AN United Kingdom	Office Facility
2001 K Street NW Suite 625 North Washington, District of Columbia 20006 United States	Office Facility
330 Second Avenue South Minneapolis, Minnesota 55401 United States	Office Facility
425 Market Street Suite 2800 San Francisco, California 94105 United States	Office Facility
1420 5th Ave Suite 1200 Seattle, Washington 98101 United States	Office Facility

CONDITIONS & LIMITATIONS:

1. The aforementioned organization has a perpetual responsibility to maintain compliance with ISO/IEC 27001:2013 during the period of certification.
2. This certificate is subject to the satisfactory completion of annual surveillance audits by Schellman & Company, LLC.
3. ISO/IEC 27001:2013 compliance audits are not designed to detect or prevent criminal activity or other acts that may result in an information security breach. As such, this certification should not be construed as a guarantee or assurance that an organization is unsusceptible to information security breaches.
4. The information in this document is provided "AS IS", without warranties of any kind. Schellman & Company, LLC expressly disclaims any representations and warranties, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose.
5. This certificate is the property of Schellman & Company, LLC and is bound by the conditions of contract. The authenticity of this certificate can be validated by contacting Schellman & Company, LLC.

Tab 5. Products and Services

Aon Cyber Security Products, Services and Solutions Identifying, Protecting, Detecting, Responding and Recovering through Aon's Seek, Shield and Solve Products and Tools

Aon's Cyber Solutions specializes in holistic cyber risk management. We approach cyber exposure with a multifaceted solution: seek, shield, and solve. Aon's Cyber Solution protective readiness approach is designed to fit within the National Institute of Standards and Technology (NIST) framework.

Aon Cyber Solutions takes an enterprise-wide, risk-based approach to evaluate cyber threat. With a full spectrum of security assessment services, we will provide deep insight and enhanced understanding of preparedness for a cyber incident. We can assess the strength of cyber defenses and overall readiness to respond to external threats, insider risks and third-party risks, Aon reviews the environment to identify cybersecurity gaps and vulnerabilities across five key areas: business practices, information technology, end users, security governance and the physical security in information assets and will assist in mitigating or transferring enterprise cyber risk.

Identify

We applied our deep experience handling some of the largest, most difficult cyber investigations to create a framework that includes tooling and scanning to help assess an entity's attack vector, attacker techniques and indicators, and provide ongoing visibility into risk exposure.

Aon's modeling is proprietary and leverages leading industry knowledge and data — not out-of-the-box that can be tailored to the Trust's unique needs. Our work product will include cyber aggregation risk, trust member tiering, and expected cost type breakdowns. We will access and quantify the exposure to cyber risk and model probable risk scenarios, delivering data to effectively manage your financial and operational risk from a cyber event.

We help align ransomware defenses and assess capabilities against attack scenarios leveraging our proactive security professionals, while combining scanning and vulnerability assessment solutions to deliver a Defense in Depth approach. We have coupled this tested framework with access to seasoned security advisory professionals to offer you tailored support.

We will conduct a comprehensive security risk assessment using a NIST-based risk assessment to evaluate an entities cyber security vulnerability. Aon will leverage guidance from recognized industry standards and best practices, as well as the cumulative knowledge and perspective of Aon, regarding information security best practices to identify opportunities for improvement in Client's current security posture.

Protect

Aon Cyber Security protection products and services are designed to holistically address the critical controls that help protect and mitigate ransomware attack vectors. Aon's Cyber Solutions specializes in performing a range of security testing services including network penetration testing, application security testing, source code review, social engineering assessments e.g., phishing & vishing campaigns, and physical penetration testing.

Core to Aon's Cyber Solutions security testing approach are test cases and testing techniques that require execution by highly skilled security engineers. Automated assessment techniques, proprietary Security Directives, and the use of premier proprietary, commercial, and open-source assessment tools in a consistent and repeatable process supplement manual testing. This approach ensures every Aon assessment maximizes depth and breadth of vulnerability coverage.

To support every Aon testing methodology, we have developed a set of proprietary Security Directives as a security framework against which an assessment target is tested. The Aon Security Directives leverage test cases from industry methodologies such as the Open-Source Security Testing Methodology Manual (OSSTMM), NIST, CREST STAR, CBEST and the OWASP Testing Guide and have been further extended from many years of enterprise security assessments completed by Aon engineers.

The Aon Penetration Testing Methodology (PTM) documents the technical framework by which Aon penetration engineers perform testing in a defined, controlled and repeatable manner. This methodology combines manual and automated assessment techniques, proprietary techniques, and the use of premier proprietary, commercial, and open-source assessment tools in a consistent and repeatable process.

Our testing methodologies are designed to test and measure conformance with each Security Directive and ensure that a consistent and comprehensive level of testing is performed against every target assessed by Aon.

Testing activities are designed to imitate/replicate the reconnaissance activities of adversaries planning to remotely target the client. The following are examples of major activities are performed during this phase:

- IP (Intellectual Property) and domain name registrar queries
- Querying of available DNS servers
- Ping sweep and targeted network service probing of in-scope networks for the purposes of identifying subnets with "live" hosts
- Targeted probing for banner enumeration and confirming type of listening network services
- Mapping and identification of exposed internet facing hosts, services, and protocols based on results from subscription-based search engines (e.g. Shodan)
- Leverage search engine technology such as Google and Bing to uncover public information leakage or security exposures
- Where possible, utilize publicly available information that has been inadvertently shared and distributed through side channels such as popular social networking websites and special interest groups

Together, this Internet Profile will be utilized during subsequent phases of the project for performing more intelligent, comprehensive port scanning and targeted vulnerability scanning. Using the Internet Profile built from Reconnaissance, Aon will perform service scans that are more comprehensive and iterative in nature. For example, scanning for a wider variety of services on those subnets found to have live hosts will be performed. Full-service scans and service detection will be performed against hosts confirmed live. This iterative approach is designed to identify as much attack surface as possible while minimizing the potential for unreliable scan results and impact on production infrastructure that is likely if a scan everything all at once approach is taken.

Each targeted network range is scanned to identify and document all available hosts, open ports, service type and fingerprint. This typically entails TCP and UDP port scanning and targeted protocol probing to facilitate the identification of service versions and well-known services running on non-standard ports. Aon security engineers leverage open-source port scanning and protocol probing tools such as Nmap and netcat as well as proprietary Aon tools.

An accurate map detailing all actual exposed infrastructure, servers, services and applications making up the Client's Internet estate is essential information for determining the enterprise/corporate security posture of an organization.

When this map is overlaid with validated vulnerability assessment results in subsequent phases, high probability attack vectors can be determined in an educated fashion, measured against risk, and defensive countermeasures be

implemented to address identified gaps. Vulnerability scanning and manual testing techniques are used to drive what vulnerability scanning tools are utilized and the types of checks to be configured based on the services exposed (HTTP, SSH, FTP, etc.). Key scanning tools utilized during this phase include Nessus (commercial feed) and Rapid7 Nexpose. All anonymously accessible components of web applications will be scanned with HP WebInspect, Aon Boxer, and/or BurpSuite Pro where relevant. Note that functionality that could materially impact business processes, for example "contact-us" pages, will be excluded from automated scanning. To the extent possible, all scan results are manually validated, however this may not Aon be feasible given engagement constraints and a high volume of results. When faced with large result sets, Aon employs a sample-based approach that accounts for issue severity and risk, volume of similar findings across hosts and outliers, and objectives and threats of specific concern to our client, such as systems handling extremely sensitive data as well as any pre-existing automated scan results that might be available. The chosen approach will be validated with the client to ensure it meets their goals and objectives of this engagement. Manual vulnerability testing is also utilized when protocols are unknown, or conditions are not appropriate for an automated scanner.

Creative and innovative exploit techniques are leveraged to provide “proof of concept” attack vectors for clearly illustrating risk to company resources. Prior to running any exploits, Aon security engineers coordinate with the client to ensure exploits do not negatively impact the target system or network service. Step-by-step screen shots (where applicable) are captured during each exploit for inclusion in the final deliverable.

Once all testing and exploit activities are completed, a comprehensive report of all identified security issues is prepared. This report includes all the necessary information for system owners and administrators to implement the necessary changes to correct or mitigate all identified vulnerabilities. Additionally, the results will be communicated to key stakeholders during a project closeout meeting.

Core to every Aon application security assessment is the proprietary Aon Application Security Directives (ASDs) which provide a security framework against which the target application is tested and scored. This facilitates the identification of systemic insecure development practices while also allowing easy comparison of applications of different size, complexity and development team.

Detect, Respond and Recover

Aon is ready to help when a cyber-attack occurs. Our experts are poised to help limit business/service interruption, ensure recovery, and expedite claims preparation. In addition, we can preserve digital evidence required for reporting purposes or in the event of legal action, and we can act as expert witnesses during regulatory proceedings or litigation.

Incident & Breach Response

We will provide a quick-acting team of incident responders, including forensic examiners and former regulators. Our involvement will help to deliver less damage, and ultimately less reputational and financial fallout. Your breach response team will undertake rapid remote support, then work onsite to understand what happened. They will contain the incident while preserving evidence, and confidently communicate with your stakeholders

Digital Forensics

We are recognized industry leaders in the field of digital forensics who have helped shape best practices in digital investigations and risk management. Our specialists have been certified in multiple states and have experience providing expert witness testimony, formal reporting to law enforcement, and complying with civil, criminal and regulatory obligations. We are credentialed specialists in network, database, mobile device, and other forms of digital forensics; malicious code and other types of malware; computer fraud and abuse; and data discovery, analytics, and disclosure.

eDiscovery

We understand the discovery challenges presented by enterprise data expansion and evolution in order to target, analyze, understand, and present the key issues in a reasonable, efficient, and defensible manner. The eDiscovery practice consists of trusted advisors — a group of the brightest minds in our field — with extensive experience assisting

clients with eDiscovery strategies, as well as data preservation, documentation, authentication, and potential spoliation issues. Our full suite of services effectively manages the most complex matters and reduce costs without compromising on quality.

Expert Witness Testimony

In litigation, the reputation and financial health of your organization is at risk. You need a battle-tested and trusted expert witness by your side who will help you find and present the facts, and what they indicate, when the stakes are high. We help organizations present their cases and diminish risk. Our expert witnesses clarify the facts impartially and present them in a manner that can stand up to scrutiny from the court and opposing counsel. We document proper chain-of-custody, testify on the validity of forensic data, and objectively present our findings. We are credentialed former prosecutors and investigators with an intimate knowledge of the law1. We can help instill confidence in your in-house and outside counsel by offering testimony that can withstand cross-examination by even the savviest opposing attorneys. We work as an integrated team. Our professionals are recognized leaders in technology, law, government, business, risk, law enforcement, intelligence, computer science, and digital forensics. This breadth of knowledge, combined with our field experience, deepens our analysis and better serves you.

Digital Evidence Preservation

Many organizations know very little about evidentiary procedures and proper chain-of-custody when it comes to keeping electronic data in an untainted state. Our approach is state-of-the-art. Whatever evidence you are trying to track down, our digital forensics team will engage in response and containment efforts until the relevant evidence is gathered and understood. We'll also look at both known and suspected technologies involved in your incident and work to leave minimal impact on the memory of the device being examined.

With your evidence in our capable hands, expect:

- forensic data preservation for sources, including desktop or laptop computers, servers, enterprise databases, mobile devices, removable media, cloud-based accounts, and full chain-of-custody records;
- assurance of evidence integrity via our state-of-the-art data encryption processes;
- secure onsite electronic and physical storage of forensic materials; and expert testimony

Workplace Misconduct Investigations

Employee misconduct takes many forms. An employee is accused of sexually harassing or making threatening remarks to a colleague, vendor or client. Maybe an employee has embezzled funds, stolen sensitive information or engaged in an activity you consider a conflict of interest. Recoverable forensic evidence can uncover an employee involved in an activity such as stealing money, proprietary information, intellectual property or trade secrets. You need to uncover the truth without implicating innocent employees. This requires a specialized team. We listen to your concerns, interview key stakeholders and investigate. We probe open source, social media and proprietary databases, and our forensic examiners identify, preserve, and analyze data to help build a chronology of the incident when dealing with fraud, our forensic accountants help confirm and calculate damages and help locate hidden assets.

Aon Cyber Solutions Products, Solutions and Services Overview

NIST Functional Framework Category	Aon Cyber Framework Category	Aon Cyber Solution	Aon Cyber Product & Service
Identify	**Seek: We help clients identify and quantify their cyber risk** Aon takes a risk-based approach to evaluate cyber threat. With a full spectrum of security assessment services, we will provide deep insight and enhanced understanding of your preparedness for a cyber incident. We can assess the strength of your cyber defenses and overall readiness to respond to external threats, insider risks and third-party risks, Aon reviews the environment to identify cybersecurity gaps and vulnerabilities across five key areas: business practices, information technology, end users, security governance and the physical security in information assets. Aon will provide actionable and prioritized recommendations for mitigating or transferring enterprise cyber risk.	**Assessments**	▪ Security Risk Assessment ▪ Cyber Quotient Evaluation (CyQu) ▪ Cyber Impact Analysis: Financial Quantification ▪ Incident Response Readiness Assessment ▪ Privacy Compliance Assessment ▪ Individual Vulnerability Assessment ▪ CyberScan
		Cyber Security Testing	▪ Red Team & Social Engineering Testing ▪ Application & Mobile Security Testing ▪ Network & Cloud Penetration Testing ▪ Cloud & Host Configuration ▪ Automotive & IoT Security Testing ▪ Source Code Security Review ▪ Security Architecture Assessment ▪ Developer Application Security Training ▪ Secure Development Training ▪ Threat Hunting
		Due Diligence & Background Investigations	▪ Background Assessments

NIST Functional Framework Category	Aon Cyber Framework Category	Aon Cyber Solution	Aon Cyber Product & Service
Protect	**Shield: We know how to protect an organization and its critical assets** Aon's cyber professionals help clients properly prepare, optimize and enhance security governance and incident detection and protocols. Simulating tabletop exercises, coordinating with stakeholders to design, refine, and validate incident response plans, assisting with architecture and design, and serving as experts who can validate corporate cybersecurity actions will help improve overall cybersecurity protection.	**Simulations/ Protection Planning and Development**	▪ Incident Response Planning & Playbook Development ▪ Cyber Threat Simulations ▪ Security Architecture & Design ▪ Security Policies & Standards Development ▪ Security Controls Optimization ▪ Third Party Cyber Risk Management ▪ Insider Risk Program Development ▪ Secure Software Development Lifecycle ▪ SOC Optimization ▪ CISO Advisory ▪ Threat Intelligence Monitoring ▪ Data Privacy Analysis ▪ Data and Workflow Mapping
Detect, Respond and Recover	**Solve: We help our clients recover quickly** Aon is ready to help when a cyber-attack occurs. Our experts are poised to help limit business/service interruption, ensure recovery, and expedite claims preparation. In addition, we can preserve digital evidence required for reporting purposes or in the event of legal action, and we can act as expert witnesses during regulatory proceedings or litigation.	**Aon Cyber Solutions Detect, Response and Recovery Services**	▪ Stroz Friedberg Incident Response ▪ Stroz Friedberg Digital Forensics ▪ eDiscovery ▪ Expert Witness Testimony ▪ Incident Response Retainer ▪ Complex Cyber Claims Preparation ▪ Cyber Claims Advocacy ▪ Investigations & Recovery Services ▪ Workplace Misconduct Investigations ▪ Digital Evidence Preservation ▪ Asset Searches ▪ Identify Attribution ▪ PHI/PII Data Mining for Risk/Compliance

Tab 8. Value Added Products and Services

Since Aon's Cyber Solutions specializes in providing enterprise-wide, holistic cyber risk management solutions, we wanted to share additional products and services which have added value to our clients globally. This section includes additional cutting-edge products and services Aon Cyber Solutions provides to current clients to greatly enhance their cyber security posture as well as our focus on three areas: Marketing and Training, M/WBE and HUB Participation and Customer Services.

Marketing and Training

Aon's Public Sector Partnership (PSP) team is dedicated exclusively to working with US federal, state, local, tribal, regulated, and quasi-governmental entities on risk management, advisory and transfer solutions including cyber services. Our PSP team will work with Aon Cyber Solutions' professionals on the full scope and capabilities of the contract statement of work and inform prospective clients within the NCPA of the vehicle and the advantages gained for new client engagements.

We will work to generate leads through local outreach/marketing efforts, prospect meetings, and other engagements across the dozen solution lines in Aon. We will include contract information in our capability's presentations to NCPA members.

Our marketing efforts may also include:

- Press release(s) – if approved by NCPA, Aon will create and distribute a press release announcing the new contract award through our media contacts.
- Webinars/Virtual Events – As a thought leader in all our industries, Aon plans and executes numerous webinars, fire-side chats, conferences, and virtual events to address customer challenges and the respective solutions. Most recently we held a webinar on cybersecurity/ransomware.
- Thought Leaders and Industry Expertise – Aon professionals are highly sought to participate and panel discussions, fire-side chats, webinars, and podcasts hosted in numerous industries and many of these provide opportunities to market the capabilities of NCPA.
- Sales collateral – We will include the NCPA contract in our public sector sell sheets that may be distributed electronically and available for download on our public sector website (aon.com/public-sector)

Minority and Women Business Enterprise (MWBE) and (HUB) Participation

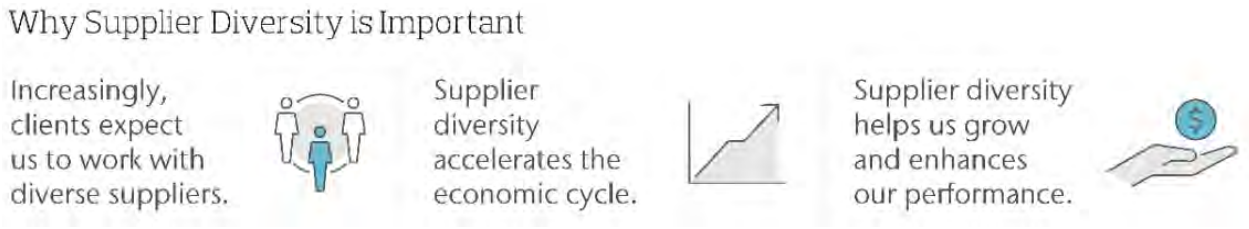
Aon is committed to driving an inclusive culture where all colleagues feel encouraged to bring their whole selves to work. We've launched the 'I'm in' inclusion commitment so each of us may have the opportunity to visibly demonstrate our personal dedication to driving an inclusive culture. Our commitment to diversity can also be found in our diversity supplier program to provide diverse enterprises with more opportunities within our industry and within Aon.

At Aon, we believe supplier diversity plays an integral role in supporting the needs of our stakeholders to create long-term value for our colleagues, clients, and communities. Aon commits significant resources to develop and maintain valuable relationships with businesses that are minority-owned, woman-, disadvantaged-, LGBT-, and veteran-owned as well as small, HUB-zone, and differently abled or disability-owned business enterprises and providing maximum practicable opportunities for suppliers that can offer quality, innovative, competitive, and cost-effective products, and services. Aon continues to increase, year-over-year, our addressable spend with diverse suppliers. In 2020, 5% of Aon's US addressable spend was with diverse suppliers, 2.5 times higher than the Fortune 500 average.

Aon's supplier and business diversity program, Aon Diversity Solutions (ADS), is a centralized team within the firm that fosters opportunities for diverse business enterprises through both internal projects as well as across external

engagements. Our unique ADS platform enables the opportunity for small businesses and diverse firms to work directly with Aon colleagues to support local, state, and federal initiatives as well as commercial client initiatives.

Our mission is to advance good corporate citizenship by engaging stakeholders, advising decision makers, and driving accountability through supplier diversity best practices, processes, and governance initiatives.



Aon routinely seeks diverse suppliers through membership in diverse supplier business advocacy organizations and participation in various capacity building and matchmaking activities across the United States. Aon is an active partner with diverse business enterprise non-governmental organizations (NGOs) to create appropriate alignment to supplier and business diversity program sourcing goals and certification processes. ADS leverages partnerships with the National Minority Supplier Development Council (NMSDC), Women's Business Enterprise National Council (WBENC), National Veteran Business Development Council (NVBDC), National Gay & Lesbian Chamber of Commerce (NGLCC) and Disability.

Customer Services

The PSP team will develop the necessary channels with NCPA to obtain regular feedback. We want to have a successful partnership where Aon exceeds expectations and provides best-in-class service. Our team will serve as the primary points of contact if there are any concerns with performance or to obtain support quickly.

Our proactive approach to managing this relationship will include:

- Periodic reviews with NCPA
- Exchange sessions where Aon can share trends, lessons-learned, cyber innovations, and more to help NCPA and its members evaluate their risks and take the necessary steps to protect their assets.

Additional Services

As shared earlier, Aon's Cyber Solutions (ACS) includes a unique combination that not only provides world class proactive and reactive cyber solutions and tools, but also can help our clients transfer risk in the form of Cyber insurance. The integration of this risk transfer capability sets ACS apart from any other Cybersecurity solutions provider in the marketplace.

Brokering Cyber Insurance (Risk Transfer)

Beyond our capabilities in the proactive and reactive cybersecurity space, Aon is uniquely positioned to provide our clients with Cyber insurances broking services. Aon has long-standing relationships with over 150 global insurers and has access to every insurance market. With Aon's distinct broking groups, composed of brokers who specialize by line of insurance coverage and client type, Aon is at the forefront of both domestic and international cyber insurance placements. The cybersecurity landscape changes quickly, and the risk seems to be growing exponentially; therefore, cyber insurance is a rapidly evolving product. Aon can provide relevant and innovative bespoke strategies to our public sector clients. Aon provides a tailor-made cyber insurance program for each insured. With over $500 million dollars in cyber premium placed annually, Aon is the largest cyber broker both domestically and internationally. This gives Aon's insureds an advantage on cyber insurance cost, coverage, and service.

When you select Aon to address your Cyber Insurance needs, we will start our work with an assessment of your cyber risks and mitigating factors. Drawing on our team of consultants from Aon Cyber Solutions, we will quickly engage the information security team at the public sector client to quantify risks and understand mitigation strategies. In parallel, the insurance broking and actuarial team will assess the program to provide benchmarking, identify ways to avoid costs and improve program performance. The output of these exercises will include recommendations and a data-driven assessment that will be used to shape your insurance program and to tell your unique story to the insurance markets.

We will provide you with suggestions, based on our experience, about how the policy language can be tightened or enhanced to ensure the policy performs as expected should a claim occur. Complex cyber losses have impacted the cyber insurance market, particularly traditional excess insurers where pricing has historically been extremely thin. Losses paid from cyber claims since 2017, and reported through public filings, exceeded $500M. Ransomware activity has stressed insurer portfolios and the regulatory environment continues to gain complexity, particularly with emerging privacy legislation connected to BIPA, CCPA, and GDPR. As a result, insurers are actively managing their global capacity deployment and have started retracting coverage for ransomware events, in terms of adding coinsurance and/or sub-limits. We anticipate amplified rate pressure on excess market placements, with material increases to underlying increased limit factors. When we meet with you, we will share observations on how Aon is responding to these changes on behalf of clients. We will continue to update our clients on market dynamics that may provide challenges or opportunities.

As we prepare for the renewal, our cyber consulting team will be closely involved with the Aon broking team to prepare for the meetings with the underwriters. Armed with thoughtful benchmarks and the intricacies of your information technology security situation, we will secure a renewal on terms attractive to both the markets and to our public sector clients.

Risk Transfer option programs include:

- Cyber Insurance
  - Aon Cyber Enterprise Solution
  - Aon's Cyber Business Interruption Plus (BI+)
  - Aon Cyber Captive Program

Cyber Insurance

Cyber security risk is not only a privacy risk; it can also result in significant business disruption, including physical property damage and implications to the supply chain and physical product. As a result, Aon offers cyber insurance solutions that continue to evolve in breadth and scope, including Aon Cyber Enterprise Solution® and Aon's Cyber Business Interruption Plus ("BI+"), which help organizations transfer cyber risks off their balance sheet through insurance and contribute to holistic risk management and enterprise-wise cyber resilience.

Cyber Claims Advocacy

If a cyber claim does need to be filed, Aon is there to help simplify the associated complexities. We have been guides through the cyber claims handling process for more than 20 years. Our goal is aligned with yours: To maximize what you receive from your insurance. Our team knows the contract wording and can negotiate on your behalf through complex situations to deliver results for you.

We also have the needed insight, and our proven methodology is disciplined, yet flexible. Our dedicated team has developed and advocated successful strategies for some of the most complex cyber claims around the globe, helping to optimize the claim recovery outcomes with your insurer. In 2020, we handled 349 cyber claims and 1,150 E&O claims. Since 2016, we have helped to our clients obtain over $1b in insurance recoveries.

Forensic Accounting Financial Transaction Lookback / Clawback Capabilities

Aon's Cyber Solutions team has utilized it deep expertise as a global provider of complex digital fraud and financial investigations, forensic accounting, and compliance assessments to support public sector clients in need of forensic accounting financial lookback capabilities. This capability enables public sector clients to analyze, identify and clawback already disbursed benefits payments which have been taken by cyber fraudsters. Some examples of applicable payments include those made as part of State unemployment Insurance programs or the recent Paycheck Protection Program (PPP).

ACS specialization in transaction lookbacks & fraud investigations, particularly related to cyber fraud, makes it uniquely qualified to assist public sector entities detect, identify, escalate, and recover funds stolen via cyber fraud. Starting with multiple data sets, Aon applies proprietary workflows to large sets of claims to prioritize those claims for further investigation and review. Our team of forensic investigators determines the likelihood that a claim is fraudulent, which assists law enforcement and, ultimately the state, increase both the speed and amount of recoveries.

Aon's Cyber Quotient Evaluation (CyQu)

Aon offers clients the ability to assess their cyber strengths and weaknesses though the award winning online cyber risk self-assessment CyQu. CyQu is an online cyber maturity self-assessment enabling you to take an important step in managing your organizations cyber risk — so you can begin to strengthen your risk posture sooner.

- Cyber risk posture is evaluated based on nine security domains which can be broken down into 35 critical control areas
- In about 90 minutes or less, CyQu will provide you with a cyber risk maturity score (CyQu Score) giving you an immediate snapshot of your cyber maturity and insight into the areas posing the greatest risk
- This will be followed up with a report, detailing key findings and opportunities for remediation to help you improve your cyber resilience

Clients have access to either CyQu or CyQu Enterprise based on the size of their firm. CyQu cis for clients with revenues up to $100 million and can be completed in 20 minutes or less. CyQu Enterprise is for organizations with revenues between $100 million and $1 billion and can be completed in 90 minutes or less.

It is done by completing a concise online self-assessment across nine security domains broken down into sub-categories or "critical Controls."

1. Data security
2. Access control
3. Endpoint and systems security
4. Network security
5. Physical security

6. Application security
7. Third party
8. Business resilience
9. Remote work

Within 10 working days, the client receives a detailed CyQu report developed by an Aon cyber risk consultant. The resulting strategic roadmap will by unique to the client and may include:

- Third-party risk management
- Network and application security
- Employee training
- Policy and procedure revision/creation
- Threat intelligence and analysis
- Vulnerability and insider threat management
- Cloud security or,
- Regular testing and verification activity

Aon's Cyber Secure

Cyber-attacks on individuals and executives including senior government officials are evolving at an alarming rate and becoming increasingly more sophisticated. With the shift to remote work in 2020, these attacks have accelerated. Aon developed a holistic offering to help protect senior government officials, high-profile individuals, and high net worth individuals and their families with industry leading identity theft protection, robust device prevention, detection, and an innovative consumer cyber insurance offering for individuals and/or executives. This comprehensive solution can be customized, but includes:

- Individual Vulnerability Assessment
- Threat Intelligence Monitoring
- Online Takedown Services
- Threat Simulation Assessment
- Cyber Advisory Services
- Personal Cyber investigation & Incident Response Services

Aon's Cyber Awareness Training

Ongoing cyber security education and training for employees is a must, for public sector organizations of all sizes, to help stay secure. Many breaches result from a simple lack of employee awareness. Although businesses may feel their employees wouldn't be fooled by something like a phishing scam, cyber criminals continue to use this attack vector because it continues to yield success. With regular training for employees, businesses can significantly help reduce cyber security risk, protect their reputation, and secure their overall cyber security investment.

Cyber Awareness Training helps organizations take an intelligent approach to cyber and information security awareness. Our proprietary program is designed around the simple principle that if your people know how to behave better online, they will be more secure—and so will your business. With decades of experience in law enforcement, military, intelligence services and the private sector, Aon's Cyber Solutions understands the latest criminal tactics,

techniques and procedures which enables us to educate organizations on all cyber risks. Cyber Awareness Training is a single platform that educates your employees through on-demand intuitive learning program via a range of twelve structured modules, containing engaging content designed to help optimize behavior change. Staff can easily be enrolled via an active directory sync, manually or via a CSV upload. Cyber Awareness Training fosters learning through gamification with leaderboards, Cycoins for champions and certificates on course completion. Management can access detailed reports via the platform for consistent tracking and reporting. Phishing simulations and instructor lead courses are also available.

Cyber Awareness Training is based on the cyber-crime equation (Target + Attack + Vulnerability = Impact). We have taken an equation that law enforcement agencies have been successfully using for years to provide physical safety awareness to communities and adapted it to help protect people against the threats brought on by the digital age.

Virtual CISO Capabilities

Being an organization's information security lead is a challenging role. The cyber threat landscape and regulatory demands are ever-changing. Furthermore, there is a shortage of cyber security talent. Every organization can benefit from advisory assistance to help build and implement a strong security framework

We offer cyber security advisory support for Chief Information Security Officers (CISOs) and, for those organizations without one in place, we advise executives tasked with securing the company. We can provide strategic guidance, give tactical project support, offer input on budgeting, and present security strategies to your board. We customize our support to meet your needs.

Ability to Help our Clients Access Specialized Capabilities and Surge via Aon's Strategic Alliance Relationships

Aon Cyber Solutions (ACS) also maintains a number of Strategic Alliance relationships with best-in-class companies which our public sector clients can access via their relationship with Aon. These companies provide needed capabilities and tools to monitor and protect a client's endpoints and Managed Security Service Providers (MSSPs). Beyond this specific type of support, our Strategic Alliances can also provide our clients with needed supplemental resources in the cybersecurity and IT space. This support could include IT services and project implementation (e.g., for controls such as multi-factor authentication (MFA)).

Recruiting, developing, and retaining needed Cybersecurity Talent

Aon is a Global leader in supporting all industries in understanding trends in the cybersecurity professional talent management through a comprehensive mix of data, analytics, and advisory capabilities. These capabilities support our clients to make data-driven, research-supported decisions about their rewards and compensation structure. This includes compensation and benefits benchmarking and the design that helps you make better and more equitable compensation and rewards decisions. Our proven expertise will help DHS strategically design a world-class, cutting-edge program to draw and attract exceptional cybersecurity talent. Aon companies, Radford and McLagan, offer industry-leading data and analytics.

- **McLagan Data & Analytics platform**, a proprietary product of Aon's Rewards practice, delivers compensation insights to more than 2,000 of the world's leading financial services companies, including asset management, banking, financial technology, insurance, professional services, and wealth management firms.

- **Radford Data & Analytics platform**, a proprietary product of Aon's Rewards practice, delivers compensation insights for over 9.5 million of employee positions working at the world's most innovative companies, including over 3,000 organizations and 3,300+ unique jobs in digital media, life sciences, medical device and manufacturing, media and gaming, retail and e-commerce, technology, and transportation and mobility firms.

- **Aon's Technology Strategic Steering Committee**. Aon created the Aon Technology Council to bring leading technology company HR officers together to discuss trends and impacts they are seeing. Although participation in

this group is by invitation only working with Aon provides our clients specific insights from this group. These insights are the most pressing issues driving the entire technology industry. Here are the current participants:

- Adobe Systems
- Advanced Micro Devices
- Airbnb
- Amazon
- Analog Devices
- Apple
- Applied Materials
- Autodesk
- Broadcom
- Cadence Design Systems
- Cisco Systems
- Citrix Systems
- Dell
- eBay
- Electronic Arts
- Facebook
- Google
- Hewlett-Packard Enterprise
- IBM
- Infosys
- Intel
- Intuit
- Juniper Networks
- LinkedIn
- Microsoft
- Micron Technology
- National Instruments
- NetApp
- Norton LifeLock
- Nvidia
- NXP Semiconductors
- Oracle Palo Alto Networks
- PayPal
- Qualcomm
- Salesforce
- Samsung Electronics America
- SAP
- Seagate Technology
- ServiceNow
- Splunk
- Synopsys
- Tesla Motors
- The Walt Disney Company
- Twitter
- VMWare
- Workday
- Xilinx

Aon's data about leading financial institutions, banking industry, technology, and transportation companies provides insight into the convergence of cyber needs across industries. Our McLagan and Radford client list includes 99 of the top 100 banks and almost all leading technology companies. We leverage these relationships to offer a compressive understanding of the market. In addition, we recently conducted a detailed role and compensation benchmarking analysis for the cyber security function at one of the largest banks in the United States. The study focused on threat management, incident response, cyber-crime prevention, and cyber security technology roles. The analysis led to the client adjusting salary ranges and levels for some employees.

Tab 9. Required Documents

- Clean Air and Water Act / Debarment Notice
- Contractors Requirements
- Antitrust Certification Statements
- Required Clauses for Federal Funds Certifications
- Required Clauses for Federal Assistance by FTA
- State Notice Addendum

Clean Air and Water Act & Debarment Notice

I, the Vendor, am in compliance with all applicable standards, orders or regulations issued pursuant to the Clean Air Act of 1970, as Amended (42 U.S. C. 1857 (h), Section 508 of the Clean Water Act, as amended (33 U.S.C. 1368), Executive Order 117389 and Environmental Protection Agency Regulation, 40 CFR Part 15 as required under OMB Circular A-102, Attachment O, Paragraph 14 (1) regarding reporting violations to the grantor agency and to the United States Environment Protection Agency Assistant Administrator for the Enforcement.

I hereby further certify that my company has not been debarred, suspended or otherwise ineligible for participation in Federal Assistance programs under Executive Order 12549, "Debarment and Suspension", as described in the Federal Register and Rules and Regulations

Potential Vendor	Stroz Friedberg, LLC
Print Name	James Trainor
Address	One Liberty Plaza, 165 Broadway, #3201
City, Sate, Zip	New York, NY 10006
Authorized signature	DocuSigned by: James Trainor E1B8E24797204EB...
Date	November 18, 2021

Contractor Requirements

Contractor Certification
Contractor's Employment Eligibility

By entering the contract, Contractor warrants compliance with the Federal Immigration and Nationality Act (FINA), and all other federal and state immigration laws and regulations. The Contractor further warrants that it is in compliance with the various state statues of the states it is will operate this contract in.

Participating Government Entities including School Districts may request verification of compliance from any Contractor or subcontractor performing work under this Contract. These Entities reserve the right to confirm compliance in accordance with applicable laws.

Should the Participating Entities suspect or find that the Contractor or any of its subcontractors are not in compliance, they may pursue any and all remedies allowed by law, including, but not limited to: suspension of work, termination of the Contract for default, and suspension and/or debarment of the Contractor. All costs necessary to verify compliance are the responsibility of the Contractor.

The offeror complies and maintains compliance with the appropriate statutes which requires compliance with federal immigration laws by State employers, State contractors and State subcontractors in accordance with the E-Verify Employee Eligibility Verification Program.

Contractor shall comply with governing board policy of the NCPA Participating entities in which work is being performed

Fingerprint & Background Checks

If required to provide services on school district property at least five (5) times during a month, contractor shall submit a full set of fingerprints to the school district if requested of each person or employee who may provide such service. Alternately, the school district may fingerprint those persons or employees. An exception to this requirement may be made as authorized in Governing Board policy. The district shall conduct a fingerprint check in accordance with the appropriate state and federal laws of all contractors, subcontractors or vendors and their employees for which fingerprints are submitted to the district. Contractor, subcontractors, vendors and their employees shall not provide services on school district properties until authorized by the District.

The offeror shall comply with fingerprinting requirements in accordance with appropriate statutes in the state in which the work is being performed unless otherwise exempted.

Contractor shall comply with governing board policy in the school district or Participating Entity in which work is being performed

Business Operations in Sudan, Iran

In accordance with A.R.S. 35-391 and A.R.S. 35-393, the Contractor hereby certifies that the contractor does not have scrutinized business operations in Sudan and/or Iran.

Authorized signature DocuSigned by: James Trainor E108E2479720AEB...

Date November 18, 2021

Antitrust Certification Statements (Tex. 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	Stroz Friedberg, LLC
Address	One Liberty Plaza, 165 Broadway, #3201
City/State/Zip	New York, NY 10006
Telephone No.	646.634.2899
Fax No.	
Email address	james.trainor@aon.com
Printed name	James Trainor
Position with company	Senior Vice President
Authorized signature	DocuSigned by: James Trainor E1B8E24797204EB...

Required Clauses for Federal Funds Certifications

Stroz Friedberg, LLC has reviewed the clauses below and will comply with one change added below.

Participating Agencies may elect to use federal funds to purchase under the Master Agreement. The following certifications and provisions may be required and apply when a Participating Agency expends federal funds for any purchase resulting from this procurement process. Pursuant to 2 C.F.R. § 200.326, all contracts, including small purchases, awarded by the Participating Agency and the Participating Agency's subcontractors shall contain the procurement provisions of Appendix II to Part 200, as applicable. For the purposes of this Agreement, Stroz Friedberg, LLC shall be determined to be a "contractor" per 2 C.F.R. 200.330 and not a "subrecipient".

APPENDIX II TO 2 CFR PART 200

(A) Contracts for more than the simplified acquisition threshold currently set at $150,000, which is the inflation adjusted amount determined by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) as authorized by 41 U.S.C. 1908, must address administrative, contractual, or legal remedies in instances where contractors violate or breach contract terms, and provide for such sanctions and penalties as appropriate.

(B) Termination for cause and for convenience by the grantee or subgrantee including the manner by which it will be effected and the basis for settlement. (All contracts in excess of $10,000)

(C) Equal Employment Opportunity. Except as otherwise provided under 41 CFR Part 60, all contracts that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 must include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 CFR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

Pursuant to Federal Rule (C) above, when a Participating Agency expends federal funds on any federally assisted construction contract, the equal opportunity clause is incorporated by reference herein.

(D) Davis-Bacon Act, as amended (40 U.S.C. 3141-3148). When required by Federal program legislation, all prime construction contracts in excess of $2,000 awarded by non-Federal entities must include a provision for compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, contractors must be required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, contractors must be required to pay wages not less than once a week. The non-Federal entity must place a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation. The decision to award a contract or subcontract must be conditioned upon the acceptance of the wage determination. The non- Federal entity must report all suspected or reported violations to the Federal awarding agency. The contracts must also include a provision

for compliance with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each contractor or subrecipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency.

(E) Contract Work Hours and Safety Standards Act (40 U.S.C. 3701-3708). Where applicable, all contracts awarded by the non-Federal entity in excess of $100,000 that involve the employment of mechanics or laborers must include a provision for compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, each contractor must be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

(F) Rights to Inventions Made Under a Contract or Agreement. If the Federal award meets the definition of "funding agreement" under 37 CFR §401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

(G) Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended— Contracts and subgrants of amounts in excess of $150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401- 7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251- 1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

(H) Debarment and Suspension (Executive Orders 12549 and 12689)—A contract award (see 2 CFR 180.220) must not be made to parties listed on the government wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), "Debarment and Suspension." SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

(I) Byrd Anti-Lobbying Amendment (31 U.S.C. 1352)—Contractors that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee

of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

RECORD RETENTION REQUIREMENTS FOR CONTRACTS INVOLVING FEDERAL FUNDS

When federal funds are expended by Participating Agency for any contract resulting from this procurement process, offeror certifies that it will comply with the record retention requirements detailed in 2 CFR § 200.333. The offeror further certifies that offeror will retain all records as required by 2 CFR § 200.333 for a period of three years after grantees or subgrantees submit final expenditure reports or quarterly or annual financial reports, as applicable, and all other pending matters are closed.

CERTIFICATION OF COMPLIANCE WITH THE ENERGY POLICY AND CONSERVATION ACT

When Participating Agency expends federal funds for any contract resulting from this procurement process, offeror certifies that it will comply with the mandatory standards and policies relating to energy efficiency which are contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act (42 U.S.C. 6321 et seq.; 49 C.F.R. Part 18).

CERTIFICATION OF COMPLIANCE WITH BUY AMERICA PROVISIONS

To the extent purchases are made with Federal Highway Administration, Federal Railroad Administration, or Federal Transit Administration funds, offeror certifies that its products comply with all applicable provisions of the Buy America Act and agrees to provide such certification or applicable waiver with respect to specific products to any Participating Agency upon request. Purchases made in accordance with the Buy America Act must still follow the applicable procurement rules calling for free and open competition.

Required Clauses for Federal Assistance provided by FTA

ACCESS TO RECORDS AND REPORTS

Contractor agrees to:

a) Maintain all books, records, accounts and reports required under this Contract for a period of not less than three (3) years after the date of termination or expiration of this Contract or any extensions thereof except in the event of litigation or settlement of claims arising from the performance of this Contract, in which case Contractor agrees to maintain same until Public Agency, the FTA Administrator, the Comptroller General, or any of their duly authorized representatives, have disposed of all such litigation, appeals, claims or exceptions related thereto.

b) Permit any of the foregoing parties to inspect all work, materials, payrolls, and other data and records with regard to the Project, and to audit the books, records, and accounts with regard to the Project and to reproduce by any means whatsoever or to copy excerpts and transcriptions as reasonably needed for the purpose of audit and examination.

FTA does not require the inclusion of these requirements of Article 1.01 in subcontracts. Reference 49 CFR 18.39 (i)(11).

CIVIL RIGHTS / TITLE VI REQUIREMENTS

1) Non-discrimination. In accordance with Title VI of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000d, Section 303 of the Age Discrimination Act of 1975, as amended, 42 U.S.C. § 6102, Section 202 of the Americans with Disabilities Act of 1990, as amended, 42 U.S.C. § 12132, and Federal Transit Law at 49 U.S.C. § 5332, Contractor or subcontractor agrees that it will not discriminate against any employee or applicant for employment because of race, color, creed, national origin, sex, marital status age, or disability. In addition, Contractor agrees to comply with applicable Federal implementing regulations and other implementing requirements FTA may issue.

2) Equal Employment Opportunity. The following Equal Employment Opportunity requirements apply to this Contract:

   a. Race, Color, Creed, National Origin, Sex. In accordance with Title VII of the Civil Rights Act, as amended, 42 U.S.C. § 2000e, and Federal Transit Law at 49 U.S.C. § 5332, the Contractor agrees to comply with all applicable Equal Employment Opportunity requirements of U.S. Dept. of Labor regulations, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor, 41 CFR, Parts 60 et seq., and with any applicable Federal statutes, executive orders, regulations, and Federal policies that may in the future affect construction activities undertaken in the course of this Project. Contractor agrees to take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, creed, national origin, sex, marital status, or age. Such action shall include, but not be limited to, the following: employment, upgrading, demotion or transfer, recruitment or recruitment advertising, layoff or termination, rates of pay or other forms of compensation; and selection for training, including apprenticeship. In addition, Contractor agrees to comply with any implementing requirements FTA may issue.

   b. Age. In accordance with the Age Discrimination in Employment Act (ADEA) of 1967, as amended, 29 U.S.C. Sections 621 through 634, and Equal Employment Opportunity Commission (EEOC) implementing regulations, "Age Discrimination in Employment Act", 29 CFR Part 1625, prohibit employment discrimination by Contractor against individuals on the basis of age, including present and prospective

employees. In addition, Contractor agrees to comply with any implementing requirements FTA may issue.

c. Disabilities. In accordance with Section 102 of the Americans with Disabilities Act of 1990, as amended (ADA), 42 U.S.C. Sections 12101 *et seq.*, prohibits discrimination against qualified individuals with disabilities in programs, activities, and services, and imposes specific requirements on public and private entities. Contractor agrees that it will comply with the requirements of the Equal Employment Opportunity Commission (EEOC), "Regulations to Implement the Equal Employment Provisions of the Americans with Disabilities Act," 29 CFR, Part 1630, pertaining to employment of persons with disabilities and with their responsibilities under Titles I through V of the ADA in employment, public services, public accommodations, telecommunications, and other provisions.

d. Segregated Facilities. Contractor certifies that their company does not and will not maintain or provide for their employees any segregated facilities at any of their establishments, and that they do not and will not permit their employees to perform their services at any location under the Contractor's control where segregated facilities are maintained. As used in this certification the term "segregated facilities" means any waiting rooms, work areas, restrooms and washrooms, restaurants and other eating areas, parking lots, drinking fountains, recreation or entertainment areas, transportation, and housing facilities provided for employees which are segregated by explicit directive or are in fact segregated on the basis of race, color, religion or national origin because of habit, local custom, or otherwise. Contractor agrees that a breach of this certification will be a violation of this Civil Rights clause.

3) Solicitations for Subcontracts, Including Procurements of Materials and Equipment. In all solicitations, either by competitive bidding or negotiation, made by Contractor for work to be performed under a subcontract, including procurements of materials or leases of equipment, each potential subcontractor or supplier shall be notified by Contractor of Contractor's obligations under this Contract and the regulations relative to non-discrimination on the grounds of race, color, creed, sex, disability, age or national origin.

4) Sanctions of Non-Compliance. In the event of Contractor's non-compliance with the non-discrimination provisions of this Contract, Public Agency shall impose such Contract sanctions as it or the FTA may determine to be appropriate, including, but not limited to: 1) Withholding of payments to Contractor under the Contract until Contractor complies, and/or; 2) Cancellation, termination or suspension of the Contract, in whole or in part.

Contractor agrees to include the requirements of this clause in each subcontract financed in whole or in part with Federal assistance provided by FTA, modified only if necessary to identify the affected parties.

DISADVANTAGED BUSINESS PARTICIPATION

This Contract is subject to the requirements of Title 49, Code of Federal Regulations, Part 26, *"Participation by Disadvantaged Business Enterprises in Department of Transportation Financial Assistance Programs"*, therefore, it is the policy of the Department of Transportation (DOT) to ensure that Disadvantaged Business Enterprises (DBEs), as defined in 49 CFR Part 26, have an equal opportunity to receive and participate in the performance of DOT-assisted contracts.

1) Non-Discrimination Assurances. Contractor or subcontractor shall not discriminate on the basis of race, color, national origin, or sex in the performance of this Contract. Contractor shall carry out all applicablerequirements of 49 CFR Part 26 in the award and administration of DOT-assisted contracts. Failure by Contractor to carry out these requirements is a material breach of this Contract, which may result in the termination of this Contract or other such remedy as public agency deems appropriate. Each subcontract Contractor signs with a subcontractor must include the assurance in this paragraph. (See 49 CFR 26.13(b)).

2) Prompt Payment. Contractor is required to pay each subcontractor performing Work under this prime Contract for satisfactory performance of that work no later than thirty (30) days after Contractor's receipt of payment for that Work from public agency. In addition, Contractor is required to return any retainage payments to those subcontractors within thirty (30) days after the subcontractor's work related to this Contract is satisfactorily completed and any liens have been secured. Any delay or postponement of payment from the above time frames may occur only for good cause following written approval of public agency. This clause applies to both DBE and non-DBE subcontractors. Contractor must promptly notify public agency whenever a DBE subcontractor performing Work related to this Contract is terminated or fails to complete its Work, and must make good faith efforts to engage another DBE subcontractor to perform at least the same amount of work. Contractor may not terminate any DBE subcontractor and perform that Work through its own forces, or those of an affiliate, without prior written consent of public agency.

3) DBE Program. In connection with the performance of this Contract, Contractor will cooperate with public agency in meeting its commitments and goals to ensure that DBEs shall have the maximum practicable opportunity to compete for subcontract work, regardless of whether a contract goal is set for this Contract. Contractor agrees to use good faith efforts to carry out a policy in the award of its subcontracts, agent agreements, and procurement contracts which will, to the fullest extent, utilize DBEs consistent with the efficient performance of the Contract.

ENERGY CONSERVATION REQUIREMENTS

Contractor agrees to comply with mandatory standards and policies relating to energy efficiency which are contained in the State energy conservation plans issued under the Energy Policy and Conservation Act, as amended, 42 U.S.C. Sections 6321 *et seq.* and 41 CFR Part 301-10.

FEDERAL CHANGES

Contractor shall at all times comply with all applicable FTA regulations, policies, procedures and directives, including without limitation those listed directly or by reference in the Contract between public agency and the FTA, as they may be amended or promulgated from time to time during the term of this contract. Contractor's failure to so comply shall constitute a material breach of this Contract.

INCORPORATION OF FEDERAL TRANSIT ADMINISTRATION (FTA) TERMS

The provisions include, in part, certain Standard Terms and Conditions required by the U.S. Department of Transportation (DOT), whether or not expressly set forth in the preceding Contract provisions. All contractual provisions required by the DOT, as set forth in the most current FTA Circular 4220.1F, dated November 1, 2008, are hereby incorporated by reference. Anything to the contrary herein notwithstanding, all FTA mandated terms shall be deemed to control in the event of a conflict with other provisions contained in this Contract. Contractor agrees not to perform any act, fail to perform any act, or refuse to comply with any public agency requests that would cause public agency to be in violation of the FTA terms and conditions.

NO FEDERAL GOVERNMENT OBLIGATIONS TO THIRD PARTIES

Agency and Contractor acknowledge and agree that, absent the Federal Government's express written consent and notwithstanding any concurrence by the Federal Government in or approval of the solicitation or award of the underlying Contract, the Federal Government is not a party to this Contract and shall not be subject to any obligations or liabilities to agency, Contractor, or any other party (whether or not a party to that contract) pertaining to any matter resulting from the underlying Contract.

Contractor agrees to include the above clause in each subcontract financed in whole or in part with federal assistance provided by the FTA. It is further agreed that the clause shall not be modified, except to identify the subcontractor who will be subject to its provisions.

PROGRAM FRAUD AND FALSE OR FRAUDULENT STATEMENTS

Contractor acknowledges that the provisions of the Program Fraud Civil Remedies Act of 1986, as amended, 31 U.S.C. §§ 3801 et seq. and U.S. DOT regulations, "Program Fraud Civil Remedies," 49 CFR Part 31, apply to its actions pertaining to this Contract. Upon execution of the underlying Contract, Contractor certifies or affirms the truthfulness and accuracy of any statement it has made, it makes, it may make, or causes to me made, pertaining to the underlying Contract or the FTA assisted project for which this Contract Work is being performed.

In addition to other penalties that may be applicable, Contractor further acknowledges that if it makes, or causes to be made, a false, fictitious, or fraudulent claim, statement, submission, or certification, the Federal Government reserves the right to impose the penalties of the Program Fraud Civil Remedies Act of 1986 on Contractor to the extent the Federal Government deems appropriate.

Contractor also acknowledges that if it makes, or causes to me made, a false, fictitious, or fraudulent claim, statement, submission, or certification to the Federal Government under a contract connected with a project that is financed in whole or in part with Federal assistance originally awarded by FTA under the authority of 49 U.S.C. § 5307, the Government reserves the right to impose the penalties of 18 U.S.C. § 1001 and 49 U.S.C. § 5307 (n)(1) on the Contractor, to the extent the Federal Government deems appropriate.

Contractor agrees to include the above clauses in each subcontract financed in whole or in part with Federal assistance provided by FTA. It is further agreed that the clauses shall not be modified, except to identify the subcontractor who will be subject to the provisions.

State Notice Addendum

The National Cooperative Purchasing Alliance (NCPA), on behalf of NCPA and its current and potential participants to include all county, city, special district, local government, school district, private K-12 school, higher education institution, state, tribal government, other government agency, healthcare organization, nonprofit organization and all other Public Agencies located nationally in all fifty states, issues this Request for Proposal (RFP) to result in a national contract.

For your reference, the links below include some, but not all, of the entities included in this proposal:

http://www.usa.gov/Agencies/State_and_Territories.shtml

https://www.usa.gov/local-governments

Appendix: Master Agreement and Matrix

ATTACHMENT 1

PRIVACY SCHEDULE

This Privacy Schedule ("**Privacy Schedule**") forms part of the Master Agreement and the Administration Agreement, subject to which Vendor providers or offers the services listed in Schedule 1 ("**Controller Services**") and/or Schedule 2 ("**Processor Services**") to this Privacy Schedule. For the purposes of this Privacy Schedule, the Master Agreement and Administration Agreement shall collectively be referred to as the "**Agreement**", and NCPA and Region 14 ESC shall be collectively referred to as the "**Referrer**".

PART 1 - DEFINITIONS

1.1. In this Privacy Schedule the following terms shall have the following meanings:

"**Affiliate**" means, with respect to a party, an entity that is Controlled by, Controlling or in common Control with that party, where "Control" means the power to direct or cause the direction of the management and policies of an entity, whether through the ownership of voting shares, by contract or otherwise;

"**Agreement Personal Data**" means any personal data (including any sensitive or special categories of data) that is transmitted, stored or otherwise processed under or in connection with the Agreement;

"**Business Day**" means a day except Saturdays and Sundays and public holidays applicable in the contracting parties' jurisdiction;

"**DP Laws**" means any applicable data protection and privacy laws relating to the protection of individuals with regards to the processing of personal data including but not limited to (i) the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"); (ii) the GDPR as transposed into the national laws of the United Kingdom ("**UK GDPR**"); (iii) Directive 2002/58/EC ("**ePrivacy Directive**"); (iv) the California Consumer Privacy Act of 2018 ("CCPA") and any corresponding or equivalent United States state or federal laws or regulations including any amendment, update, modification to or re-enactment of such laws (together, "**US Privacy Laws**"); and (v) any corresponding or equivalent national laws or regulations including any amendment, supplement, update, modification to or re-enactment of such laws;

"**EEA**" means the European Economic Area;

"**Independent DP Audit**" means a data protection audit conducted by third party auditors to verify compliance with Vendor's obligations under the Processor Obligations under Part 3 of this Privacy Schedule;

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Agreement Personal Data;

"**Restricted Transfer**" means a transfer of the Agreement Personal Data between Referrer (or a and Vendor (or Vendor Affiliate(s)) which, in the absence of the SCCs, would be unlawful under DP Laws;

"**SCCs**" means (i) the standard contractual clauses set out in Commission Implementing Decision (EU)2021/914 for the transfer of personal data to third countries pursuant to GDPR as updated, amended, replaced and superseded from time to time ("**EU SCCs**"); (ii) the standard contractual clauses for the transfer of personal data set out in European Commission Decision C(2004)5271 ("**Controller SCCs**"); the standard contractual clauses for the transfer of personal data set out in European Commission Decision C(2010)593 ("**Processor SCCs**"); or any corresponding or

2

equivalent international data transfer agreement ("**IDTA**") adopted by the supervisory authority in the United Kingdom (together the "**UK SCCs**");

"**Sell[ing]**", "**Sale**", or "**Sold**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means personal data by one business to another business or a third party for monetary or other valuable consideration;

"**Sub-processor**" means another processor or service provider engaged by Vendor as processor to carry out specific processing activities on the Agreement Personal Data; and

The terms "**business**", "**business purposes**", "**controller**", "**data subject**", "**personal data**", "**personal information**", "**processing**", "**processor**", "**sensitive personal data**", "**service provider**", "**special categories of data**", "**supervisory authority**" and "**transfer**" shall have the same meanings ascribed to them under DP Laws, provided that references to the term "personal data" shall be interpreted to include any information defined as "personal information" or any other such similar term as defined in DP Laws.

1.2. Capitalized terms not defined herein shall have the meaning ascribed to them elsewhere in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

PART 2 - PROVISIONS APPLICABLE TO ALL SERVICES

2. **DATA PROTECTION OBLIGATIONS**

2.1. The parties envisage that under the terms of this Privacy Schedule:

(a) Each party is a separate controller or business in respect of the Agreement Personal Data processed for the provision or offering of the services applicable to the Agreement listed in Schedule 1 ("**Controller Services**"); and

(b) Vendor acts as a processor or service provider on behalf of Referrer, who is a controller or business, in respect of the Agreement Personal Data processed for the provision or offering of the services applicable to the Agreement listed in Schedule 2 ("**Processor Services**").

2.2. If, Vendor or its Affiliate(s) (as applicable) agrees to offer services to Referrer which:

(a) are listed in Schedules 1 and/or 2 then the relevant services shall be deemed applicable for the purposes of Schedules 1 and/or 2 from the date of the appropriate services; or

(b) are not covered by Schedule s1 and/or 2, then the parties or their Affiliates (as applicable) may agree in writing to update Schedules 1 and/or 2 to insert details of the relevant services.

2.3. Vendor and its Affiliates may process, transfer and disclose personal data as described in Vendor's privacy notice in particular for (i) the delivery of the Processor Services, (ii) the delivery of the Controller Services; (iii) administration of engagement and general correspondence with Referrer; (iv) screening of individuals associated with Referrer against international sanctioned parties lists; and (v) aggregation, de-identification and, where feasible, full anonymization of personal data for benchmarking, market research and data analysis purposes associated with the development of Vendor and its Affiliates' products and services. Referrer acknowledges and understands that Vendor shall act as a controller or business of any personal data which is processed pursuant to this Clause 2.3 (ii)-(v) and shall comply with DP Laws in respect of such processing.

2.4. Each party shall implement appropriate technical and organizational security measures in relation to the processing of the Agreement Personal Data under or in connection with the Agreement, which shall ensure a level of security appropriate to the risk including, as appropriate, (i) pseudonymization and encryption; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to the Agreement Personal Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of those measures.

2.5. In respect of Clause 2.4 above, Vendor shall maintain a global data governance framework which mandates strict technical and organizational security measures applicable to the processing of Agreement Personal Data including those relating to, without limitation, access control, data handling, malware protection, security organization, system configuration and hardening, personnel security, physical security, business continuity plans and disaster recovery and third party security.

2.6. Vendor shall retain the Agreement Personal Data pursuant to its corporate record retention schedules for the purposes of meeting Vendor's legal and regulatory obligations, and enabling Vendor to establish, exercise or defend legal claims.

PART 3 - PROVISIONS APPLICABLE TO CONTROLLER SERVICES - EEA DP Laws

3. **CONTROLLER OBLIGATIONS:** This Part 2 shall apply only to the extent Vendor's processing of Agreement Personal Data in performance or offering of Controller Services is governed by DP Laws enacted in the EEA, including, but not limited to, the GDPR and the UK GDPR.

3.1. Each party acknowledges, confirms and represents for its own part that, to the extent that it processes Agreement Personal Data as a separate controller:

(a) it will observe all applicable requirements of DP Laws and this Privacy Schedule in relation to its processing of Agreement Personal Data; and

(b) all Agreement Personal Data collected or sourced by it or on its behalf for processing in connection with the Agreement or which is otherwise provided or made available to the other party shall have been collected or otherwise obtained in compliance with DP Laws, and may be processed, disclosed and transferred as described in or in connection with the Agreement.

3.2. The parties will work together in good faith to ensure the information prescribed by DP Laws is made available to relevant data subjects, including where necessary the Referrer's provision of such information to data subjects on Vendor's behalf.

3.3. If either party receives any complaint, notice or communication from a supervisory authority which relates to the other party's: (i) processing of the Agreement Personal Data; or (ii) potential failure to comply with DP Laws in respect of the Agreement Personal Data, that party shall direct the supervisory authority to the other party.

3.4. If a data subject makes a written request to a party to exercise any of their rights in relation to the Agreement Personal Data that concerns processing of the other party, that party shall direct the data subject to that other party. Where such a request relates to the processing of Agreement Personal Data by Vendor as processor on behalf of the Referrer, the obligations set out in Clause 3.5 below shall apply.

3.5. If either party becomes aware of a Personal Data Breach that requires notification to a supervisory authority, it shall notify the other party without undue delay, and each party shall co-operate with

the other, to the extent reasonably requested, in relation to any notifications to supervisory authorities and/or to affected data subjects.

PART 4 - PROVISIONS APPLICABLE TO PROCESSOR SERVICES - EEA DP Laws

4. **PROCESSOR OBLIGATIONS:** This Part 3 shall apply only to the extent Vendor's processing of Agreement Personal Data in performance or offering of Processor Services is governed by DP Laws enacted in the EEA, including, but not limited to, the GDPR and the UK GDPR.

4.1. Vendor shall process the Agreement Personal Data only in accordance with Referrer's instructions as set out in the Agreement, or from time to time by written agreement of the parties, including as to the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, in each case, which are more specifically set out in Attachment 2, unless required by law to act without such instructions, in which case Vendor shall, to the extent legally permitted, promptly inform Referrer upon becoming aware of such legal requirement.

4.2. If Vendor considers that any instructions from Referrer relating to processing of Agreement Personal Data may put Vendor in breach of DP Laws, Vendor will inform Referrer and will be entitled not to carry out that processing and will not be in breach of the Agreement or otherwise liable to Referrer as a result of its failure to carry out that processing.

4.3. Vendor shall ensure that any personnel, agents and/or contractors who process the Agreement Personal Data are subject to appropriate contractual or statutory obligations of confidentiality.

4.4. Vendor shall implement appropriate technical and organizational security measures as described in Clauses 2.4 and 2.5.

4.5. In relation to the Agreement Personal Data, taking into account the nature of the processing activities, and the information available to Vendor, Vendor shall, upon written request, provide reasonable assistance to Referrer in ensuring compliance with Referrer's obligations under DP Laws with respect to:

(a) responding to requests by data subjects in relation to their rights under DP Laws;

(b) the performance of data protection impact assessments and prior consultation with a supervisory authority regarding high-risk processing; and

(c) without prejudice to Clause 4.5(a), where Vendor receives a request directly from a data subject exercising their rights under DP Laws in relation to the Agreement Personal Data, Vendor shall forward the request to the Referrer promptly, and in any event within five (5) Business Days from the date on which Vendor received such request, and will provide reasonable assistance to Referrer to enable Referrer to respond to that request.

4.6. At Referrer's choice and request, Vendor shall delete or return the Agreement Personal Data to Referrer at the end of the term of the Agreement and delete any copies of the Agreement Personal Data unless it is required to retain such copies pursuant to applicable law.

4.7. Vendor will, upon becoming aware, notify Referrer without undue delay of any Personal Data Breach and will provide reasonable assistance to Referrer in response to such Personal Data Breach, to enable Referrer to meet its obligations under DP Laws as regards the notification to supervisory authorities and/or affected data subjects. For these purposes Vendor will provide Referrer all details as required by applicable DP Laws including Article 33 of the GDPR. The parties agree that such details may be provided to Referrer in phases and to the extent these are known to Vendor.

4.8. Vendor is hereby generally authorized by Referrer to engage any Sub-processor, provided that Vendor shall (i) ensure in each case that the Sub-processor is bound by data protection obligations that are substantially the same as those contained in the Agreement; (ii) subject to the terms of the Agreement (including but not limited to any limitations on liability agreed therein), remain fully liable to Referrer for the performance of that Sub-processor's obligations; and (iii) provide a list of all such Sub-processors to Referrer upon written request.

4.9. Upon request, Vendor shall notify Referrer of any intended changes concerning the addition or replacement of Sub-processors, thereby giving Referrer the opportunity to object to such changes. Notwithstanding anything to the contrary in the Agreement, the parties expressly agree that such notice may be provided via any medium including but not limited to email, a public website or a web-based portal.

4.10. Referrer agrees that Vendor may continue to use those Sub-processors already engaged by Vendor or any Vendor Affiliates as at the date of this Privacy Schedule provided that in each case as practicable Vendor meets the obligations set out in Clause 4.8 (i)(ii) and (iii) above.

4.11. Vendor shall, on written request, (i) make available to Referrer information that is reasonably necessary to demonstrate compliance with Vendor's Processor Obligations and (ii) allow for and contribute to audits, including inspections, conducted by Referrer or another auditor mandated by Referrer, but in each case only if such information and audits are in relation to the Agreement Personal Data processed pursuant to the Agreement. Vendor shall notify Referrer in writing if it believes in good faith that the exercise of rights under this Clause 4.11 would infringe DP Laws.

4.12. Referrer agrees to exercise its rights for information, audits and inspections under Clause 4.11 above by permitting Vendor to carry out an Independent DP Audit, pursuant to which Vendor agrees to provide Referrer, upon written request, with a confidential audit report to enable Referrer to reasonably verify Vendor's compliance with its Processor Obligations under the Privacy Schedule.

4.13. Notwithstanding Clause 4.12, in the event of a Personal Data Breach, Referrer shall be entitled on ten (10) Business Days' prior notice to Vendor, during normal business hours, causing minimal disruption and subject to Vendor's obligations of confidentiality to carry out an audit of Vendor to reasonably verify Vendor's compliance with its Processor Obligations, subject to the requirements of Clause 4.11.

4.14. Should any audit report identify material non-compliance with Vendor's Processor Obligations, the parties shall work together in good faith to mutually agree steps to reasonably address such non-compliance.

4.15. The parties acknowledge that Agreement Personal Data may be transferred or otherwise processed or transferred outside the United Kingdom and the EEA ("**International Transfers**") by Vendor including by any Sub-processors engaged in accordance with the Agreement, provided that such International Transfer is made in compliance with DP Laws, including, if applicable, by adoption of SCCs, or such other international transfer mechanism that effectively complies with DP Laws.

PART 5 - PROVISIONS APPLICABLE TO BUSINESS OR SERVICE PROVIDER - US PRIVACY LAWS

5. **BUSINESS OR SERVICE PROVIDER OBLIGATIONS:** This Part 4 applies only to the extent US Privacy Laws apply to Vendor's processing of Agreement Personal Data.

5.1. To the extent Vendor is providing or offering Controller Services pursuant to the Agreement, Referrer has contractually engaged Vendor to perform or offer the Controller Services in support of one of more permissible Business Purposes. In order for Vendor to provide or offer the Controller Services to Referrer and to perform its obligations under the Agreement, Referrer must provide, direct others to provide, or otherwise make available (herein, collectively "provide") to Vendor

certain data, including Agreement Personal Data (the "**Relevant Data**"). Referrer agrees to provide to Vendor the Relevant Data that is necessary for Vendor's performance of its obligations under the Agreement, and to only provide such personal data as is reasonably necessary to the performance or offering of the Controller Services. The parties agree that (i) Vendor is not able to perform its obligations to Referrer under the Agreement unless Referrer provides the Relevant Data, (ii) the Relevant Data is necessary to the performance or offering of the Controller Services in support of Referrer's Business Purposes, and (iii) the personal data is not provided to Vendor in exchange for any monetary or other valuable consideration from Vendor to Referrer. Vendor does not Sell any personal data as part of the Controller Services provided or offered under the Agreement.

5.2. To the extent that Vendor provides or offers Processor Services pursuant to the Agreement, the parties intend and agree that Referrer is a Business and Vendor is a Service Provider for the purposes of and as defined by the CCPA in respect of the Agreement Personal Data processed pursuant to the Processor Services which Vendor provides or offers to Referrer under the Agreement. Vendor shall only retain, use, or disclose Agreement Personal Data under this Privacy Schedule for the specific purpose of performing or offering the services under the Agreement and this Privacy Schedule. Vendor does not Sell any Personal Information as part of the Processor Services provided under the Agreement.

PART 6 - PROVISIONS APPLICABLE TO RESTRICTED TRANSFERS – EEA DP Law

6. **RESTRICTED TRANSFERS OBLIGATIONS:**

6.1. With respect to Restricted Transfers subject to the GDPR, the EU SCCs are hereby incorporated into this Agreement by reference and the following terms shall apply and the description of the transfer (Annex 1 of the EU SCCs) is as set out in the Appendices to this Privacy Schedule:

(a) For the purposes of Modules 1 and 2 of the EU SCCs: Clause 7 and the optional language in clause 11(a) shall not apply, for the purposes of clause 9, the parties select Option 2 (general authorization), the supervisory authority for the purposes of clause 13(a) shall be determined by the place of establishment of the data exporter, the governing law and choice of forum and jurisdiction stipulated in the Agreement shall apply to the extent that it is the law and the courts of an EU member state otherwise it shall be those of the Republic of Ireland and the technical and organizational security measures set out in Clauses 2.4 and 2.5 shall apply. The frequency of the transfer shall be continuous, as necessary to deliver the Controller and Processor Services, and retention shall be determined by the data exporter(s), except where the data importer(s) is required by applicable laws to retain Agreement Personal Data in accordance with its corporate record retention schedules and policies.

6.2. With respect to Restricted Transfers subject to the UK GDPR, the UK SCCs are hereby incorporated into this Agreement by reference and the following terms shall apply and the description of the transfer is as set out in the Appendices to this GDPR Schedule for the purposes of Annex B of the Controller SCCs and Schedule 1 of the Processor SCCs and/or any equivalent IDTA:

(a) For the purposes of the Controller SCCs: at clause 2(h) of the Controller SCCs, the parties select option (iii). The data subjects, categories of personal data and the purposes of the transfer are as specified in Schedule 1 to this GDPR Schedule; the recipients are the recipients to whom it is necessary to disclose data to achieve the purposes; and the contact points for data protection enquiries are the usual business contacts for each party.

(b) For the purposes of the Processor SCCs: Schedules 1 and 2 of the Processor SCCs shall be deemed to incorporate respectively the data subjects, categories of personal data and

processing operations set out in Schedule 2 of this GDPR Schedule and the organisational and technical measures described in Clauses 2.4 and 2.5.

6.3. For the avoidance of doubt (and without prejudice to third party rights for data subjects under the SCCs) the parties hereby submit to the limitations stipulated in the Agreement with respect to their respective liability towards one another under the SCCs.

6.4. If at any time the supervisory authority in the United Kingdom approves the EU SCCs for use under the UK GDPR, the provisions of Clause 6.1 shall apply in place of Clause 6.2 in respect of Restricted Transfers subject to the UK GDPR, subject to any modifications to the EU SCCs required by the UK GDPR (and subject to the governing law of the EU SCCs being English law).

8

Schedule 1: Controller Services

Description of processing			
Where applicable, for the purposes of Annex 1 to Module 1 of the EU SCCs, Annex B of the Controller SCCs and/or any IDTA, the data exporter(s) is the party disclosing the Agreement Personal Data and the data importer(s) is the party receiving the Agreement Personal Data. The Agreement Personal Data is processed for the purposes of providing or offering the Controller Services listed below and is processed for the duration of the Agreement. Processing operations may be set out more specifically in the Agreement.			
Solution Line	**Service Offering**	**Type of Personal Data**	**Categories of Data Subject**
Cyber Solutions	**Due diligence, forensic accounting, investigatory, and intelligence gathering**	• Personal details • Financial details • Family, lifestyle & social circumstances • Employment details • Business related activities • Criminal or civil litigation records • Personal data may also concern the following special categories of data: data concerning health, data concerning a natural person's sex life or sexual orientation	• Referrer's current or former employees and representatives • Referrer's users or customers • Referrer's suppliers/contractors • Members of the public

Schedule 2: Processor Services

Description of processing			
Where applicable, for the purposes of Annex 1 to Module 2 of the EU SCCs and Appendix 1 of the Processor SCCs and/or any IDTA, the data exporter(s) is the party disclosing the Agreement Personal Data and the data importer(s) is the party receiving the Agreement Personal Data. The Agreement Personal Data is processed for the purposes of providing or offering the Processor Services listed below and is processed for the duration of the Agreement. Processing operations may be set out more specifically in the Agreement.			
Solution Line	**Service Offering**	**Type of Personal Data**	**Categories of Data Subject**
Cyber Solutions	**Cyber security services and electronic discovery**	The nature of the personal data is data present in materials, devices or systems disclosed to Vendor under this Agreement, including: • Personal details • Financial details • Family, lifestyle & social circumstances • Employment details • Business related activities • Personal data may also concern the following special categories of data: data concerning health, data concerning a natural person's sex life or sexual orientation	• Referrer's current or former employees and representatives • Referrer's users or customers • Referrer's suppliers/contractors • Members of the public

Aon NCPA State Service Matrix

Please see attached excel titled:
Aon NPCA State Service Matrix

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

www.aon.com

Empower Results®