

Solicitation # 34-21

Cyber Security Solutions, Malware, Ransomware Protections, Other related products and services.



Due: November 18th, 2021 @ 2:00PM CST

Submitted To:
National Cooperative Purchasing Alliance

Submitted By:
David Wiese
United Data Technologies
100 Congress Avenue Suite 2000
Austin, TX 78701
Phone: 512-466-3405
Email: dwiese@udtonline.com

Table of Contents

Cover Page	1
Table of Contents	1
Executive Summary	3
TAB 1 - Master Agreement / Signature Form	5
Signature Form	12
TAB 2 - NCPA Administration Agreement	13
TAB 3 - Vendor Questionnaire	16
TAB 4 - Vendor Profile	19
NMSDC Minority Certificate	30
State of Florida Certification	31
Broward County Local Business Tax	33
UDT W-9	34
TAB 5 - Product and Services / Scope	35
TAB 6 - References	50
TAB 7 - Pricing (See Attached Excel)	
TAB 8 - Value Added Products and Services	59
TAB 9 - Required Documents	63
Clean Air and Water Act & Debarment Notice	64
Contractor Requirements	65
Antitrust Certification Statements	66
Required Clauses for Federal Funds Certifications	67
Required Clauses for Federal Assistance provided by FTA	70
State Notice Addendum	74



Executive Summary

Founded in 1995 by Henry Fleches and Gerard Amaro, United Data Technologies (UDT) is a 100% certified (NMSDC) minority (Hispanic) owned and operated firm that has become an industry-leading technology enabler and solutions provider. Since the firm's inception, Mr. Fleches, Mr. Amaro, and staff have focused on UDT's corporate vision to "*accomplish more*" by supporting the firm's clients as they navigate a hyper-connected world by providing outstanding customer support, innovative technology, and cost-saving solutions.

Since UDT's founding, the company has grown both its infrastructure and capabilities. UDT started with its headquarters in Doral, Florida, eventually building a new location and relocating to Miramar, Florida. Over the years, UDT has added two state-of-the-art facilities in the Orlando area. UDT's current Configuration Center has serviced the firm's configuration and deployment needs for more than nine years and is transitioning into a dedicated UDT Customer Support Center (CSC) to expand capacity and capability to support extensive enterprise efforts. The UDT CSC has been re-designed to meet fleet management challenges through dedicated depot workflows, inventory controls, contingent storage capabilities, technician expansion, and business continuity priorities through safe social distancing in case of the ongoing pandemic. Currently, UDT is also opening a new state-of-the-art Customer Integration Center (CIC). This purpose-built facility will be wholly dedicated to increasing First Touch Services (imaging, etching, tagging, warehousing, and delivery). The CIC will have the capacity to support the firm's clients and provide the ability to turn around fully configured devices more efficiently with higher daily volumes and the ability to warehouse more than three times UDT's current storage capacity. UDT's CIC will also allow for continuity of operations to minimize the impact of natural disasters and pandemic situations.

In addition to these two facilities, UDT maintains a 24/7 Help Desk and a Network Operations Center (NOC). The NOC is located in a safeguarded location where UDT's experts work to monitor all customer devices, track activity, and handle issues in real-time. UDT also has physical locations in Oklahoma, Tennessee, and Texas. In addition to firm facilities, UDT maintains an extensive fleet of vehicles and logistical support operations tools, such as UDT's Asset Tracking and Management System (ATMS).

Regarding capabilities, UDT, in its infancy, began supporting K-12 educational organizations based in Florida. This support of K-12 educational organizations expanded to include commercial and government organizations. With this expansion, UDT increased its corporate capabilities to offer services that include consulting, selection, procurement, configuration, deployment, integration, in and out of warranty support, as well as asset disposition. As the years have passed, UDT has leveraged its extensive experience, permitting the firm to simplify its technology procurement and



implementation plans, processes, and resources to execute long-term strategies that allow UDT to quickly adapt to new situations, such as the COVID-19 pandemic.

Over the years, UDT has also expanded its security services. The firm's inclusion of a comprehensive security offering is a direct result of the need UDT witnessed among clients in response to cyberattacks experienced within their respective industries. UDT has invested heavily in its security practice and continues to expand and enhance its offerings to provide UDT clients with a total technology solution. UDT employs certified security professionals who are experts in their respective practice areas such as penetration testing, security, and vulnerability assessment, risk assessment, and incident response. As a result of UDT's security experience and expertise, in 2019, the firm introduced its UDTSecure™ product, an advanced suite of managed security and threat intelligence services and solutions that help secure assets and enhance overall security posture.

UDT's infrastructure and capabilities are further enhanced by the firm's 210 plus dedicated employees who day-in and day-out provide UDT clients with exceptional service and truly embrace the firm's corporate values and mission.

Throughout UDT's history, a high value has been placed on the firm's partnerships with its clients and industry partners. UDT proudly supports a wide range of public and commercial clients. In the commercial sector, the firm supports companies such as Petco, Auto Nation, Marriott, and Del Monte. UDT also counts several major Federal organizations as clients, including the Department of State, Department of the Navy, and Department of Energy. Regarding our support of state, local, and educational institutions, UDT supports the State of Texas, the State of Tennessee, the State of North Carolina, and the State of Florida. Concerning our long-established commitment to K-12 educational organizations, UDT currently provides products and services to five of the largest school districts in Florida and, in total, supports over 40 school districts in the state.

UDT has been an active member on advisory boards for some of the leading technology innovators such as Intel, Microsoft, HPI, Cisco, Samsung, and Lenovo. Due to UDT's presence in the market, the firm is able to stay at the forefront of leading-edge technologies while providing valuable insight to its partners regarding the industries the firm supports, resulting in benefits to UDT's clients.

Over the last 26 years, UDT's demonstrated excellence has been recognized by clients and industry publications. UDT has been the recipient of series of awards, including Inc.500, CRN's Top 150, and the South Florida Business Journal as one of South Florida's 50 fastest-growing private companies. UDT's continued focus on commercial entities, state and local governments, and educational organizations have propelled UDT to be the largest privately held technology company headquartered in Florida.

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. Region 14 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	United Data Technologies
Address	100 Congress Avenue Suite 2000
City/State/Zip	Austin, Texas 78701
Telephone No.	512*466-3405
Fax No.	954-432-5203
Email address	dwiese@udtonline.com
Printed name	David Wiese
Position with company	Vice President
Authorized signature	<i>David Wiese</i>

Tab 2 – NCPA Administration Agreement

This Administration Agreement is made as of December 13, 2021, by and between National Cooperative Purchasing Alliance (“NCPA”) and United Data Technologies, Inc. (“Vendor”).

Recitals

WHEREAS, Region 14 ESC has entered into a certain Master Agreement dated December 13, 2021, referenced as Contract Number 01-134, 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 _____

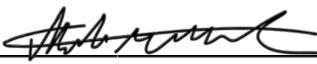
- Each quarter NCPA will invoice the vendor based on the total of sale amount(s) reported. From the invoice the vendor shall pay to NCPA an administrative fee based upon the tiered fee schedule below. Vendor’s annual sales shall be measured on a calendar year basis. Deadline for term of payment will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

<u>Annual Sales Through Contract</u>	<u>Administrative Fee</u>
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:	United Data Technologies
Name: <u>Matthew Mackel</u>	Name: <u>David Wiese</u>	
Title: <u>Director, Business Development</u>	Title: <u>Vice President</u>	
Address: <u>PO Box 701273</u>	Address: <u>100 Congress Avenue Ste 2000</u>	
<u>Houston, TX 77270</u>	<u>Austin, Texas 78701</u>	
Signature: <u></u>	Signature: <u>David Wiese</u>	
Date: <u>December 13, 2021</u>	Date: <u>11-18-21</u>	

Tab 3 – Vendor Questionnaire

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

◆ 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.

50 States & District of Columbia (Selecting this box is equal to checking all boxes below)

- | | | |
|---|---|---|
| <input type="checkbox"/> Alabama | <input type="checkbox"/> Maryland | <input type="checkbox"/> South Carolina |
| <input type="checkbox"/> Alaska | <input type="checkbox"/> Massachusetts | <input type="checkbox"/> South Dakota |
| <input type="checkbox"/> Arizona | <input type="checkbox"/> Michigan | <input type="checkbox"/> Tennessee |
| <input type="checkbox"/> Arkansas | <input type="checkbox"/> Minnesota | <input type="checkbox"/> Texas |
| <input type="checkbox"/> California | <input type="checkbox"/> Mississippi | <input type="checkbox"/> Utah |
| <input type="checkbox"/> Colorado | <input type="checkbox"/> Missouri | <input type="checkbox"/> Vermont |
| <input type="checkbox"/> Connecticut | <input type="checkbox"/> Montana | <input type="checkbox"/> Virginia |
| <input type="checkbox"/> Delaware | <input type="checkbox"/> Nebraska | <input type="checkbox"/> Washington |
| <input type="checkbox"/> District of Columbia | <input type="checkbox"/> Nevada | <input type="checkbox"/> West Virginia |
| <input type="checkbox"/> Florida | <input type="checkbox"/> New Hampshire | <input type="checkbox"/> Wisconsin |
| <input type="checkbox"/> Georgia | <input type="checkbox"/> New Jersey | <input type="checkbox"/> Wyoming |
| <input type="checkbox"/> Hawaii | <input type="checkbox"/> New Mexico | |
| <input type="checkbox"/> Idaho | <input type="checkbox"/> New York | |
| <input type="checkbox"/> Illinois | <input type="checkbox"/> North Carolina | |
| <input type="checkbox"/> Indiana | <input type="checkbox"/> North Dakota | |
| <input type="checkbox"/> Iowa | <input type="checkbox"/> Ohio | |
| <input type="checkbox"/> Kansas | <input type="checkbox"/> Oklahoma | |
| <input type="checkbox"/> Kentucky | <input type="checkbox"/> Oregon | |
| <input type="checkbox"/> Louisiana | <input type="checkbox"/> Pennsylvania | |
| <input type="checkbox"/> Maine | <input type="checkbox"/> Rhode Island | |

All US Territories and Outlying Areas (Selecting this box is equal to checking all boxes below)

American Samoa

Northern Marina Islands

Federated States of Micronesia

Puerto Rico

Guam

U.S. Virgin Islands

Midway Islands

◆ **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

◆ **Residency**

➤ Responding Company's principal place of business is in the city of Miramar,
State of Florida

◆ **Felony Conviction Notice**

➤ Please Check Applicable Box;

A publically 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

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

◆ **Distribution Channel**

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

Manufacturer Direct Certified education/government reseller

Authorized Distributor Manufacturer marketing through reseller

Value-added reseller Other: _____

◆ **Processing Information**

➤ Provide company contact information for the following:

▪ **Sales Reports / Accounts Payable**

Contact Person: Julia Salas

Title: DSO Admin

Company: United Data Technologies, Inc.

Address: 2900 Monarch Lakes Blvd. Suite 300

City: Miramar State: Florida Zip: 33027

Phone: 800-882-9919 Email: jsalas@udtonline.com

- Purchase Orders

Contact Person: Seymour Chajet
Title: Account Support Manager
Company: United Data Technologies, Inc.
Address: 2900 Monarch Lakes Blvd. Suite 300
City: Miramar State: Florida Zip: 33027
Phone: 800-882-9919 Email: schajet@udtonline.com

- Sales and Marketing

Contact Person: David Wiese
Title: Vice President
Company: United Data Technologies, Inc.
Address: 100 Congress Avenue Ste 2000
City: Austin State: Texas Zip: 78701
Phone: 512-466-3405 Email: dwiese@udtonline.com

- ◆ Pricing Information

- In addition to the current typical unit pricing furnished herein, the Vendor agrees to offer all future product introductions at prices that are proportionate to Contract Pricing.
 - If answer is no, attach a statement detailing how pricing for NCPA participants would be calculated for future product introductions.
 Yes No
- Pricing submitted includes the required NCPA administrative fee. The NCPA fee is calculated based on the invoice price to the customer.
 Yes No
- Vendor will provide additional discounts for purchase of a guaranteed quantity.
 Yes No

Tab 4 – Vendor Profile

Please provide the following information about your company:

- Company's official registered name.

UDT Response:

United Data Technologies dba UDT

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

UDT Response:

Founded in 1995 by Henry Fleches and Gerard Amaro, United Data Technologies (UDT) is a 100% certified (NMSDC) minority (Hispanic) owned and operated firm that has become an industry-leading technology enabler and solutions provider. UDT is a technology integrator with over 25 years of experience providing a wide range of products, services, and solutions to its clients, including services such as – managed infrastructure services, managed security services, managed cloud, cybersecurity professional consulting, incident response, continuous Security Information and Event Management (SIEM) monitoring, information assurance, and Auditing services. Our firm has offices in 14 different locations in Florida, Texas, Oklahoma, and Tennessee and serves over 5,000 clients across the US.

Additional Facts about UDT:

- Partners with Cisco, Microsoft, HPE, HP Inc, Intel, and others
- Ranked as one of the 50 fastest growing IT companies in the US (Everything Channel)
- Winner of Microsoft's 2016 Azure Acceleration, 2015 Triple Crown, 2015 CRN awards, and more
- Lead advisory council participant in – HP Public Sector, Cisco Advisory, Microsoft Cloud Solution, HP CEO roundtable, etc.
- 100% certified (NMSDC) minority (Hispanic) owned and operated firm.
- Team of over 250 hand-picked experts that are carefully screened and evaluated, engineers, consultants, strategists, and specialists.
- Company culture that prioritizes integrity, excellence, and teamwork.
- Community outreach programs that focus on giving back with a smile.

Established in 2010, UDT's Cybersecurity capabilities consist of Cybersecurity Assessment and Advisory Services and Managed Security Solutions. Our advisory services focus on providing Clients with auditing and assessment services of all types and complexities regardless of industry and geographical location. UDT's fully certified team of Information Security Consultants have no fewer than 5 years of

experience in performing information security assessments of all types and are full-time employees of UDT. Our regulatory compliance risk assessment services include Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), General Data Protection Regulation (GDPR), Federal Financial Institutions Examination Council's (FFIEC)-based, Payment Card Industry Data Security Standard (PCI DSS) Audits, ISO 27001, and NIST.

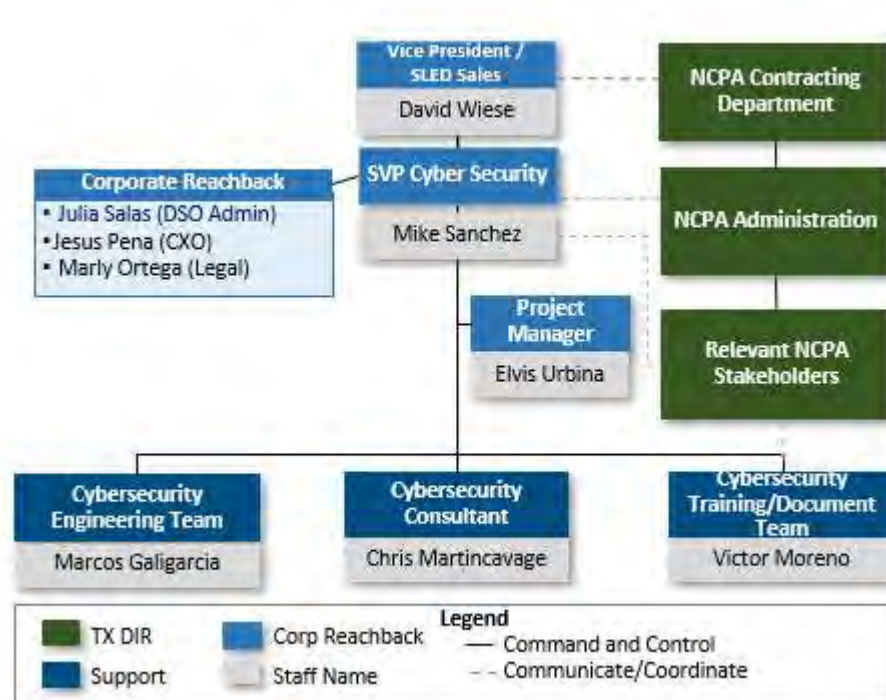
- Company's Dun & Bradstreet (D&B) number.

UDT Response:

United Data Technologies (UDT) D&B Number is 93-364-0682

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

UDT Response:



- 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.

UDT Response:

Team Member	Title	Address	Phone Number	Email
David Wiese	Vice President of SLED Sales - Midwest	100 Congress Avenue Suite 2000 Austin, TX 78701	Phone: 512-466-3405	dwiese@udtonline.com
Brandon Bryant	General Manager - Central	13900 N. Portland Avenue Suite 170 Oklahoma City, OK 73134	Phone: 405 567-4080	bbryant@udtonline.com
Tony Cossio	Vice President of SLED Southeast	2900 Monarch Lakes Blvd. Miramar, FL 33027	Phone: 800-882-9919 Ext. 5146	tcossio@udtonline.com
Paula Euse	VP Marketing	2900 Monarch Lakes Blvd. Miramar, FL 33027	Phone:	peuse@udtonline.com
Marly Ortega	Legal / Contract Management	2900 Monarch Lakes Blvd. Miramar, FL 33027	Phone: 800-882-9919 Ext 5256	legalsupport@udtonline.com
Mike Sanchez Chief Information Security Officer	Chief Information Security Officer	2900 Monarch Lakes Blvd. Miramar, FL 33027	Phone: 954-554-9674	Msanchez@udtonline.com
Elvis Urbina	Project Management	2900 Monarch Lakes Blvd. Miramar, FL 33027	Phone: 305-606-6214	Eurbina@udtonline.com
Marcos Galigarcia	Senior Cyber Security Consultant	2900 Monarch Lakes Blvd. Miramar, FL 33027	Phone: 800-882-9919	mgaligarcia@udtonline.com
Noah Witte	Senior Cyber Security Engineer	2900 Monarch Lakes Blvd. Miramar, FL 33027	Phone: 800-882-9919	nwitte@udtonline.com
Victor Moreno	Cyber Security Consultant	2900 Monarch Lakes Blvd.	Phone: 800-882-9919	vmoreno@udtonline.com

Team Member	Title	Address	Phone Number	Email
		Miramar, FL 33027		

UDT Locations:

HEADQUARTERS	2900 Monarch Lakes Blvd. Suite 300 Miramar, FL, 33027 P: (954) 308-5100	TEXAS	100 Congress Avenue Suite 2000 Austin, TX 78701 P: (512) 466-3405
MIAMI LAKES	14042 N.W. 82nd Ave. Miami, FL 33016 P: (786) 364-6097	ORLANDO CUSTOMER SUPPORT CENTER	9436 Southridge Park Ct. Suite 800 Orlando, FL 32819 P: (800) 882-9919
TALLAHASSEE	1621 Metropolitan Blvd. Suite 102 Tallahassee, FL 32308 P: (850) 329-6215	ORLANDO CUSTOMER INTEGRATION CENTER	2612 Consulate Drive, Suite 100 Orlando, FL 32819 P: (800) 882-9919
TAMPA	5426 Bay Center Dr. Suite 725 Tampa, FL 33609 P: (800) 882-9919	OKLAHOMA	13900 N. Portland Ave. Suite 170 Oklahoma City, OK 73134 P: (405) 567-4080
TENNESSEE	209 10TH Ave. South Suite 530 Nashville, TN 37203 P: (615) 567-4080		

- Define your standard terms of payment.

UDT Response:

UDT Standard Payment Terms Are Net 30 Days.

- Who is your competition in the marketplace?

UDT Response:

UDT competitors include other security and solution providers such Mandiant, Accenture, CDW, and AT&T.

- What differentiates your company from competitors?

UDT Response:

UDT has established its reputation as the technology resource of choice for its clients in Commercial Enterprise and Small Business, Federal/State/Local government, and Education. Our organization subscribes to a Total Solutions approach that includes consulting, design, engineering, product procurement, systems integration, and support services. UDT takes the guesswork out of the process, creating customized integration plans and sketching out detailed, long-term strategies that align with our clients' business objectives

- Describe how your company will market this contract if awarded.

UDT Response:

The following marketing plan will be managed by United Data Technologies Marketing Department at the corporate office and there is a commitment at the Executive level to execute to this plan.

The following includes a detail of all the Marketing Activities which are part of the overall Marketing Plan for the region.

Marketing Generation Campaigns: These will be all based on demand generation activities like Events, specifically around lunch and learns, demo days. We will create integrated campaigns around a demo center and hands on trainings. The funding will also be invested in building a

demo center to bring our customers/prospects to and create demand around these products and services available through this contract.

1) Demand Generation Events

- Email Marketing Campaigns
- Seminars/Event
- Customer Briefings
- Industry Tradeshows
- Online Digital Marketing Campaigns

2) Telemarketing Campaigns

- White Space
- Existing Customers – New Opportunities

Based on any upcoming activities, each quarter UDT will work with the VP of Sales to create a plan that is beneficial for both parties based on current funding, initiatives and as needed.

- Describe how you intend to introduce NCPA to your company.

UDT Response:

UDT provides ongoing training for our Sales team. Any Account Manager doing business with State, Local and Education agencies are required to attend the training. They will be trained on the terms, conditions, product, services, and fees associated with this contract upon award.

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

UDT Response:

UDT will also provide each NCPA member procurement department access to UDT E-Store. The UDT E-Store is located at xchange.udtonline.com. UDT will provide the users identified by the district’s personnel. Purchasing and IT will have the ability to browse the catalog showing rich content descriptions and photos, and complete technical specifications. Agency or School District Standards and contract pricing will be reflected on store-site.

UDT will work with the district’s Purchasing Team to determine the access and views allowed to end-users.

Accessing the store -

- Store can be made public or private based on to whom you want to provide access
- Quick & Easy registration for new Users.

UDTXchange

Returning Customer

Email (Your email Address) *

SAMPLE@ISD.com

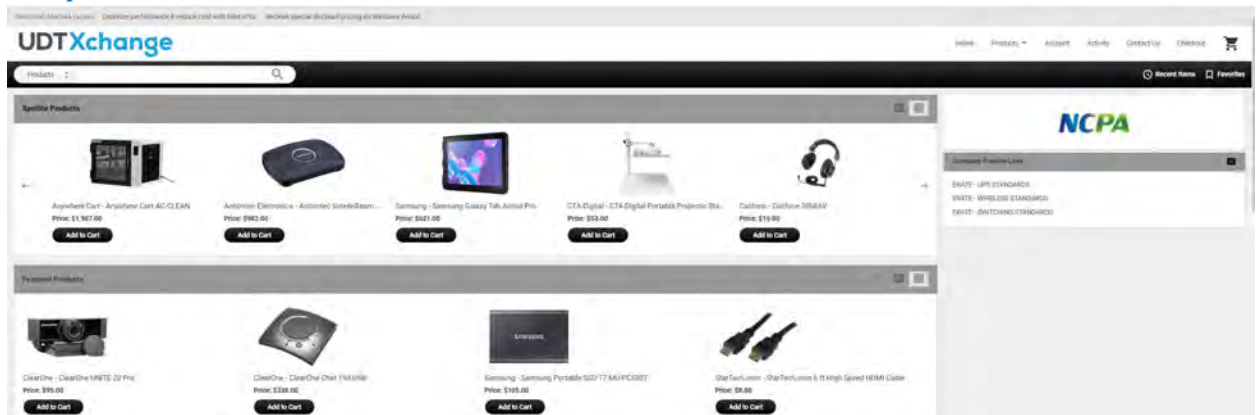
Password *

Remember E-mail

Login


[Forgot Password?](#)

Sample E-Store Screenshot



Catalog & Content

- Adding a new product/catalog is quick and easy. We currently have a catalog of 1M + IT SKU's coming from multiple distributors.
- Rich content like Images, Tech Specs, Long description, Brochures, Related and similar products etc.
- Easy to order pre-configured bundles and standards
- Contract Catalog- Ability to handle contract specific SKUs
- Ability to associate multiple contracts to a buyer so that they can browse and buy from multiple contracts
- EPEAT, 508 etc. compliance & other Green Compliance Data



F5 Networks - F5 BIG-IP Advanced Web Application Firewall i11800
Security appliance - 10 GigE, 40 Gigabit LAN - 1U - rack-mountable

Manufacturer:	F5 Networks
Part #:	F5-BIG-AWF-i11800
UPC:	N/A
Replacement Product:	N/A
Product Condition:	New

Overview **Specifications** Related Products Product Review

Specifications

Main Specifications

Product Description	F5 BIG-IP Advanced Web Application Firewall i11800 - security appliance
Device Type	Security appliance
Form Factor	Rack-mountable - 1U

Searching on Store

- Powerful search engine with guided "refine search" and filtering capability
 - Advanced Search supported on Store
 - Parametric Search Supported on Store
 - Side by Side Comparison between two or more products
 - Favorites – both login-based favorites and organization wide favorites supported.
- 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.

UDT Response:

All work is performed within United States. Please find percentage of worked performed by each group.

Employees	Contractors/Subcontractors
80%	20%

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

UDT Response:

UDT Cybersecurity Consultants average no less than ten (10) years' experience conducting information security-based assessments and technical evaluations. Each have obtained advanced University Degrees in the areas of Computer Sciences, Industrial and System Engineering disciplines. All consultants are recruited through

a rigorous selection process that includes a comprehensive background check for criminal records, verification of past employment, credit history, and are undergo drug tested prior to onboarding with the company.

Our consultants participate in a rigorous continuing education program to stay ahead of emerging threats and regulatory compliance requirements. In addition, they are required to maintain prestigious professional certifications and licenses, such as:

- Certified Information Systems Auditor – CISA
 - Certified Information Systems Security Professional - CISSP
 - Certified Internal Auditor – CIA
 - Certified Information Security Manager - CISM
 - Certified Ethical Hacker - CEH
 - GIAC Certified Incident Handler - GCIH
 - Certified Business Continuity Professional – CBCP
-
- 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?

UDT Response:

Depending on the type of service provided licensing fees may be included in monthly subscription. If the license is a one-time charge or requires annual renewal fees this will be identified during the design and quoting process.

- 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?

UDT Response:

Each party owns its own confidential data and IP.

Each party shall return or destroy the other party’s Confidential Information on completion of the Services, or earlier on request of the other party, provided that a party may retain the other party’s Confidential Information in backup medium where return or deletion is not commercially reasonable, or otherwise as required by law. On request of a party, an officer of the other party shall certify its compliance with the preceding sentence.

In addition, for services include the hosting, maintaining or otherwise managing of any Client Data where Client does not otherwise have the ability to download a copy of such Client Data, UDT shall provide Client with a copy of such Client Data within thirty (30) days after the effective date of termination in a standard, electronic format to be mutually agreed upon by the parties.

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

UDT Response:

UDT believes in a high touch sales model and will provide the NCPA members a dedicated team to include an Account Manager, Inside Sales Support Representative, Sales Operations Administrator, and Customer Service Representative

UDT’s dedicated account manager must handle questions and resolve problems that may arise. At least one Customer Service Representative will be available during UDT’s operating hours. UDT will offer a “wait in queue” or voicemail option with a callback. All service representatives will have on-line access to information to provide an immediate response to inquiries concerning the status of orders (shipped or pending), delivery information, back-order information, district-wide contract pricing, contracted product offerings/exclusions, contract compliance requirements, and general product information. Representatives will be available by phone (local or toll-free number preferred) or email.

Hours of Operation: UDT’s hours of operation are 7:00 AM to 5:00 PM EST.

UDT Locations:

HEADQUARTERS	2900 Monarch Lakes Blvd. Suite 300 Miramar, FL, 33027 P: <u>(954) 308-5100</u>	TEXAS	100 Congress Avenue Suite 2000 Austin, TX 78701 P: <u>(512) 466-3405</u>
MIAMI LAKES	14042 N.W. 82nd Ave. Miami, FL 33016 P: <u>(786) 364-6097</u>	ORLANDO CUSTOMER SUPPORT CENTER	9436 Southridge Park Ct. Suite 800 Orlando, FL 32819 P: <u>(800) 882-9919</u>
TALLAHASSEE	1621 Metropolitan Blvd. Suite 102 Tallahassee, FL 32308 P: <u>(850) 329-6215</u>	ORLANDO CUSTOMER INTEGRATION CENTER	2612 Consulate Drive, Suite 100 Orlando, FL 32819 P: <u>(800) 882-9919</u>
TAMPA	5426 Bay Center Dr. Suite 725 Tampa, FL 33609 P: <u>(800) 882-9919</u>	OKLAHOMA	13900 N. Portland Ave. Suite 170 Oklahoma City, OK 73134 P: <u>(405) 567-4080</u>
TENNESSEE	209 10TH Ave. South Suite 530 Nashville, TN 37203 P: <u>(615) 567-4080</u>		

- 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.

UDT Response:

Where applicable, and to continue to drive the UDT Green IT initiative, desktops and workstations will be delivered by UDT resources unboxed to end user location.

As an example, laptops will be delivered within laptop carts where possible.

- This allows for less cardboard to end up at end user location.
- UDT can responsibly recycle this cardboard at its Configuration Center location as opposed to this cardboard being disposed of within site dumpster
- While this option may not always be feasible within the customer environment, UDT utilizes this model as a standard practice within its Configuration Center location to recycle over 5 tons of cardboard monthly

In addition, UDT offers enhanced support program that increases hardware lifespan, reducing environmental impacts from replacing products that still have useful life. With this uplifted service we will recycle parts from customer devices that meet the beyond economic repair criteria to repair their own product.

- Vendor Certifications (if applicable)

- Provide a copy of all current licenses, registrations and certifications issued by federal, state, and local agencies, and any other licenses, registrations, or certifications from any other governmental entity with jurisdiction, allowing respondent to perform the covered services including, but not limited to, licenses, registrations, or certifications. Certifications can include M/WBE, HUB, and manufacturer certifications for sales and service.

UDT Response:

UDT partners with top tier leaders in the industry to provide the latest products, from personal computing to customized, complex solutions. In addition to holding many manufacturer certifications, UDT participates in the following Advisory Councils:

Intel Solution Provider Advisory Council
HP Public Sector Advisory Council
HP CEO Roundtable Council
Cisco Advisory Council
Microsoft Cloud Solution Provider Council

By participating in these advisory councils, UDT remains on the forefront of technology and has the ability to impact roadmaps and changes in product solutions if needed. UDT is a Cisco Gold Partner and has over 20+ Cisco Certified Engineers. UDT's has an array of certified engineers as it relates to the more complex technologies such as Virtualization, Security, and VOIP to name a few. In addition, UDT has in house repair warranty authorized technicians for HP, Dell and Lenovo.

UDT Certifications & Classifications

PCI-QSA Firm

SOC 1 & SOC 2 Certified

SSAE-16 & 18 certified platforms

NAICS – 541513

Socio Economic – Minority Owned Enterprise (Hispanic Owned) – NMSDC Certificate shown below.



State of Florida

Department of State

I certify from the records of this office that UNITED DATA TECHNOLOGIES, INC. is a corporation organized under the laws of the State of Florida, filed on March 23, 1995.

The document number of this corporation is P95000023595.

I further certify that said corporation has paid all fees due this office through December 31, 2020, that its most recent annual report/uniform business report was filed on January 6, 2020, and that its status is active.

I further certify that said corporation has not filed Articles of Dissolution.

*Given under my hand and the
Great Seal of the State of Florida
at Tallahassee, the Capital, this
the Fifth day of January, 2021*



Ronald R. DeSantis
Secretary of State

Tracking Number: 5830216187CU

To authenticate this certificate, visit the following site, enter this number, and then follow the instructions displayed.

<https://services.sunbiz.org/Filing/CertificateOfStatus/CertificateAuthentication>

Request for Taxpayer Identification Number and Certification

Give Form to the requester. Do not send to the IRS.

* Go to www.irs.gov/FormW9 for instructions and the latest information.

1 Name (do not check on your insurance coverage). Name is required on U.S. form, do not leave it to the blank.

2 Business name/disregarded entity name, if different from above

UDT: UDT Financial Services

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only one of the following seven boxes.

Individual/sole proprietor or single-member LLC

Corporation

S Corporation

Partnership

Trust/estate

Limited liability company. Enter the tax classification (C-Corporation, S-B corporation, P-Partnership) ▶

Other (see instructions) ▶

4 Address (number, street, and apt. or suite no.) See instructions.

2900 Monarch Lakes Blvd. #300

5 City, state, and ZIP code

Miramar, FL 33027

6 List account number(s) here (optional)

7 Exemptions (codes apply only to certain entities, not individuals, see instructions on page 3):

Exempt payee code (if any) _____

Exemption from FATCA reporting code (if any) _____

8 Requester's name and address (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. This TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Notes: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number									
OR									
Employer identification number									
6	5	-	0	5	8	6	1	3	8

Part II Certification

Under penalties of perjury, I certify that:

- The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
- I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
- I am a U.S. citizen or other U.S. person (defined below); and
- The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here Signature of U.S. person ▶ *[Signature]* Date ▶ *1/20/2021*

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to www.irs.gov/FormW9.

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following:

- Form 1099-INT (Interest earned or paid)
- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1096 (home mortgage interest), 1099-E (student loan interest), 1096-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See *What is backup withholding*, later.

Request for Taxpayer Identification Number and Certification

Give Form to the
 requester. Do not
 send to the IRS.

* Go to www.irs.gov/FormW9 for instructions and the latest information.

1 Name (do not check on joint return or joint return). Name is required on U.S. form, do not leave blank.

2 Business name/disregarded entity name, if different from above

UDT: UDT Financial Services

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only one of the following seven boxes.

Individual/sole proprietor or single-member LLC

Corporation

S Corporation

Partnership

Trust/estate

Limited liability company. Enter the tax classification (C-Corporation, S-B corporation, P-Partnership) ▶

Other (see instructions) ▶

4 Address (number, street, and apt. or suite no.) See instructions.

2900 Monarch Lakes Blvd. #300

5 City, state, and ZIP code

Miramar, FL 33027

6 List account number(s) here (optional)

7 Exemptions (codes apply only to certain entities, not individuals, see instructions on page 3):

Exempt payee code (if any) _____

Exemption from FATCA reporting code (if any) _____

8 Requester's name and address (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. This TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Notes: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number									
OR									
Employer identification number									
6	5	-	0	5	8	6	1	3	8

Part II Certification

Under penalties of perjury, I certify that:

- The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
- I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
- I am a U.S. citizen or other U.S. person (defined below); and
- The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must check out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here Signature of U.S. person ▶ *[Signature]* Date ▶ *1/20/2021*

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to www.irs.gov/FormW9.

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following:

- * Form 1099-INT (interest earned or paid)
- * Form 1099-DIV (dividends, including those from stocks or mutual funds)
- * Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- * Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- * Form 1099-S (proceeds from real estate transactions)
- * Form 1099-K (merchant card and third party network transactions)
- * Form 1096 (home mortgage interest), 1098-E (student loan interest), 1096-T (tuition)
- * Form 1099-C (canceled debt)
- * Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See *What is backup withholding*, later.

Tab 5 – Products and Services

- ◆ Respondent shall perform and provide these products and/or services under the terms of this agreement. The supplier shall assist the end user with making a determination of their individual needs.
- ◆ Offeror's must be able to provide services the following pillars as adopted by the National Institute of Security Technology (NIST).
<https://www.nist.gov/cyberframework>. Vendors who offer these services either individually or in a combination are qualified to respond to this solicitation.
- ◆ The following is a list of suggested (but not limited to) Cyber-Security Solutions, Malware, Ransomware Protection, Other Related Products and Services requirements. The successful respondent(s) will provide products and services that include, but are not limited to the following:
- ◆ **Identify** - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
 - Asset Management
 - Asset Discovery
 - Business Environment
 - Governance
 - Risk Management
 - Risk Management Strategy
 - Vulnerability Scanning and Management
 - Supply Chain Risk Management
- ◆ **Protect** - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
 - Identity Management
 - Authentication and Access Control
 - Multi-factor Authentication (MFA)
 - Awareness & Training
 - Data Security
 - Information Protection + Procedures
 - Maintenance
 - Protective Technology
- ◆ **Detect** - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
 - Anomalies & Events

- Security Continuous Monitoring
- Detection Process
- Log and Event Correlation (SIEM)
- User Behavioral Analytics (SIEM)
- ◆ **Respond** - Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
 - Response Planning
 - Data Enrichment
 - Communication
 - Analysis
 - Mitigation
 - Automated Response
 - Improvements
- **Recover** - Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
 - Recover Planning
 - Forensic Investigation
 - Findings Report
 - Improvements
 - Communications

IT Cybersecurity Products have 5 key capabilities:

1. Asset Management
2. Identity and Access Management
3. Network Security Management
4. Data Protection Management
5. Future Capabilities.

IT Cybersecurity Services includes a wide range of fields such as, risk management framework services, information assurance, virus detection, network management, situational awareness and incident response, secure web hosting, and backup, security services and, Security Operations Center (SOC) services.

Product Categories Suggested (but not limited to) for this RFP

- ◆ **Hardware & On-Prem Software**
 - Cloud Security
 - Hard Disk Drives

- Input Device Accessories
- Network Accessories
- Network Adapters & Cables
- Network Devices
- UTM (Firewall)
- Web App Firewall
- Anti-virus
- Anti-spam
- URL Filtering (CIPA Compliance)
- ISD/IPS Systems
- Email Gateways
- Network Storage
- Power Accessories, Adapters, and Supplies
- Rack System and Accessories
- RAM Mods
- Repeaters/Transceivers
- Security Hardware and Software
- SSD (Solid State Drives)
- Storage Controllers
- .. **Cloud Services**
 - Cloud Security
 - Cloud-based SIEM Services
 - Cloud-based Endpoint Protection (EPP/MDR)
 - Internet/Commination Apps
 - Web Application Firewall (WAF)
 - Security Service and Support
 - Cloud-based Vulnerability Scanner
 - Security Software
- .. **Other Services**
 - Security Audits
 - Data acquisition (1-off)
 - Per audit services
 - Risk Assessment audit - Internal exposure
 - Gap Assessments or Readiness Assessments against Security Framework
 - Professional Services
 - Installation services (list approved/qualified partners)
 - Migration Services (list approved/qualified partners)
 - Open-Source Integration (list approved/qualified partners)
 - Managed Services
 - Content Filtering Management
 - Data Aggregation Report Management
 - Managed Detect and Response Service (MDR)

- Vulnerability Management as a Service
- Security Information and Event Management (SIEM) as a Service
- Identity and Access Management (IAM) as a Service
- Training Services
 - Professional Training and Development (IT Staff)
 - IT Product Training (list approved/qualified partners)

UDT Response:

Cybersecurity Capabilities

United Data Technologies' UDTSecure™ Cybersecurity Services and Solutions is made up of advanced, yet flexible set of Managed Security Services that are complemented by a broad selection of comprehensive professional assessment and compliance focused services designed to align with Client business objectives.

For more than twenty years, UDT have been a technology enabling company and a leader in the information security industry. Our firm is privately owned, independent of affiliate firms, technology vendors and service providers.

Our managed security services provide each Client the ability to detect, respond and recover quickly from a security event. Keeping up with the latest security platforms and retaining the right in-house skill sets to support them, is both challenging and capital intensive. Supported and delivered from a fully manned, 24x7 Security Operations Center (SOC), UDTSecure's Managed Security Services allows Clients to quickly integrate its infrastructure of firewalls, servers and applications to an advanced threat intelligence platform that monitors for the latest set of cyber-attacks. A team of certified cybersecurity engineers can quickly spot security events that matter from those which do not. This helps reduce costs and increases efficiencies by eliminating most of the false positives that clients must respond to.

UDTSecure's Cybersecurity Professional Assessment Services includes a wide range of comprehensive information security assessments, IT audits and compliance evaluations Clients can choose from no matter their size or industry vertical. From technical security evaluations, incident response investigations to more comprehensive risk and compliance-based assessments, our team of fully certified cybersecurity consultants have the required background to uncover important risks that impact remediation, maintains compliance, and prioritizes investment strategies.

Based on industry security frameworks that include NIST, ISO, CoBIT, FFIEC and others, our proprietary UDTSecure Risk and Vulnerability Assessment methodology identifies a Client's true risk exposure value and impact to mission critical systems, and assets.

UDT is a certified PCI-QSA firm with three in-house Senior PCI QSA assessors with the experience to help organizations become and maintain their PCI attestation requirements. Our PCI-QSA consultants conduct PCI based gap analysis audits which provide actionable remediation strategies to achieve compliance at any level.

Detect:

At the core, UDT SOC Services have been designed to meet the challenges of the Detection requirements listed in the NIST cyber security framework. These requirements consist of a combination of Continuous Security Monitoring (SOC), Log and Event Correlation (SIEM), and Log Retention while performing the following as part of the MSS for Standard Service Level:

Security Operations Center (SOC)

The UDT SOC team is responsible for 24x7 security monitoring of end-client environment. The team is situated at a UDT location in an area that is closely monitored using CCTV cameras, and that only allows access to authorized personnel.

A UDT SOC security analyst first responds to any perceived or real threat to an end-client's managed security environment. Security threats may be to end-client servers, firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus, network devices, web applications, and other security assets.

Security Monitoring, Incident Management, and Events of Interest

For security monitoring, UDT SOC performs 24x7 monitoring of logs and audit trails to locate security events to detect known and unknown attacks.

For incident management, UDT SOC enables restoration of services as soon as possible by communicating actionable guidelines and remediation actions to the end-client. It manages the support and delivery interface to the end-client that includes call management, communication, and support. UDT SOC does not fix the underlying problem (i.e., root cause) of the incident, as it is out-of-scope. It is the responsibility of the end-client's problem and change management teams to identify and fix the root cause of the incident.

The incident management process is triggered through one or more of the following, when:

1. End-client contacts the Single Point of Contact (SPOC) in UDT SOC to report service disruption, or
2. An auto detected SIEM event creates an incident in the incident management tracking tool, or
3. An internal support group at end-client identifies a service disruption (or potential disruption) to the devices under security management by UDT SOC and subsequently creates an incident

UDT uses ITIL best practices and tools to manage the environment to agree upon service levels. It proactively and continuously monitors all the KPIs. It ensures that control points

with threshold levels are defined properly and attempts to identify possible service interruptions before they occur.

Log Management

A log, in a computing context, is the automatically produced and time-stamped documentation of events, relevant to a particular system. Virtually all software applications and systems produce log files. Log management is the collection of processes and policies used to administer and facilitate the generation, transmission, analysis, storage, archival, and ultimate disposal of the large volumes of log data created within an information system.

The UDT SOC team performs the following activities as part of log management:

- Monitor log health
- Perform manual analysis and correlation of logs in context of end-client specific environment, on a commercially reasonable effort basis
- Retain logs for one year
- Provide on-demand access to all log data
- Generate periodic log monitoring reports

UDTSecure SIEM Tool Integration & Administration

UDT SOC performs the following activities as part of UDTSecure SIEM tool integration and management:

- Setup and install UDTSecure SIEM solution
- Configure various UDTSecure SIEM modules
- Customize UDTSecure SIEM as per end-client's compliance requirements
- Conduct project definition exercise (PDE)
- Configure hybrid deployment support for centralized collection of security logs from on-premises as well as cloud-based setups
- Tune and configure UDTSecure SIEM collector, processor, and console modules
- Perform controlled integration of identified devices and OS – e.g., Windows Exchange, Windows IIS, Windows Domain Controller, UNIX, LINUX, Cisco switches & routers, Palo Alto switches & routers, etc.,
- Integrate to UDTSecure SIEM's X-Force threat intelligence, track malicious IPs, and assign a risk to web domains (e.g., if a user communicates with a potentially malicious IP or visits a risky web domain, the user's risk score is automatically increased)
- Enable custom reporting capabilities for end-client support groups
- Create executable dashboards for end-client support groups
- Create post implementation document (PID)
- Integrate to external ticketing system
- Integrate existing baseline security system with UDTSecure SIEM, if integration is available
- Backup and restore UDTSecure SIEM appliances

Security Investigations on UDTSecure SIEM

UDT SOC investigations quickly focus analysis on who initiated the threat, how they did it and what was compromised. Our scripts are first applied on top of the data that is normalized and parsed from UDTSecure SIEM appliance. Indexes and summaries are then created on every field that is mapped to the multi-dimensional cross correlation engine in UDTSecure SIEM. UDT SOC team can retrace the step-by-step actions of cyber criminals and analyze the logs and flows of data that is related to a security incident.

When an organization first becomes aware of a threat or a potential security risk or compliance breach, it is important to set objectives to assess the scope, identify the entities involved, and understand the motivations. Log and incident forensics is used in specific scenarios of different investigations. UDTSecure SIEM's log activity module will be used to perform log and incident forensic searches. (Note: cyber forensics is out-of-scope)

The activities that UDT SOC performs as a part of security investigations are:

- Recover logs and flow data
- Query categories of attributes to gather evidence from the security incidents created
- Update security incidents with all the collected forensics logs and flows
- Retrieve further information of interest using search filters

Consultant Qualifications

UDT Cybersecurity Consultants average no less than ten (10) years' experience conducting information security-based assessments and technical evaluations. Each have obtained advanced University Degrees in the areas of Computer Sciences, Industrial and System Engineering disciplines. All consultants are recruited through a rigorous selection process that includes a comprehensive background check for criminal records, verification of past employment, credit history, and are undergo drug tested prior to onboarding with the company.

Our consultants participate in a rigorous continuing education program to stay ahead of emerging threats and regulatory compliance requirements. In addition, they are required to maintain prestigious professional certifications and licenses, such as:

- Certified Information Systems Auditor – CISA
- Certified Information Systems Security Professional - CISSP
- Certified Internal Auditor – CIA
- Certified Information Security Manager - CISM
- Certified Ethical Hacker - CEH
- GIAC Certified Incident Handler - GCIH

- Certified Business Continuity Professional – CBCP

Certifications & Classifications

- PCI-QSA Firm
- SOC 1 & SOC 2 Certified
- SSAE-16 & 18 certified platforms
- DUNS Number – 933640682
- NAICS – 541513
- Socio Economic – Small Business

UDTSecure Risk Management and Consulting Services

Our comprehensive set of professional consulting services include the following:

Assessments and Audits	Technical Evaluations
<ul style="list-style-type: none"> • IT and Information Security Audits • Compliance Based Evaluations (GLBA, PCI, HIPAA, FFIEC, SSAE-18) • Privacy Assessments (NYDFS, GDPR, CCPA) • Incident Response Services • Cybersecurity Liability Policy Evaluations • Information Security Program Development • Remediation Implementation Services • 3rd Party Vendor Program Evaluations • CISO as a Service 	<ul style="list-style-type: none"> • Network Vulnerability Scans • Web Application Penetration testing • Network Penetration testing • WiFi Network Penetration testing • Azure Penetration testing • IT Security & Vulnerability Assessments • Social Engineering Evaluations • Digital Forensic Analysis and Subject Matter Expert Services • Red and Blue Team Evaluations • Threat Hunting as a Service • AD Risk and Threat Modelling • M365 Risk and Threat Modelling

Advanced Cybersecurity Professional Services

Finding and employing skilled and experienced cybersecurity personnel are hard to find and even harder to retain. UDT’s advanced cybersecurity professional services allow customers a channel to outsource or retain services from our team of subject matter experts. These services include the following:

- Chief Information Security Officer as a Service (CISO)
- Incident Response Services on Demand or on Retainer

RESPOND AND RECOVER

Incident Response Evaluation

- Evaluates the effectiveness of an organization's information security program by identifying gaps to industry frameworks and best practices.
Reviews key components of the plan (i.e. BCP and DR plans, Team Member identification, Communication and Notification Plans, Insurance coverage and claims procedures
Provides recommendations based on findings that enhance and fortify the plan to meet business objectives and aligned to recovery time objectives.
- **Incident Response Tabletop Exercises**
Performs incident response tabletop exercises that test real world-based scenarios within a controlled and scripted environment.
Primary objective is to identify weaknesses or gaps within existing incident response plan and provide actionable mitigation recommendations to enhance the plan and present for board approval

UDTSecure Managed Security Services

Consisting of Monitoring Only or Monitoring and Management, our managed security services allow Clients to select the service solutions that best aligns to business objectives and needs.

Security Monitoring – In this deployment, UDTSecure's threat intelligence and correlation platform receive security logs from devices. SOC analysts alert and advise client on recommended changes based on service level agreements. Access to compliance reports and daily security activities, are easily accessible through a secure Client portal.

Security Monitoring and Management – Includes monitoring services of devices and additionally leverages UDTSecure Analysts and Engineers to make changes to Client's environment based on change requests, events collected and security intelligence.

Supported Systems Our threat intelligence platform is vendor agnostic allowing for quick integration of broad array of devices, systems and applications operating in physical or virtual infrastructures which include the following: include the following:

- Firewall (Next Generation and High Availability)
- Routers & Switches

- Load Balancers
- Application Firewalls
- IDS/IPS
- Virtual Private Network
- Application Servers
- Management Servers
- End Point Security Solutions
- On Premises, Cloud or Hybrid solutions
- eMail Security
- Mobile Device Security
- Web Content Filtering

Key Components and Features – Managed Security Services are delivered via UDT’s Threat Intelligence Platform hosted in a security certified and manned Security Operations Center (SOC). The service includes a portfolio of features designed to quickly detect and protect mission critical systems against a variety of known and unknown attacks. Customers benefit from lowering operational costs and efficiently and minimizing an organization’s operational costs.

- Log Collection, retention, and management
- Behavioural and Signature based detection analysis
- Online and Offline Log Search Capabilities to meet compliance and forensic requirements
- Threat analysis, correlation, and detection of system logs to identify attacks
- Endpoint Security Solutions (Anti-Virus, DLP, NAC, File Integrity Management, Web Content Filtering, eMail Security and Cloud hosted applications)
- Security Incident escalation and notification based on severity levels
- User Security Portal & Dashboard Access
- Executive and Management reports
- Compliance based activity reports
- Quarterly Business Reviews
- Behavioural and Signature based attack detection capabilities
- Policy and Rules based Change Requests
- Vulnerability Management

Cyber Risk Management Platform offering:

Conquest (Scyops) platform contains 7 modules:

Shield

- Vulnerability management, patch management, asset inventory, and other technology hygiene functions

Inspect

- Establish mature cyber risk management programs, enabling the rapid development of cyber operational maturity, compliance drift control monitoring, comprehensive reporting

SOC

- Direct access to reporting, playbooks, communication plans, and categorized escalation to align asset criticality and service levels

Simulate

- Compare new technologies and service solutions against your organization's maturity requirements

Defend

- A base solution for cybersecurity strategy that uses a cyber program baseline and adapts to any change in operational maturity or growth, scaling to organizations of any size.

Evaluate

- Our risk management module lets you categorize your assets by their level of criticality and evaluate how available technologies and service solutions address threat scenarios specific to your organization

Overwatch

- Provides risk evaluation and continuous monitoring, enabling comprehensive risk management across the entire attack surface of multi-tiered organizations.

Examples of Cyber Securities Services provided to Clients

IT Security Assessment and PCI Readiness Assessment

UDT completed an IT security assessment for a Florida county government. The purpose of the engagement was to evaluate IT security across key components of the technology environment. Our procedures included external and internal network vulnerability assessments and penetration tests; firewall and network device configuration analyses; application security assessments; social engineering; reviews of the Information Security Program, IT governance policies and technology asset management procedures; data center (physical) security reviews; and a PCI readiness assessment.

We reassessed remediated items six months after completing our initial testing. Our deliverables included a comprehensive management report and an executive-level presentation of our findings and recommendations.

WebApp Pentest as a Service

UDT provides pen-testing as a service to test multiple Client applications in accordance with industry best practices and security testing frameworks including but not limited to OWASP and internal methodologies developed over time. Testing is performed using authenticated and unauthenticated procedures to thoroughly identify vulnerabilities that could potentially be exploited.

Incident Response and Forensic Analysis

Primary contractor conducting ransomware attack investigation alongside Federal Bureau of Investigation (FBI) for large public entity. Client's infrastructure consisted of more than 40,000 hosts. UDTSecure Incident Response Team identified source of attack, successfully reengineered the malware and assisted the Client in successfully restoring their environment. UDT led additional investigations to determine whether data breach had occurred.

IT Security Assessments

UDT performed an IT security assessment for a Commercial client and its subsidiaries. The engagement included assessments of external and internal network security; internal security applications and services; server, firewall and DMZ configuration reviews; denial-of-service and incident response procedures; document management procedures; change management policies; organizational structure and select IT processes.

Managed Security Services

UDT currently provides Security Monitoring services for the Client's infrastructure. Services are delivered via UDT's Threat Intelligence and Unified Security Management platform. Devices and Components currently being monitored include Firewalls, Routers, Switches, Servers, and End Point Security Solutions. Our platform is currently processing 800,000,000 Events Per Day generated from the Client's infrastructure which filters out false positives using our correlation and detection policy capabilities.

IT Risk and Security Assessment & Managed Security Services

UDT performed a risk-based vulnerability assessment, penetration test and technical information security assessment for International currency Client which included subsidiaries in Europe and Latin America. The scope of our engagement included conducting a risk-based assessment which covered PCI and GDPR standards and security controls, development of information security program, evaluation of external and internal network security, firewall configurations, enterprise, and web-based application security, third party vendor assessment and user security awareness. We combined manual audit procedures with vulnerability assessment techniques to identify and analyze security risks within the agency's IT environment.

IT Audit - UDT currently provides Security Monitoring services of client's Network components and Mission Critical Systems and Applications

UDT performed an audit of the bank's IT environment. Our objective was to ensure that IT infrastructure was secure, that network hardware was configured appropriately, and that IT general controls were operating effectively. Our review included analyses of key IT processes, internal wireless network security, the configuration of the Internet-facing firewall, and compliance with FFIEC, NIST and PCI Data Security Standards. Additionally, subsequent engagements included the performance of a cloud-based security risk assessment and general IT security controls review on mobile banking application.

IT Risk and Security Assessment

UDT performed a comprehensive risk-based vulnerability assessment, penetration test and technical information security assessment on MDCPS' infrastructure. The scope of our engagement included conducting a risk-based assessment which covered NIST, FERPA and ISO 27001 standards and security controls, development of information security program, evaluation of external and internal network security, firewall configurations, enterprise, and web-based application security, third party vendor assessment and user security awareness. UDT assessors combined manual audit procedures with vulnerability assessment techniques to identify and analyze security risks within the organization's IT environment.

Cyber Risk Consulting Services (CISOaaS)

Lead development and implementation of company strategy for Information Security, Cybersecurity, and Data Privacy Protection, including risk-based control objectives and technical architecture framework.

- Establish strategic alignment with IT and Corporate leadership for security and privacy strategy and plans, and secure necessary resources to enable execution.
- Define and communicate global security policies, standards, guidelines, and procedures to ensure ongoing compliance with security requirements.
- Provide ongoing guidance and expertise in regulatory and industry developments related to Security, Cybersecurity, and Data Privacy Protection to senior leadership.
- Represent Company to customers, regulators, and other external parties for all types of information security matters.
- Support the organization to continuously improve expertise in security design and planning of enterprise-wide networks, technology infrastructure, middle ware, platforms and applications through effective leadership, staff development, and strategic recruitment.
- Lead monitoring, enforcement, and continuous improvement of internal security controls, policies, and standards through internal audit, customer audit, and third-party certifications.
- Spearhead a compliance program to achieve legal obligations and business goals by prioritizing initiatives and assessing the evaluation, deployment, and management of current and future technologies.
- Audit existing compliance practices across the organization; isolate potential risks or liabilities and develop mitigation plans.
- Participate as a member of the IT senior management team in processes of the organization's strategies for legal compliance.

HIPAA Risk Assessment

UDTSecure Security Assessors performed a HIPAA Risk Assessment for the listed Clients consisting of the following activities:

A gap analysis comparing the standards and implementation specifications of the HIPAA Security Rule identified in Subpart C of Part 164 of Title 45 of the Code of Federal Regulations to current policies, procedures, and practices of any technical and non-technical systems used to create, maintain, receive, or transmit Protected Health Information. The gap analysis deviations from HIPAA regulatory requirements and each deviation assessed for severity and impact.

A vulnerability assessment of the Client's internal systems and endpoints used to create, receive, store, or transmit Protected Health Information for or on behalf of the Clients.

A report for Client's contracting organizations that summarizes the HIPAA security gap analysis

Report on Findings delivered to Client summarizing the results of the risk assessment, identifying high, medium, and low risks for Client's systems. The report provided detailed recommendations for control or technological improvements which Client implemented to meet HIPAA-HITECH standards.

PCI GAP ANALYSIS / UDTSecure Risk & Vulnerability Assessment / MFA Solution Selection

UDT performed a Gap Analysis for the client focused in identifying gaps in existing procedures, policies, and security controls against PCI-DSS requirements. Prioritized remediation recommendations to include recommendations for compensating controls required to meet PCI-DSS annual requirements.

UDTSecure Security Assessors performed a comprehensive risk-based vulnerability assessment, penetration test and technical information security assessment on Client's infrastructure.

The scope of our engagement included conducting a risk-based assessment which covered NIST, FERPA and ISO 27001 standards and security controls, evaluation of external and internal network security, firewall configurations, enterprise and web-based application security, third party vendor assessment and user security awareness. UDTSecure Security Assessors combined manual audit procedures with vulnerability assessment techniques to identify and analyze security risks within the organization's IT environment.

Led project to assist Rooms to Go in the selection of a Multi-Factor Authentication solution. Activities included Project Management, Analysis oversight and evaluations, Recommendation and Solution Selection, and implementation management of Proof of Concept.

Tab 8 – Value Added Products and Services

Include any additional products and/or services available that vendor currently performs in their normal course of business that is not included in the scope of the solicitation that you think will enhance and add value to this contract for Region 14 ESC and all NCPA participating entities.

UDT Response:

UDT has included additional products and services offerings in Tab 7.

Known by our clients as a trusted partner, we provide flexible and interoperable solutions. Along the way, we offer a complete spectrum of technical, professional, and managed services to a broad range of industries. Whether your enterprise is private or public, medium or massive, we will move you forward with solutions that work within your timelines, budget, and unique technology framework. *We will maximize the impact of your mission.*

UDT's portfolio of services include:

Managed Services

Cooperative IT • Remote Monitor and Manage • Help Desk • Onsite Support • Advisory (Virtual CIO)

Managed Security

Managed Firewall • Managed IPS/IDS • End Point Security • Managed SIEM • Incident Response

Managed Cloud

Back Up • Desktop as a Service • Office 365 • Unified Communications

Advanced

Advisory and Consulting • Deployment • Implementation • Integration • Staff Augmentation • Project Management

Technical

Etching • Asset Tagging • Warranty • Field Repair • Asset Tracking
UDT's portfolio of solutions include:

Collaboration

Collaborative Workspaces • Audio / Visual Communications • Conferencing

Data Center

Management and Automation • Customized Network Solutions • Network Performance Optimization

Cloud

Readiness Assessment • Public, Private, Hybrid • Microsoft Azure and 365 • Backup and Restore

Cybersecurity

Threat Management Services • Technical Security Assessment • Compliance

Mobility

Assessment and Design • Outdoor Mobility • Device Management • Internet of Things

Education

Hands-On Learning Solutions • STEAM and Makerspaces • Digital Learning Convergence

If awarded the opportunity to be listed as one of the suppliers for this bid, we will be able to offer the members of NCPA a comprehensive portfolio of other IT industry leaders. In addition, UDT offers a Balance of Line category to provide NCPA members the ability to buy other devices and services outside of the current products listed in the catalogs represented currently as new product introductions are made or required.

Along with UDT's valuable partnerships with the industry's top OEM's, UDT has partnered with most of the major distributors in the US. Through these partnerships, the NCPA members can tap into a vast array of brand name products available to them in several warehouses strategically located throughout the country. Every business day, UDT collects the pricing and availability information from each one of our distribution partners resulting in an online catalog with over 100,000 items and the ability to process orders of available products for next day shipping.

UDT only works with authorized manufacturer distributors.

UDT's Primary Distribution Partners are:

- Ingram Micro
- Tech Data
- Synnex
- D&H Distributing

Distributor line cards include the following:

THIS SPACE INTENTIONALLY LEFT BLANK
LINE CARD NEXT PAGE

LINE CARD					
ADVMICRO	Acer	VIDEO GAMES PLUS.COM	ENCORE SOFTWARE LLC	MONOPRICE, INC.	SHAREGATE GROUP INC.
ALLROUND AUTOMATION	Allied Telesis	1754012 ONTARIO INC. DBA	ENVISION PERIPHERALS INC.	MONOPRICE, INC.	SHARP ELECTRONICS OF
ALTOVA	Altaro	MYGICA	ENVISION PERIPHERALS INC.	MONSTER TECHNOLOGY	SHARP-TRADE
ANIXTER	Amazon	203 TRADING LLC	ENVISION PERIPHERALS, INC.	INTERNATIONAL LTD.	SHENZHEN RAPOO
AOC	Amazon Digital Services	3M	ENVOY DATA CORP	MOORECO, INC	TECHNOLOGY CO. LTD.
APRICORN	American Industrial Systems	3M TOUCH SYSTEMS	EPOS CANADA LIMITED	MOTIV INC.	SHURE INCORPORATED
ATTO TECH	Inc	A-Data	Epson	Motorola	SHUTTLE COMPUTER GROUP
AVAGO	Apple	A2C SERVICES LIMITED	ERGOREST	MOUSETRAPPER NORDIC AB	INC
COHESITY	Autodesk	ACECAD DIGITAL DBA	Ergotech	MSI	SIGNAGELIVE, INC.
COMMVault	Avaya	SOLIDTEK	ERGOVERSE	MTM INC.	SIGNIFY CANADA LTD.
CONDUSIV	AvePoint	AddOn Networks	Ericom	MULTI-TECH SYSTEMS, INC.	SILICONDUST USA, INC.
DISTINOW	Avocor	Adesso	ERWIN INC.	MURATEC STRATEGIC	SIMPALTEK LLC
EDITHMIN INTL	Axiom	ADVANCED SKYLINE	Esker	NANONATION, INC	SIMPLIFIED IT PRODUCTS LLC
EGANTEAMBOARD	BitTitan	TECHNOLOGY LTD.	EVE SYSTEMS LLC	NANOV DISPLAY, INC	SINGLEWIRE SOFTWARE,LLC
EIZO	Bretford	AEVOE CORP	EVGA	NAVORI INC.	SIOS TECHNOLOGY CORP
EMC	Brother	AfterShokz	Evoluent Llc	NCIPHER SECURITY LLC	SKYWORTH USA CORP.
EXCLAIMER	Canon	AG Neovo	Extensis	Nest	SMARTEYES DIRECT INC.
EXITCERTIFIED	Carbonite, Inc	AIDATA	FACEBOOK TECHNOLOGIES LLC.	NETMOTION SOFTWARE, INC	(GALAXY)
F-SECURE	CCX	ALC MICRO	FEIT ELECTRIC COMPANY	NEW AGE ELECTRONICS,INC.	SMARTLABS, INC.
FILEMAKER	Check Point	Alien Vault	Fellowes	NEW ENGLAND TECHNOLOGY,	SMK ELECTRONICS
FORTINET	Cisco Systems	ALTHON INC.	Finisar	INC	CORPORATION, U.S.A.
FREEDOM MOBILE	CyberPower Systems	ALTIS GLOBAL LIMITED	FireEye	NEWLINK.CA INC	SOL REPUBLIC
HECKTECH	D-Link Systems	Aluratek	Firemon	NEXENTA BY DDN, INC	SOLARFLARE
HITACHI	Dell	Amaryllo	FIVE9 INC.	NITRO PDF, INC	COMMUNICATIONS INC.
HITACHIGLB	Digi International	AMBIR TECHNOLOGY, INC.	FixMeStick	NOBLE SECURITY	SOLE SOURCE TECHNOLOGY LLC
IBM	Eaton	AMD	ForeScout Technologies	NOKIA CANADA INC.	SOLO, A DIVISION OF UNITED
ILLUMINARI	Engenius Technologies	Amer Com	Foxit Software Company LLC	NORRIS TECHNOLOGIES, LLC	STATES LUGGAGE CO., LLC
IMPINJ LOGISTICS	Ergotron	AMERICAN WELL CORPORATION	Fujifilm	NORTONLIFELOCK INC. - ESD	INC.
JAMF	Extreme Networks	CORPORATION	G-STYLE LTD.	NORTONLIFELOCK INC. CAD	SONOS INC.
JOLERA					
KAMINARIO	F5 Networks	ANDA SEAT TECHNOLOGY INC.	GAMA WORLD TECHNOLOGIES, INC	NUANCE COMMUNICATIONS NURA OPERATIONS PTY LTD.	SONUS
KHLANDSBG	Fujitsu Google	Andrea Electronics	Gamber Johnson	NUJUO US INC	SOPHOS, INC.
KODAK	Hewlett Packard Enterprise	Antec	Garner Products	NYCOMP INC	SOUL ELECTRONICS LIMITED
KRAMER	HP	Aopen	GENTEC INTERNATIONAL	NYL HOLDINGS LLC.	SPACEPOLE, INC.
LANTRONIX	Intel		GENTEC MARKETING INC	OBUSFORME	SPARKLE POWER INC.
LAPCABBY	KASPERSKY LAB INC.	APC	GENTEK MARKETING INC.	OKIDATA AMERICAS INC.	SPECTRUM BRANDS CANADA, INC.
LEGRAND	KASPERSKY LABS CDN\$	AppSpace			SPEECH PROCESSING
MAXON	KASPERSKY LABS CDN\$	Arbor Networks	GENTEK MARKETING INC.	OKIDATA SUPPLIES	SOLUTIONS CANADA INC.
MCAFFEE	CONSIGNMENT	AREA 1 SECURITY, INC.	Getac Inc.	ONELAN LTD.	SPOTIFY AB
MELLANOX	KASPERSKY LABS, INC. ESD	Arista Networks	GFI Software	OPEN TEXT CORPORATION	SPRACHT
MICROFOCUS	KINGSTON DIGITAL, INC	Arlo	Gigabyte	OPENGear, INC.	STANDARD IP SOLUTIONS LTD., DBA STANDARD TELECOM
MITEL NETW	KINGSTON TECHNOLOGY	ARROW ELECTRONICS, INC.	GLOBAL KNOWLEDGE	OPTOMA TECHNOLOGY INC.	STEELCASE INC.
NETAPP	COMPANY	ASCOM WIRELESS	GOLDSEAL PALO ALTO	ORESUS INC	STM BAGS, LLC
NETGEAR	KYOCERA DOCUMENT SOLUTIONS CANADA, LTD.	SOLUTIONS	GOLDSEAL POLYCOM	ORTHOVIA COMERCIO DE PRODUTOS DE INFORMATICA	STORAGECRAFT TECHNOLOGY CORPORATION

NUTANIX OMNIVEX	Lenovo Lexmark	ASSA ABLOY RESIDENTIAL GROUP, INC. D/B/A/ YALE RESIDENTIAL	Gumdrop Cases GUNNAR OPTIKS LLC	OVERLAND STORAGE Palo Alto Networks	STORMAGIC LTD SUNFLEX
OVERLAND	LG	ASUS	Hammond Manufacturin	PANORAMA ANTENNAS LTD	SWANN COMMUNICATIONS USA INC.
QUATRRO	Logitech	Asustor	HAVIS, INC HEADWIND CONSUMER PRODUCTS	PANORAMA ANTENNAS LTD.	SWIFTPAGE ACT! LLC
RARITAN	MALWAREBYTES INC.	Aten Technology		PARA SYSTEMS, INC. PARAGON SOFTWARE GROUP CORPORATION	SWISS ARMY BRANDS LTD
REALVNC	Microsoft	Audiocodes AVANQUEST NORTH AMERICA, INC.	HID Corporation		SYBASE INC
RSA SAFCO PRODUCTS	MOBILE EDGE LLC NEC Display	AVTEQ	Hikvision Digital Technology HIPPIUS N.V.	PARROT INC. PATRIOT MEMORY	SYNACOR, INC. SOLUTIONS CAD
SERVICE	ORACLE CANADA ULC	Axis Communications	HOMEVISION TECHNOLOGY INC.	PEERLESS INDUSTRIES	SYNNEX SUPPLY CHAIN SOLUTIONS USD
SHARP	PANASONIC CANADA	AZiO	House of Marley	PELICAN PRODUCTS, INC PERFECT PRESSURE POINT LLC	SYNOLOGY AMERICA CORP.
SHERWEB	PANASONIC CANADA	BABYTEL INC.	HOVMAND A/S HUMANSCALE CORPORATION		T.G.3 ELECTRONICS, INC.
SKYIAAS	PANASONIC CANADA	BAKKER ELKHUIZEN		PERFORMANCE DESIGNED	TAPLOCK
SOFTCHOICE	CONSUMER DIV	INTERNATIONAL BV	IGEL AMERICA SALES CORP	PRODUCTS LLC	TEAM GROUP INC.
SOLARWINDS	PANASONIC CANADA INC.	Barco	IGLOO PRODUCTS CORP.	PFU CANADA INC.	TEAMVIEWER GMBH
SONICWALL	PANASONIC CANADA INC.	Barracuda Networks	IKEY LTD.	PHYBRIDGE INC.	TECH WRECKERS INC.
SUSE SYMANTEC	PANASONIC-TRADE PARALLELS INC	Battery Technology Inc. Belkin	IMAGICLE SPA IMPACT PRINTING AND	PI ENGINEERING PLANAR SYSTEMS INC.	TEKLYNX INTERNATIONAL TELEFIELD NA, INC.
TECH DATA	PARALLELS INC,	BenQ	GRAPHICS, LTD	Polycom	TELSTRAT INTERNATIONAL LTD
THINKON	PNY TECHNOLOGIES	BeyondTrust Corp	IMPERVA INC	POSH MANUFACTURING LTD.	TELUS COMMUNICATIONS
TRANSITION NET	QNAP INC.	BitDefender	INDIVIDUAL SOFTWARE INC.	POSTURITE LTD	COMPANY
TRENDMICRO	QUANTUM CORPORATION	Black Box Corporation	Infoblox	PRECISION MOUNTING TECHNOLOGIES LTD. PRESSPLAY	TERADICI CORPORATION TESSCO TECHNOLOGIES INC.
ULINE	QUARK INC.	BLACK PEARL MAIL INC.	INNOVATIVE		
VARIDESK	QUEST USA CORP.	BlackBerry	INSPIRAL MARKETING (A DIVISION OF SYNNEX)	PRESTIGE INTERNATIONAL INC.	TEXAS INSTRUMENTS CANADA THALES DIS CPL CANADA, INC.
VEEAM	Red Hat	BLU PRODUCTS, INC.	INTRACOM USA INC.	PRIME IMAGING PRODUCTS PRINTEK, INC. PRINTER PROPERTIES PRO, LLC	THE GOOD USE COMPANY LTD
VERITAS	RIVERBED TECHNOLOGY, INC	BLUECAT NETWORKS INC.	INTUIT CANADA ULC		THE JOY FACTORY, INC. THERMALTAKE TECHNOLOGY INC.
VERTIV	RUCKUS WIRELESS, INC.	Bosch	INTUIT CANADA ULC ESD	D/B/A/PRINTERLOGIC	THOUSANDEALS INC.
VMWARE	Samsung	Bose	IOGEAR INC.	PRINTRONIX LLC	THREATTRACK SECURITY, INC.
	Seagate	Brainboxes BRAND MANAGEMENT GROUP	IT FOR LESS	PRO GAMERSWARE GMBH	
	SEAL SHIELD CORPORATION		Jabra	PROMETHEAN INC	THULE INC.
	SKYKICK, INC.	BROAD ELECTRONICS	JAM	PROMISE TECHNOLOGY, INC	TIBCO SOFTWARE (IRELAND)
	SONY ELECTRONICS INC SONY OF CANADA Startech.com	(AMERICA) INC. BROADCOM INC BROADCOM INC	JAR SYSTEMS LLC. JT COMPUTERS INC. Juniper Networks	PROTECT COMPUTER PRODUCTS INC PULSE SECURE, LLC PURPLE WIFI LTD QUICKEN INC. ESD QUNIFI LIMITED	LIMITED TLM TRADING INC. TP-LINK CANADA INC.
	SUPERMICRO COMPUTER INC	Brydge	JVCKENWOOD CANADA INC.		TRACTIVE GMBH
	TARGUS CANADA	Buffalo Technology	KANO COMPUTING LTD. KEATING - EREPLACEMENTS, LLC KEATING - RIVA CASE	R-GO TOOLS	TRANSCEND INFORMATION
	TOSHIBA AMERICA ELECTRONIC COMPONENTS, INC. TOSHIBA OF CANADA LIMITED	BULLGUARD US, INC. ESD C/O WEINER LLC.	KEATING- BROADSIGN INTERNATIONAL	RACK SOLUTIONS, INC RACKMOUNT.IT, LLC	TRENDNET, INC TRIPWIRE,INC
	TOSHIBA-TRADE	C2G CANADA - Calendar 2020 CANADIAN ESSENTIALS LTD. CAPITAL NETWORKS LIMITED	KEMP TECHNOLOGIES INC	RADWARE INC.	TROY GROUP INC.
	TRIPP LITE	CAPSA SOLUTIONS, LLC, DBA	KERIO TECHNOLOGIES INC	RAZER USA LTD.	TUFIN SOFTWARE NORTH
	VERBATIM AMERICAS LLC		KEY OVATION	REACHSIGHT INC.	U.S ROBOTICS
	VERBATIM AMERICAS LLC - MAD CATZ	CAPSA HEALTHCARE Casio	KEYSIGHT TECHNOLOGIES CANADA INC. KINESIS KKM ELECTRONICS GROUP INC.	REALDEFENSE LLC- CONSIGNMENT	UNITECH AMERICA INC. UNYTOUCH
	Viewsonic	CBM METAL (CANADIAN		REALITY BYTES INC	USA VISION SYSTEMS INC
	WATCHGUARD TECHNOLOGIES INC.	BUSINESS M CDI COMPUTER DEALERS INC	KONFTEL INC KONICA-TRADE	RELAUNCH AGGREGATOR RELAUNCH AGGREGATOR	UTIMACO INC VALCOM INC
	Xerox	CEDAR ELECTRONICS	KORE DESIGN, LLC	CONSIGNMENT	VARONIS SYSTEMS CORP.

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	United Data Technologies
Print Name	David Wiese / Vice President
Address	100 Congress Avenue Ste 2000
City, State, Zip	Austin, Texas 78701
Authorized signature	<i>David Wiese</i>
Date	11-18-21

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 statutes 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

David Wiese

Date

11-18-21

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	United Data Technologies
Address	100 Congress Avenue Ste 2000
City/State/Zip	Austin, Texas 78701
Telephone No.	512*466-3405
Fax No.	954-432-5203
Email address	dwiese@udtonline.com
Printed name	David Wiese
Position with company	Vice President
Authorized signature	<i>David Wiese</i>

Required Clauses for Federal Funds Certifications

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.

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 applicable requirements 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 be 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 be 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>