Contents

Marketing Concepts for Award Engagements

Caetra.io will work with specific AEPA agencies to craft a marketing model that would resonate with the respective region or territory. Because each region may have different objectives or engagement styles that work best for the constituent base, Caetra.io will utilize a variety of approaches to inform not only AEPA agencies but local Education Service Agencies (ESA) and discrete districts on why the CyMetric platform can support risk management, cyber program assessment, risk communication and risk remediation needs. Historically, Caetra.io has used a combination of direct email campaigns, educational webinar series, and co-promotions with managed security service provider vendors/partners, ESAs and our law firm partner organization. However, given the relationship the AEPA has with its member agencies and constituents, working with the AEPA to model something that they feel would work within specific geographies would likely be the best approach. We have been told by AEPA personnel that when communications come from the AEPA, they are generally opened/reviewed significantly more than emails coming directly from vendors. We would seek to leverage those relationships to maximize opportunities and people's time.

Marketing concepts aligned to the mission of the AEPA RFP (Cyber security):

- Webinar/Education Series: Risk management with attorney partners (e.g. "What to Expect When You Are Expecting: The Anatomy of a Data Incident"), Insurance Industry Risk Seminar, Real-Life Stories: Surviving a Ransomware Event with a K-12 District, How to Prevent and Prepare for Data Incidents, Educating the Administrator: Teaching What is Important and How to Ask the Right Questions of Your Cyber Governance and IT Team, What is the Dark Web and What Can be Found There?

- Traditional Outbound Email Campaigns

- Co-Promotion with Managed Security Service Providers Aligning Objectives for Data Privacy and Data Security

Partner/Customer Training Plan Initiatives

Caetra.io is responsible for training our business partners, agencies and end users on the use of the platform. Once they are conversant in the tool, they will be able to handle functional questions from the user base. Scheduled quarterly trainings serve as a refresh on existing functionality along with updates on new functionality built in or will be built into the platform. Caetra.io participates in sales/pre-sales calls with prospective customers to support agencies and business partners to the extent it is needed. Depending upon the model ultimately defined between agencies, the AEPA and Caetra.io, all entities can be provided access to a sandbox platform to test, train and experiment with the platform. All delivery personnel will be highly trained and capable of high levels of execution and efficiency with CyMetric. Should a customer choose to acquire CyMetric and begin to self-service their account, the proper engagement model can be designed that allows for proper handoff and training.

Due to the nature of the platform and the needs of customers, various modules are leveraged in stages. The stages can be broken down into the following rough outline:

1. Onboarding: system and data management, data risk analysis, system ownership, compliance objectives/control definition

2. Control ownership and approval (governance), control configuration, policy generation and approval

3. Assessment plan generation, assessment methods and objects, control scoring, findings definition, POAM report

4. Reporting and dashboard, program maintenance, program evolution

Each of these stages comprises a training element that is typically 60-90 minutes in duration. Caetra.io does not get many real-time requests for support – currently 1-2 messages per month. In many cases, real-time inquiries are handled by the chat feature built into the platform managed by Caetra.io personnel.Caetra.io has built in a comprehensive self-service help file available within the platform. Many questions are answered via those articles with new articles being created regularly.

CyMetric Sample Training Plan: Onboarding to Assessments

Part 1: CyMetric Set Up (60-90 Mins)

- Defining Organization Details
- Inputting Users and Contacts
- Reviewing Information Types and Systems
- Add/Edit Information Type
- Add/Edit Information System
- Understanding Control Owners
- Approving Controls
    - o By Triggering Event
    - o Bulk Approval
- System and Data Reports

Part 2: CyMetric Set Up: Continued (60-90 Mins)

- Review Approving Controls
- Configure Controls with Variables (if applicable)

- Create Multiple Configurations for a Control

- Apply Control Configurations to a System

- Generate Standards/Procedural Documents/Written Information security Plan

- Control Reports

Part 3: Assessing/Auditing Compliance Program (90 Mins)

- Building an Assessment Plan

- Executing an Assessment Plan

  o Define Methods and Objects

  o Rating/Scoring Control Implementation

  o Documenting Rationale for Rating

  o Appending documents/artifacts to the assessment

  o Adding/Documenting Findings (Issues) with Control Implementation

  o Saving/Editing Control Assessment

  o Applying Control Assessment to Multiple Systems

  o Closing an Assessment

- Generate Assessment Report/View Dashboard

AFFIRMATIVE ACTION QUESTIONNAIRE

1. Our company has a federal Affirmative Action Plan approval. ☐ Yes ☒ No

      If yes, please attach a copy of the plan to this questionnaire.

2. Our company has a New Jersey State Certificate of Employee Information Report. ☐ Yes ☒ No

      If yes, please attach a copy of the certificate to this questionnaire.

3. If you answered "*NO*" to both questions above, No. 1 and 2, you must apply for an Affirmative Action Employee Information Report – Form AA302.

Please visit the New Jersey Department of Treasury website for the Division of Public Contracts Equal Employment Opportunity Compliance:

https://www.nj.gov/treasury/contract_compliance/

    a. Click on "Employee Information Report"
    b. Complete and submit the form with the *appropriate payment* to:

Department of Treasury
Division of Purchase and Property
Contract Compliance and Audit Unit
EEO Monitoring P.O. Box 206
Trenton, New Jersey 08625-0206

All fees for this application are to be paid directly to the State of New Jersey. A copy shall be submitted to the ESCNJ prior to the execution or award of contract.
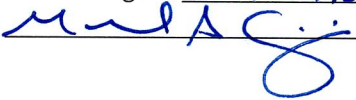
I certify that the above information is correct to the best of my knowledge.

Name of Company/Firm __CAETRA.10, INC__

Address __99 GARNSEY RD__
City, State, Zip __PITTSFORD NY 14534__

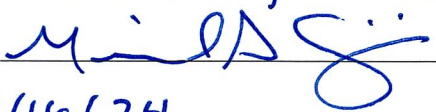Name of Authorized Agent __MICHAEL COMPISI__ Title __PRESIDENT__
SIGNATURE _____ Date __9/16/24__

The contractor and the Educational Services Commission of New Jersey (hereafter "owner") do hereby agree that the provisions of Title 11 of the Americans with Disabilities Act of 1990 (the "Act") (42 U.S.C. S121 01 et seq.), which prohibits discrimination on the basis of disability by public entities in all services, programs, and activities provided or made available by public entities, and the rules and regulations promulgated pursuant there unto, are made a part of this contract. In providing any aid, benefit, or service on behalf of the owner pursuant to this contract, the contractor agrees that the performance shall be in strict compliance with the Act. In the event that the contractor, its agents, servants, employees, or subcontractors violate or are alleged to have violated the Act during the performance of this contract, the contractor shall defend the owner in any action or administrative proceeding commenced pursuant to this Act. The contractor shall indemnify, protect, and save harmless the owner, its agents, servants, and employees from and against any and all suits, claims, losses, demands, or damages, of whatever kind or nature arising out of or claimed to arise out of the alleged violation. The contractor shall, at its own expense, appear, defend, and pay any and all charges for legal services and any and all costs and other expenses arising from such action or administrative proceeding or incurred in connection therewith. In any and all complaints brought pursuant to the owner's grievance procedure, the contractor agrees to abide by any decision of the owner which is rendered pursuant to said grievance procedure. If any action or administrative proceeding results in an award of damages against the owner, or if the owner incurs any expense to cure a violation of the ADA which has been brought pursuant to its grievance procedure, the contractor shall satisfy and discharge the same at its own expense.

The owner shall, as soon as practicable after a claim has been made against it, give written notice thereof to the contractor along with full and complete particulars of the claim, If any action or administrative proceeding is brought against the owner or any of its agents, servants, and employees, the *owner shall* expeditiously forward or have forwarded to the contractor every demand, complaint, notice, summons, pleading, or other process received by the owner or its representatives.

It is expressly agreed and understood that any approval by the owner of the services provided by the contractor pursuant to this contract will not relieve the contractor of the obligation to comply with the Act and to defend, indemnify, protect, and save harmless the owner pursuant to this paragraph.

It is further agreed and understood that the owner assumes no obligation to indemnify or save harmless the contractor, its agents, servants, employees and subcontractors for any claim which may arise out of their performance of this Agreement. Furthermore, the contractor expressly understands and agrees that the provisions of this indemnification clause shall in no way limit the contractor's obligations assumed in this Agreement, nor shall they be construed to relieve the contractor from any liability, nor preclude the owner from taking any other actions available to it under any other provisions of the Agreement or otherwise at law.

Company _CAETRA.10, INC_   Name _MICHAEL COMPISI_

Signature _[signature]_   Title _PRESIDENT_

Date: _9/16/24_

133

ASSURANCE OF COMPLIANCE

Contact with Students

There may be times during the performance of this contract, where a contracted service provider may come in contact with students of the school district. The district fully understands it obligation to provide to all students and staff members, a safe educational environment. To this end, the district is requiring all bidders to sign a statement of Assurance of Compliance, acknowledging the bidder's understanding of the below listed requirements and further acknowledging the bidder's assurance of compliance with those listed requirements.

Anti-Bullying Reporting--Requirement

When applicable, the contracted service provider shall comply with all applicable provisions of the New Jersey Anti-Bullying Bill of Rights Act—N.J.S.A. 18A:37-13.1 et seq., all applicable code and regulations, and the Anti-Bullying Policy of the Board of Education. In accordance with N.J.A.C. 6A:16-7.7 (c), a contracted service provider, who has witnessed, or has reliable information that a student has been subject to harassment, intimidation, or bullying shall immediately report the incident to any school administrator or safe schools resource officer, or the School Business Administrator/Board Secretary.

Criminal History Background Checks—N.J.S.A. 18A:6-7.1--Requirement

When applicable, the contracted service provider, shall provide to the school district prior to commencement of contract, evidence or proof that each employee assigned to provide services and that comes in **regular contact** with students, has had a criminal history background check, and furthermore, that said background check indicates that no criminal history record information exists on file for that worker. Failure to provide a proof of criminal history background check for any employee coming in regular contact with students, prior to commencement of contact, may be cause for breach of contract. See NJDOE Broadcast 9/9/19.

Pre-Employment Requirements

When applicable, all contracted service providers, whose employees have **regular contact with students**, shall comply with the Pre-Employment Requirements in accordance with New Jersey P.L. 2018 c.5, N.J.S.A. 18A:6-7.6 et seq. Contracted service providers are to review the following New Jersey Department of Education Office of Student Protection—Pre-Employment Resource P.L. 2018 c.5 link below for guidance and compliance procedures.

https://www.nj.gov/education/crimhist/preemployment/

Name of Company _CAETRA. 10, INC._

Name of Authorized Representative _MICHAEL COMPISI_

Signature _____ Date _9/16/24_

EXHIBIT A
MANDATORY EQUAL EMPLOYMENT OPPORTUNITY LANGUAGE
N.J.S.A. 10:5-31 et seq. (P.L. 1975, C. 127)
N.J.A.C. 17:27
GOODS, PROFESSIONAL SERVICE AND GENERAL SERVICE CONTRACTS

During the performance of this contract, the contractor agrees as follows:

The contractor or subcontractor, where applicable, will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Except with respect to affectional or sexual orientation and gender identity or expression, the contractor will ensure that equal employment opportunity is afforded to such applicants in recruitment and employment, and that employees are treated during employment, without regard to their age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Such equal employment opportunity 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. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Public Agency Compliance Officer setting forth provisions of this nondiscrimination clause.

The contractor or subcontractor, where applicable will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex.

The contractor or subcontractor will send to each labor union, with which it has a collective bargaining agreement, a notice, to be provided by the agency contracting officer, advising the labor union of the contractor's commitments under this chapter and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

The contractor or subcontractor, where applicable, agrees to comply with any regulations promulgated by the Treasurer pursuant to N.J.S.A. 10:5-31 et seq., as amended and supplemented from time to time and the Americans with Disabilities Act.

The contractor or subcontractor agrees to make good faith efforts to meet targeted county employment goals established in accordance with N.J.A.C. 17:27-5.2.

The contractor or subcontractor agrees to inform in writing its appropriate recruitment agencies including, but not limited to, employment agencies, placement bureaus, colleges, universities, and labor unions, that it does not discriminate on the basis of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, and that it will discontinue the use of any recruitment agency which engages in direct or indirect discriminatory practices.

The contractor or subcontractor agrees to revise any of its testing procedures, if necessary, to assure that all personnel testing conforms with the principles of job related testing, as established by the statutes and court decisions of the State of New Jersey and as established by applicable Federal law and applicable Federal court decisions.

In conforming with the targeted employment goals, the contractor or subcontractor agrees to review all procedures relating to transfer, upgrading, downgrading and layoff to ensure that all such actions are taken without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, consistent with the statutes and court decisions of the State of New Jersey, and applicable Federal law and applicable Federal court decisions.
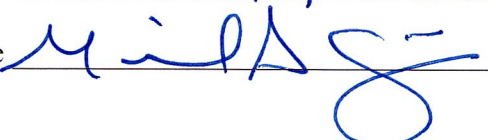
The contractor shall submit to the public agency, after notification of award but prior to execution of a goods and services contract, one of the following three documents:
- Letter of Federal Affirmative Action Plan Approval
- Certificate of Employee Information Report
- Employee Information Report Form AA302 (electronically provided by the Division and distributed to the public agency through the Division's website at https://www.nj.gov/treasury/contract_compliance/

The contractor and its subcontractors shall furnish such reports or other documents to the Division of Purchase & Property, CCAU, EEO Monitoring Program as may be requested by the office from time to time in order to carry out the purposes of these regulations, and public agencies shall furnish such information as may be requested by the Division of Purchase & Property, CCAU, EEO Monitoring Program for conducting an investigation pursuant to N.J.A.C. 17:27-1.1 et seq.

Company _CAETRA.10, INC._   Name _MICHAEL COMPISI_

Signature _[signature]_   Title _PRESIDENT_

135

Form AA302
Rev. 02/22

STATE OF NEW JERSEY
Division of Purchase & Property
Contract Compliance Audit Unit
EEO Monitoring Program
EMPLOYEE INFORMATION REPORT

IMPORTANT-READ INSTRUCTIONS CAREFULLY BEFORE COMPLETING FORM. FAILURE TO PROPERLY COMPLETE THE ENTIRE FORM AND TO SUBMIT THE REQUIRED $150.00 FEE MAY DELAY ISSUANCE OF YOUR CERTIFICATE. DO NOT SUBMIT EEO-1 REPORT FOR SECTION B, ITEM 11. For Instructions on completing the form, go to:
https://www.nj.gov/treasury/contract_compliance/documents/pdf/forms/aa302ins.pdf

SECTION A - COMPANY IDENTIFICATION

1. FID. NO. OR SOCIAL SECURITY	2. TYPE OF BUSINESS	3. TOTAL NO. EMPLOYEES IN THE ENTIRE COMPANY
82-4157572	☐ 1. MFG ☐ 2. SERVICE ☐ 3. WHOLESALE ☐ 4. RETAIL ☒ 5. OTHER	1

4. COMPANY NAME: Caetra.io, Inc.   COMPANY E-MAIL: contact@caetra.io

5. STREET	CITY	COUNTY	STATE	ZIP CODE
99 Garnsey Rd	Pittsford	Monroe	NY	14534

6. NAME OF PARENT OR AFFILIATED COMPANY (IF NONE, SO INDICATE)	CITY	STATE	ZIP CODE
None			

7. CHECK ONE: IS THE COMPANY: ☒ SINGLE-ESTABLISHMENT EMPLOYER ☐ MULTI-ESTABLISHMENT EMPLOYER

8. IF MULTI-ESTABLISHMENT EMPLOYER, STATE THE NUMBER OF ESTABLISHMENTS IN NJ

9. TOTAL NUMBER OF EMPLOYEES AT ESTABLISHMENT WHICH HAS BEEN AWARDED THE CONTRACT: 1

10. PUBLIC AGENCY AWARDING CONTRACT

	CITY	COUNTY	STATE	ZIP CODE

Official Use Only	DATE RECEIVED	INAUG.DATE	ASSIGNED CERTIFICATION NUMBER

SECTION B - EMPLOYMENT DATA

11. Report all permanent, temporary and part-time employees ON YOUR OWN PAYROLL. Enter the appropriate figures on all lines and in all columns. Where there are no employees in a particular category, enter a zero. Include ALL employees, not just those in minority/non-minority categories, in columns 1, 2, & 3. *DO NOT SUBMIT AN EEO-1 REPORT.*

JOB CATEGORIES	ALL EMPLOYEES			PERMANENT MINORITY/NON-MINORITY EMPLOYEE BREAKDOWN											
	COL. 1	COL. 2	COL. 3	********* MALE*********						*********FEMALE*********					
	Total	Male	Female												
	(Cols.2 &3)			BLACK	HISPANIC	AMER INDIAN	ASIAN	NON MIN	2 OR MORE RACES	BLACK	HISPANIC	AMER INDIAN	ASIAN	NON MIN	2 OR MORE RACES
Officials/ Managers	1	1						1							
Professionals															
Technicians															
Sales Workers															
Office & Clerical															
Craftworkers (Skilled)															
Operatives (Semi-skilled)															
Laborers (Unskilled)															
Service Workers															
TOTAL															
Total employment From previous Report (if any)															
The data below shall NOT be included in the figures for the appropriate categories above.															
Temporary & Part-Time Employees															

12. HOW WAS INFORMATION AS TO RACE OR ETHNIC GROUP IN SECTION B OBTAINED?
☒ 1. Visual Survey ☐ 2. Employment Record ☐ 3. Other (Specify)

14. IS THIS THE FIRST Employee Information Report Submitted?
1. YES ☒   2. NO ☐

15. IF NO, DATE LAST REPORT SUBMITTED
MO. DAY YEAR

13. DATES OF PAYROLL PERIOD USED
From: 08/26/2024   To: 09/06/2024

SECTION C - SIGNATURE AND IDENTIFICATION

16. NAME OF PERSON COMPLETING FORM (Print or Type)	SIGNATURE	TITLE	DATE MO DAY YEAR
Michael Compisi		President	09 16 2024

17. ADDRESS NO. & STREET	CITY	COUNTY	STATE	ZIP CODE	PHONE (AREA CODE, NO.,EXTENSION)
99 Garnsey Rd	Pittsford	Monroe	NY	14534	585 - 955 - 4905

Educational Services Commission of New Jersey

Business Office
1660 Stelton Road, Floor 2
Piscataway, New Jersey 08854

Chapter 271
Political Contribution Disclosure Form

(Contracts that Exceed $17,500.00)
Ref. N.J.S.A. 19:44A-20.26

The undersigned, being authorized and knowledgeable of the circumstances, does hereby certify that __CAETRA.IO, INC.__ (Business Entity) has made the following **reportable** political contributions to any elected official, political candidate or any political committee as defined in N.J.S.A. 19:44-20.26 during the twelve (12) months preceding this award of contract:

Reportable Contributions

Date of Contribution	Amount of Contribution	Name of Recipient Elected Official/ Committee/Candidate	Name of Contributor

The Business Entity may attach additional pages if needed.

☒No Reportable Contributions (Please check (✔) if applicable.)

I certify that __CAETRA.IO, INC.__ (Business Entity) made no reportable contributions to any elected official, political candidate or any political committee as defined in N.J.S.A. 19:44-20.26.

Certification

I certify that the information provided above is in full compliance with Public law 2005 – Chapter 271.

Name of Authorized Agent __MICHAEL COMPISI__

Signature __[signature]__ Title __PRESIDENT__

Business Entity __CAETRA.IO, INC.__

139

Prohibited Russia-Belarus Activities & Iran Investment Activities

Person or Entity	CAETRA. 10, INC

Part 1: Certification

COMPLETE PART 1 BY CHECKING **ONE OF THE THREE BOXES BELOW**

Pursuant to law, any person or entity that is a successful bidder or proposer, or otherwise proposes to enter into or renew a contract, for goods or services must complete the certification below prior to contract award to attest, under penalty of perjury, that neither the person or entity, nor any parent entity, subsidiary, or affiliate, is identified on the Department of Treasury's Russia-Belarus list or Chapter 25 list as a person or entity engaging in prohibited activities in Russia, Belarus or Iran. Before a contract for goods or services can be amended or extended, a person or entity must certify that neither the person or entity, nor any parent entity, subsidiary, or affiliate, is identified on the Department of Treasury's Russia-Belarus list. Both lists are found on Treasury's website at the following web addresses:

https://www.nj.gov/treasury/administration/pdf/RussiaBelarusEntityList.pdf
www.state.nj.us/treasury/purchase/pdf/Chapter25List.pdf.

As applicable to the type of contract, the above-referenced lists must be reviewed prior to completing the below certification.

A person or entity unable to make the certification must provide a detailed, accurate, and precise description of the activities of the person or entity, or of a parent entity, subsidiary, or affiliate, engaging in prohibited activities in Russia or Belarus and/or investment activities in Iran. The person or entity must cease engaging in any prohibited activities and provide an updated certification before the contract can be entered into.

If a vendor or contractor is found to be in violation of law, action may be taken as appropriate and as may be provided by law, rule, or contract, including but not limited to imposing sanctions, seeking compliance, recovering damages, declaring the party in default, and seeking debarment or suspension of the party.

CONTRACT AWARDS AND RENEWALS

☒	*I certify, pursuant to law, that neither the person or entity listed above, nor any parent entity, subsidiary, or affiliate appears on the N.J. Department of Treasury's lists of entities engaged in prohibited activities in Russia or Belarus pursuant to P.L. 2022, c. 3 or in investment activities in Iran pursuant to P.L. 2012, c. 25 ("Chapter 25 List"). I further certify that I am the person listed above, or I am an officer or representative of the entity listed above and am authorized to make this certification on its behalf. (Skip Part 2 and sign and complete the Certification below.)*

CONTRACT AMENDMENTS AND EXTENSIONS

☐	*I certify, pursuant to law, that neither the person or entity listed above, nor any parent entity, subsidiary, or affiliate is listed on the N.J. Department of the Treasury's lists of entities determined to be engaged in prohibited activities in Russia or Belarus pursuant to P.L. 2022, c. 3. I further certify that I am the person listed above, or I am an officer or representative of the entity listed above and am authorized to make this certification on its behalf. (Skip Part 2 and sign and complete the Certification below.)*

IF UNABLE TO CERTIFY

☐	*I am unable to certify as above because the person or entity and/or a parent entity, subsidiary, or affiliate is listed on the Department's Russia-Belarus list and/or Chapter 25 Iran list. I will provide a detailed, accurate, and precise description of the activities as directed in Part 2 below, and sign and complete the Certification below. <u>Failure to provide such will prevent the award of the contract to the person or entity, and appropriate penalties, fines, and/or sanctions will be assessed as provided by law.</u>*

Part 2: Additional Information

<u>PLEASE PROVIDE FURTHER INFORMATION RELATED TO PROHIBITED ACTIVITIES IN RUSSIA OR BELARUS AND/OR INVESTMENT ACTIVITIES IN IRAN.</u>

You must provide a detailed, accurate, and precise description of the activities of the person or entity, or of a parent entity, subsidiary, or affiliate, engaging in prohibited activities in Russia or Belarus and/or investment activities in Iran in the space below and, if needed, on additional sheets provided by you.

Part 3: Certification of True and Complete Information

    I, being duly sworn upon my oath, hereby represent and state that the foregoing information and any attachments there, to the best of my knowledge, are true and complete. I attest that I am authorized to execute this certification on behalf of the above-referenced person or entity.

    *I acknowledge that the <**Name of Contracting Unit**> is relying on the information contained herein and hereby acknowledge that I am under a continuing obligation from the date of this certification through the completion of any contracts with the <**Name of Contracting Unit**> to notify the <**Name of Contracting Unit**> in writing of any changes to the answers of information contained herein.*

    *I acknowledge that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification. If I do so, I recognize that I am subject to criminal prosecution under the law and that it will also constitute a material breach of my agreement(s) with the <**Name of Contracting Unit**> and that the <**Name of Contracting Unit**> at its option may declare any contract(s) resulting from this certification void and unenforceable.*

Full Name (Print)	MICHAEL A COMPISI	Title	PRESIDENT
Signature	*(signature)*	Date	9/16/2024

Statement of Suspension or Debarment

STATE OF NEW JERSEY/ _STATE OF NEW YORK_
Specify, of other

COUNTY OF _MONROE_

I, _MICHAEL COMPISI_ of the (City, Town, Borough)

of _PITTSFORD_ State of _NEW YORK_ of full age,

being duly sworn according to law on my oath depose and say that:

I am _PRESIDENT_ of the firm

of _CAETRA.10, INC._ the Bidder

making the Proposal for the above named projects, and that I executed the said Proposal with full authority to do so; that said Bidder is not at the time of the making this bid included on the New Jersey State Treasurer's or the Federal Government's List of Debarred, Suspended or Disqualified Bidders or the State Department of Labor and Workforce Development; Prevailing Wage Debarment List as a result of action taken by any State or Federal Agency.

Name of Contractor: _CAETRA.10, INC._
(Company Name)

By: _____
(Signature of authorized representative)

Subscribed and sworn to before me

This _16th_ day of _September_, 20 _24_

_____
(Seal) Notary Public of New Jersey/
Specify Other State

My Commission expires _8/31_ 20 _26_

KAREN M TROST
Notary Public, State of New York
Qualified in Monroe County
No. 01TR4676208
My Commission Expires August 31, _2026_

146

STATEMENT OF OWNERSHIP DISCLOSURE
N.J.S.A. 52:25-24.2 (P.L. 1977, c.33, as amended by P.L. 2016, c.43)

This statement shall be completed, certified to, and included with all bid and proposal submissions. Failure to submit the required information is cause for automatic rejection of the bid or proposal.

Name of Organization: *CAETRA.10, INC.*
Organization Address: 99 GARNSEY RD. B
City, State, ZIP: PITTSFORD NY 14534

Part I Check the box that represents the type of business organization:

🚒 Sole Proprietorship (skip Parts II and III, execute certification in Part IV)

🚒 Non-Profit Corporation (skip Parts II and III, execute certification in Part IV)

🚒 For-Profit Corporation (any type)   🚒 Limited Liability Company (LLC)

🚒 Partnership   🚒 Limited Partnership   🚒 Limited Liability Partnership (LLP)

🚒 Other (be specific): _____

Part II Check the appropriate box

🚒 The list below contains the names and addresses of all stockholders in the corporation who own 10 percent or more of its stock, of any class, or of all individual partners in the partnership who own a 10 percent or greater interest therein, or of all members in the limited liability company who own a 10 percent or greater interest therein, as the case may be. (**COMPLETE THE LIST BELOW IN THIS SECTION**)

OR

🚒 No one stockholder in the corporation owns 10 percent or more of its stock, of any class, or no individual partner in the partnership owns a 10 percent or greater interest therein, or no member in the limited liability company owns a 10 percent or greater interest therein, as the case may be. (**SKIP TO PART IV**)

(Please attach additional sheets if more space is needed):

Name of Individual or Business Entity	Home Address (for Individuals) or Business Address
HARRIS BEACH PLLC	99 GARNSEY RD PITTSFORD NY 14534

147

Part III DISCLOSURE OF 10% OR GREATER OWNERSHIP IN THE STOCKHOLDERS, PARTNERS OR LLC MEMBERS LISTED IN PART II

If a bidder has a direct or indirect parent entity which is publicly traded, and any person holds a 10 percent or greater beneficial interest in the publicly traded parent entity as of the last annual federal Security and Exchange Commission (SEC) or foreign equivalent filing, ownership disclosure can be met by providing links to the website(s) containing the last annual filing(s) with the federal Securities and Exchange Commission (or foreign equivalent) that contain the name and address of each person holding a 10% or greater beneficial interest in the publicly traded parent entity, along with the relevant page numbers of the filing(s) that contain the information on each such person. **Attach additional sheets if more space is needed**.
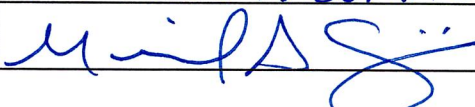
Website (URL) containing the last annual SEC (or foreign equivalent) filing	Page #'s

Please list the names and addresses of each stockholder, partner or member owning a 10 percent or greater interest in any corresponding corporation, partnership and/or limited liability company (LLC) listed in Part II **other than for any publicly traded parent entities referenced above**. The disclosure shall be continued until names and addresses of every non-corporate stockholder, and individual partner, and member exceeding the 10 percent ownership criteria established pursuant to N.J.S.A. 52:25-24.2 has been listed. **Attach additional sheets if more space is needed.**

Stockholder/Partner/Member and Corresponding Entity Listed in Part II	Home Address (for Individuals) or Business Address
HARRIS BEACH PLLC.	99 GARNSEY RD, PITTSFORD NY 14534

Part IV Certification

I, being duly sworn upon my oath, hereby represent that the foregoing information and any attachments thereto to the best of my knowledge are true and complete. I acknowledge: that I am authorized to execute this certification on behalf of the bidder/proposer; that the *ESCNJ and/or its members* is relying on the information contained herein and that I am under a continuing obligation from the date of this certification through the completion of any contracts with the *ESCNJ and/or its members* to notify the *ESCNJ and/or its members* in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification, and if I do so, I am subject to criminal prosecution under the law and that it will constitute a material breach of my agreement(s) with the, permitting the *ESCNJ and/or its members* to declare any contract(s) resulting from this certification void and unenforceable.

Full Name (Print):	MICHAEL A COMPISI	Title:	PRESIDENT
Signature:	*[signature]*	Date:	9/16/2024

This statement shall be completed, certified to, and included with all bid and proposal submissions. Failure to submit the required information is cause for automatic rejection of the bid or proposal.

caetra.io™
Simplifying Compliance, Reducing Risk

CyMetric reflects and facilitates district cybersecurity strategy and drives the process to achieve the overall mission

cymetric™ RISK MANAGEMENT AND COMPLIANCE PLATFORM

CyMetric is a one-stop shop for understanding and documenting the strategy, accountability, activities and status of the cybersecurity program.

The CyMetric platform is a centralized repository that:

- Defines activities that satisfy the requirements of state or federal privacy laws or cybersecurity frameworks written in language technology and risk resources understand

- Documents the cybersecurity and privacy program components that District and State stakeholders need to understand

- Directly ties District network and security processes to elements of their cybersecurity and data privacy program

- Produces reports that articulate the status of the program

- Demonstrates progress of the cybersecurity program over time

- Adapts to changes in state laws or mandates by proactively delivering updated program recommendations reflecting the latest guidance

TO LEARN MORE ABOUT HOW CYMETRIC CAN HELP YOU SUPPORT YOUR SCHOOL:

www.caetra.io | (833) 955-4900

CyMetric Functionality Questions and Answers for K-12 School Districts

Numerous state laws require educational agencies to adopt a policy on data security and privacy that aligns with the state's data security and privacy standard. Many states are choosing the National Institute for Standards and Technology Cybersecurity Framework (NIST CSF) as the standard for educational agencies but that is not the only option. CyMetric is a risk management and compliance platform that helps schools districts and organizations from any industry define, document, manage, evaluate and evolve their cybersecurity and privacy programs. Additionally, CyMetric is a communication tool that enables technology leaders and Data Protection Officers to communicate district risk and maturity of their cyber/privacy programs to stakeholders leveraging graphical dashboards and reports digestible by non-technical personnel. The following content outlines common questions Caetra.io has been asked by our customers as to the applicability and capabilities of the CyMetric platform.

1. Does Caetra.io have experience working with school districts to help them with risk management and compliance initiatives?

Caetra.io has been working with New York State school districts to assist them with Education law 2-d and 8 NYCRR 121 since 2020 and is also working with other K-12 entities in other states with their cybersecurity and privacy challenges. While the K-12 space is not the only market the CyMetric platforms services, it is a very important vertical for the company. Caetra.io currently has 44 school districts subscribing to the CyMetric platform across multiple states.

K-12 Districts Currently Subscribing to CyMetric		
Beacon CSD	Highland Falls-Fort Montgomery CSD	Port Jervis CSD
Bedford CSD	Honeoye Falls Lima CSD	Poughkeepsie CSD
Berks County Intermediate Unit 14	Hyde Park CSD	Red Hook CSD
Byram Hills CSD	Liberty CSD	Rhinebeck CSD
Dover UFSD	Livingston Manor CSD	Rondout Valley CSD
Dutchess BOCES	Marlboro CSD	Roscoe CSD
East Irondequoit CSD	Monroe Woodbury CSD	Sag Harbor CSD
East Rochester UFSD	Monticello CSD	Spackenkill CSD
Eastern Suffolk BOCES	Northwest Tri-County Intermediate Unit 5	Sullivan County BOCES
Eldred CSD	Oley Valley SD	Sullivan West CSD
Fallsburg CSD	Onteora CSD	Tri Valley CSD
Florida UFSD	Orange-Ulster County BOCES	Washingtonville CSD
Gates Chili CSD	Pawling CSD	Webutuck CSD
Greenwood Lake UFSD	Pine Bush CSD	Yorktown CSD
Highland CSD	Pittsford CSD	

2. How does the product help determine the current profile of a district's cybersecurity activities and at what level?

CyMetric helps Districts, and Educational Service Agencies (ESAs) determine their current cybersecurity profile at several stages during the use of the product through a process of definitions and assessments. Our response will be according to each level.

On boarding and initial engagement with CyMetric

CyMetric has, native to the platform, the ability to define the risk associated with the data stored by each organization. These data elements are associated with systems. From this, the overall risk each system creates for the organization is calculated and reported both on screen and in reports which can be provided to various stakeholders for review and approval. As discussed above, new school district customers can leverage the considerable efforts their district colleagues already utilizing CyMetric and borrow from their information systems inventory list, risk classification of these systems, and the data elements that they store. Accordingly, through this process, each scholastic entity has completed both a FIPS 199 and FIPS 200 risk process for all their student, teacher and principal data storing systems with minimal effort. A comprehensive information system and data map is delivered through this process.

The definition of the systems defined by the above process also automatically generates the required NIST or CIS controls needed to meet the obligations of state privacy and security laws or simply implement best practices. CyMetric allows scholastic entities to uniquely configure the controls they use to satisfy the cybersecurity categories and subcategories described by the NIST CSF to suit their specific risk profile. Again, customers under this agreement will benefit from the work of the other Data Protection Officers (DPO) and also have available to them the default configurations for the controls many of their district peers have chosen for their programs. This is particularly valuable for Districts moving from an ad hoc security program to a programmatic one as some of the definition process will be new to them. This will give new customers a baseline to start from and provide peace of mind that these choices are being used by others as reasonable configurations for district security programs. As their program matures, they can then alter selections to meet the unique needs of their district. For DPOs more versed in this process, they can contribute to and improve the selection choices and advance the security profiles for other Districts.

Finally, CyMetric allows Districts to document the procedures they use to support their security controls which defines how they are implementing the controls that support the NIST CSF and state or federal mandates. CyMetric enables districts to add technical or operational procedures to each control along with assigning ownership of the control to a unique individual or role so that they can ensure procedures are followed and reflect the latest developments in their cybersecurity program. The procedures can be viewed within CyMetric or produced as reports for review and collaboration. Defining proper processes and establishing accountability across

the district promotes broader adoption and execution of the security program supporting compliance initiatives.

Security Program Maintenance and Implementation

A CyMetric feature that has resonated with many of our school district customers is the ability to develop a phased implementation program of their final system security plan. Native to the platform are all the recommended NIST 800-53 controls required to fulfill the five categories of the CSF as well as the privacy requirements of state laws or federal laws should they get passed. Numerous districts have elected to develop the maturity or implementation of some controls faster than others. CyMetric worked with K-12 district DPOs and cybersecurity professionals to segment the CSF controls into four unique phases prioritizing controls that would best address vulnerabilities. This segmentation allows these districts to focus on the controls that best address their immediate risk concerns. The definition of the four phases was produced as a result of audits of several districts along with the domain expertise of cybersecurity professionals that refined the models. Using this approach, the evolution of the program can be measured both against the complete stack of controls required by the law and the phases to show how the program is maturing against the system security plan.

CyMetric helps district personnel keep their program current by easily enabling users to update the system security plan to reflect new systems being brought online, defining new data elements stored in their computing environment, modify risk classifications or even add supplemental security controls to the program to reflect changed circumstances or changes in the threat landscape. CyMetric's structured database ensures that any change to the way a system or control is configured will propagate across the entire platform. This process is typically managed by multiple spreadsheets creating error points that are eliminated by the CyMetric structure. Additionally, if the risk analysis shows that a particular system requires a different approach to that control, the system allows the user to create a unique configuration for that system and create special procedures that apply only to it. Accordingly, the platform is both as general and as specific as it needs to be for every system it supports.

CyMetric also allows users to regenerate their system security plan and procedural documents with a simple wizard. After new controls, configurations, systems, or data types are added, our customers can create new versions of their system security program documentation in less than a minute. Before, with spreadsheets, this could take organizations weeks to accomplish.

Assessments and Audits

An important design function of CyMetric is its association of controls with the unique requirements of each regulation and framework it supports. Because measuring or evaluating controls are the basis for determining compliance, this association is significant because when an organization measures the maturity of its controls, we can automatically measure the overall compliance to a regulation or security framework. Customers can assess their controls either globally across all systems or on a system by system level. This allows CyMetric to report on the organization's overall performance with respect to its compliance obligations or to the security

framework it is seeking to implement. Scoring is automatically calculated and where a control has implementation issues or findings, CyMetric reports on the organization's plan for remediation as well as how that finding impacts the organization's ability to satisfy each requirement of the regulation or framework.

Other approaches to assessments are questionnaire based and solicit interviewee opinion about the organizations' ability to deliver on its responsibilities and capabilities.   The primary shortcoming of this approach is that it is not based upon objective measurements of the constituent controls required by the mandate. Accordingly, when a significant cybersecurity event occurs and specific controls are identified as not being properly implemented, the organization will not be able to defend or justify its prior assessments because the individual controls were never actually measured or evaluated in accordance with best practices.

A further power of CyMetric is that it stores each assessment. When performing a new assessment, users can appreciate what was previously determined and either carry those findings forward or edit them to reflect any changes. Utilizing previously evaluated controls saves a significant amount of work and creates efficiencies allowing for districts to do more with less resources.

General Features

o   Linking to source documents. CyMetric offers its user several opportunities to create links to external documents. When defining systems, performing assessments or creating procedures, users can, in addition to adding any rich text they deem appropriate, hyper-link to a reference or demonstrative document which is stored on a server or location controlled by the organization. This has two benefits. It allows an organization to maintain "a single source of truth" by keeping only one instance of the reference document. It also reduces risk for the organization because the content is protected in only one place and only those authorized to access that document can do so.

o   Multifactor Authentication. Although no student, teacher or principal data is expected to be stored in CyMetric, we still appreciate the risk presented by documenting a system security plan and any findings associated with the controls that support that plan. To protect this information, we have implemented MFA as an option so that users can better protect their information.

o   An existing userbase of DPO's and CISO's from neighboring BOCES, RICs and Districts to interact with and improve Districts' cybersecurity programs. Since CyMetric normalizes security and privacy requirements to a set of controls, Districts have a common lexicon and set of activities that they can work with and seek to achieve. No one needs to wonder what others are doing or how they are doing it. They can work together to improve the protection of private data.

o   Tracks trends within the district cybersecurity and privacy program by enabling year-to-year comparisons of audits to see how the program is evolving and where resources need to be applied to ensure risks are being properly addressed.

o The CyMetric approach of utilizing a standard set of controls and assessment process allows the consortium to comprehend how the collective group of school districts are performing in the context of their peers. The concept of "big data" is not new but being able to utilize anonymized data to share security program maturity ratings across the statewide audience is very powerful. The consortium can understand how districts in their respective regions are performing and where they are having challenges with implementation. This will help the consortium develop professional development and training programs, negotiate better contracts with third-party vendors who can support districts in the areas where they have deficiencies and keep NYSED informed with overall performance of the state.

3. Can the product generate a Target Profile for common desired cybersecurity outcomes?

Yes. As described above, CyMetric has within it the analysis of the lawyers from Harris Beach PLLC and presents a target profile of desired cybersecurity outcomes to meet various state laws and cyber frameworks designed to protect student and staff data. Goals for effective implementation can be defined at the district level with CyMetric providing reports that define how well the districts are meeting those targets. Moreover, thanks to the efforts of other district DPOs and the BOCES with which they work, there is a phased implementation or maturity plan that lets them execute their programs in defined and manageable stages while measuring how far along they are towards their long-term target profile.

4. Describe how the product can create an action plan to identify necessary steps and prioritize the mitigation of gaps.

CyMetric meets this requirement during the assessment phase described above. In addition to measuring and scoring the functional effectiveness of a control, the assessor can also document any findings or issues discovered regarding the control and score the severity of those issues. Further, the organization has the ability to document its remediation plan and its anticipated closure date. All of this is then produced in an editable Plan of Action and Milestone (POAM) report. The POAM also aligns these findings with the requirements of the regulation or framework the control supports so an organization can appreciate the risks associated with the findings both from a cybersecurity standpoint and from a regulatory perspective.

5. Describe the ease of implementation.

Ease of use and understanding for users at any skill level

The CyMetric tool is generally very easy to use and navigate. It was designed using contemporary approaches to user experience to minimize the training requirements needed to get started. The ease of use from an interface perspective is supported by Caetra.io training programs to help contextualize why districts need to execute processes and procedures that are a part of their respective programs. Technical resources enjoy the benefit of CyMetric's translation of regulatory requirements into procedural language they can understand. CyMetric

promotes collaboration between business units within an organization seeking to support enterprise-wide involvement in the security and compliance process.

Ease of customization, without training or skills required

Customizing system security plans or specific controls to reflect the unique needs of a district is easy to accomplish. Each CyMetric instance reflects the specific environment of a district in terms of the applications, systems and risk profile identified in the security plan. Districts can use a baseline version of controls and control configurations as a starting point but modify those elements as required by their needs. While it is straightforward to make customizations or changes to a district's program without training, the concept of doing so is still covered in the CyMetric training program delivered to users.

Ease of IT Administration, integration of Directory Services and/or access management system

As a cloud-based application, CyMetric is easily managed and configured. Users can be added or removed from the system depending upon their role and all of this is managed from a dashboard. CyMetric is a completely independent and secure system protected by its own two factor authentication process so that even if the organization suffers a breach, the CyMetric platform will remain self-contained. As a result, CyMetric does not integrate with Directory Services or other access management systems and users will need their own unique passwords.

6. What is the ability of the application to show the level of risk across all activities? Explain

CyMetric has the ability to demonstrate the level of risk across all activities in two ways. First, the platform has a risk module where customers can identify and document risks their information systems pose to the organization. The second way the level of risk is identified is during an assessment. As described above, the organization can document and rank in terms of severity, the implication of any findings associated with a control or process. Since the controls are further associated by the Harris Beach attorneys to the regulation or framework, any defects or gaps in the framework or regulation are revealed and understood by the organization. Moreover, since the risk is expressed in both cybersecurity and legal terms, the risk can be appreciated by a broader group of stakeholders. CyMetric's entire approach is a legal or risk-based methodology. It is unique in its ability to deliver on this requirement.

7. How does the product help prioritize and scope the school district's business objectives and priorities?

CyMetric helps prioritize and scope a school district's business objectives and priorities initially by phasing the maturity plan for the controls that will ultimately comprise the entire system security and privacy plan that supports state laws and cyber framework objectives. This phased strategy was developed by District DPOs and ESA experts and reflects the priorities and scope for each phase that were deemed most important. While this approach reflects the considered prioritization and scope of a few regions, it does not need to be the exclusive plan for all Districts

on the platform. CyMetric has the capability of creating different phased plans depending upon the risks and priorities of different ESA or other supporting entities. Districts have also prioritized their efforts based upon the mission criticality of the systems within their environment. Caetra.io does not have any influence on what those systems are but the CyMetric platform supports whatever priority criteria the districts move forward with.

Following an assessment, CyMetric can further help scope and prioritize the District's objectives by allowing it to prioritize the findings deemed either most significant or the controls viewed as least mature. Since all of these controls are ultimately mapped back to the regulations and frameworks which require them, the school district's business and legal obligations are both appreciated and able to be met.

8. Describe how the product can audit and manage district data privacy policies to align with current policies?

CyMetric has built into it the ability to generate program documents that set forth all the actions a scholastic entity must perform to meet the security and privacy requirements of their cyber security program or state laws. In the event that there are no standard controls that address privacy or notification requirements, the attorneys at our partner Harris Beach create special controls that meet the privacy requirements or custom needs of a cyber security mandate or program objective. Thus, unlike products that support only the NIST CSF, CyMetric executes on all the legal requirements of any law. CyMetric is the only platform that has these custom privacy controls integrated into the general security plan which has been vetted by a law firm. This fulfills our vision of allowing our customers to focus on the activities of security and privacy and let the product take over the function of demonstrating and aligning those activities with policies and the law. As with other aspects of the assessment process, the data privacy and notification elements of the law are also a part of the audit function facilitated by the CyMetric platform.

9. Describe the alignment with functions-controls-processes?

At its core, CyMetric is a control, procedure and process driven platform in its approach to security and data privacy. The policy and standards documents are then created from this set of controls so there is always perfect alignment between all three. Mechanistically at the customer level, CyMetric's database stores the inventory of the district's systems and controls required for those systems. Further, the controls are directly associated with the regulation or framework the organization is trying to meet ensuring the alignment between the systems, controls and procedures needed for meeting obligations. From this, general standards or policy documents are created with language created from templates created by the lawyers at Harris Beach. The policy or standards language integrated into CyMetric is essentially a wrapper surrounding the controls and processes the organization intends to implement. An added benefit of the product is that after new systems or compliance obligations are added, a simple refresh button can be clicked and all the policies, functions and controls are updated, with version control to reflect those changes. These processes and capabilities ensure that alignment is always current.

10. Provide a description of your training model and support system.

Implementation/Onboarding Support: Due to the cloud-based architecture of the CyMetric platform, there is no hardware or software implementation requirements to get CyMetric up and running. To assist with expedited deployment and rapid time to value, Caetra.io offers its school software title inventory with its corresponding baseline data mapping and data risk profile to all school districts that use the CyMetric platform. School districts will select the software titles they use in their district and Caetra.io will import those titles into their specific instance of the CyMetric platform. This process expedites district onboarding reducing significant data entry time in documenting and mapping their environment. It also facilitates the production of deliverables required by the state.

Additionally, should districts require supplemental resources outside of their districts, Caetra.io's network of service provider partners and domain experts/consultants can be introduced to provide immediate and ongoing support for districts to get them where they need to go.

Training: Caetra.io has developed a three-phase, web-based training program specific to K-12 entities that it has already implemented and delivered to existing customers. The CyMetric application also has substantial in-app/online support tools available for users to utilize for self-service training. CyMetric incorporates the use of Intercom, an online support tool enabling customers to contact Caetra.io support via an instant messaging chat function for real-time support with Caetra.io personnel. Intercom also has built-in support documentation detailing product use guidance as well as configuration, operational, and other business considerations.

On-Going Support: Caetra.io strives to ensure its customers are fully equipped to maximize their investment in the CyMetric platform. In addition to onboarding training, online tools and tutorials are continually being added to the platform to support on-going education and use case support.

Regional based refresh/new feature trainings could be scheduled to ensure all personnel are current with the use and capability of the CyMetric platform.

Additional features and functions will be added to CyMetric over time based upon our current development road map and input from the CyMetric user base. Caetra.io produces outbound newsletter announcements of feature enhancements, insights on scenario use-case functionality and scheduled maintenance as a practice to ensure customers are informed on all matters related to CyMetric. Caetra.io will also share insights from our business partner/ownership group law firm that are relevant to the K-12 school district community.

System security - Security Updates and Patch schedules

The application is designed and implemented using modern security design implementation patterns. Customer data is encrypted at rest and TLS is enforced on all communications from the browser to the application instance.

Each quarter, the application dependencies are reviewed and updated to ensure all known security issues are addressed. In addition, new critical security issues are addressed as soon as identified and an analysis indicates the issue impacts the platform.

The application leverages a public 3rd party cryptographic library to authenticate each user during the server-side logon process. Once a user is authenticated, an authorization token is generated and managed via an expiring JavaScript web token (jwt). The jwt and associated server-side allow list validate each request is authorized. Authorization is further enforced at the server and database level to limit access to relevant customer data. On user logout or session expiration, the token is invalidated and purged from the allow list.

11. Does the product have the multi-tenant capability to manage all districts from a single platform?

Because each district is required to have its own security and privacy program in place, all districts/ESAs will have their own instance of the CyMetric application. Districts can invite external entities (ESAs/Third-Party vendors) to access the district instance to provide inputs, assessments and other functions in support of the districts. The inverse of this is also accurate where an ESA can be the principal manager of a district instance and invite school district personnel to the district's discrete CyMetric instance. A true multi-tenant model is not available at the time.

12. Describe the compatibility with other systems.

While our platform is designed to support APIs and uses APIs in its operation, it is a self-contained platform that allows its customers to design policies, system security plans to document their computing environment to assess their security and privacy controls independent of other systems. To date, software products that monitor system security and network status do not currently associate security activities with unique controls rendering compatibility as not an essential element to the automation of the CyMetric platform. Should network security and network monitoring products evolve to accomplish that objective, Caetra.io could align that capability with the CyMetric platform.

13. What other features does the platform bring to the table?

Regulation Monitoring: The lawyers of Harris Beach provide ongoing management and insight to the list of controls associated with the regulation so that as regulations or their interpretation change, the list is updated to reflect the law firm's latest understanding of the legal requirements of each regulation. The monitoring of regulations and the controls is not something districts need to manage as Caetra.io and the CyMetric platform will take care of that for them. School districts or any other organization have the ability to accept or reject these recommendations depending upon the advice they receive from their counsel or the special circumstances of their system environment.

14. How does Caetra.io price the CyMetric platform?

Caetra.io offers its CyMetric platform as a compliance-as-a-service subscription license model. The annual subscription price is based upon the regulation a customer is seeking to comply with. There is no limit to the number of users that can access the tool, no limit on the number of systems that can be populated into the platform or any other limitation that may be imposed by

other platforms. For the purposes of this proposal, the license structure is based upon district acquisition for Education Law 2-d and its regulatory element, 8 NYCRR Part 121 along with the four "phases" of CSF controls that have been designed by a team of New York State school district DPOs to assist with building a structured system security program in manageable phases. The latter of these options is optional to utilize.

Caetra.io has crafted an aggressive pricing schedule for school districts across New York State. Pricing is based upon school district size to accommodate challenges districts have based upon their respective sizes as well as accommodate any services that may be required to support the tool.

15. Is any software required on the client to optimally use your software?

Only an industry standard browser (Chrome, Microsoft Edge, Firefox, Apple Safari) is required to use CyMetric.

CyMetric Talking Points for K-12 School Districts

Mission: Risk Reduction. The primary District goal is to implement cyber frameworks (e.g. NIST CSF) as well as state required control elements into a data security and privacy program. However, there may be areas of specific risk that a District may want to address as a priority like ransomware or cybersecurity insurance acquisition. CyMetric's built in flexibility enables Education Service Agencies (ESAs) and Districts the capability to focus their implementation strategy on immediate threats and risks most important to Districts and thus phase their implementation of the program in a way that is achievable and meaningful. Moreover, since a framework is a prism for viewing the controls that define the functions of the framework, it allows for the custom design of controls that address the functions of the framework without being constrained to a one size fits all approach. ESAs can define custom control sets based on functions within the framework that target specific threat vectors (ransomware) or business focused risk factors (cybersecurity insurance) to address specific needs.

SHORT TERM:

- Questionnaire or environmental assessment-based solutions tend to provide a superficial look at where an organization is with its security program implementation. The execution or measurement of a program cannot be achieved without understanding what activities or controls need to be fulfilled at the system level.
- For public schools, CyMetric defines all of the elements and tasks necessary to meet state mandates out of the box.
- Enables the inventorying of software/hardware assets along with a detailed data map with associated risk profiles. Much of this inventory definition can be automated leveraging the work of other data protection officers.
- Automatically generates framework controls AND the controls for complying with a state's data privacy and notification requirements. CyMetric is the only tool that can supply both the framework control set and the state privacy and notification control sets required to meet the expectations of the law.
- Aligns the controls to the specific elements of the framework and state laws that are being satisfied by the implemented controls - **all legally vetted by a nationally recognized law firm ensuring the output supports the requirements of the law.**
- Standardizing the approach to meeting the compliance obligation makes supporting the mandate easier to manage from an ESA perspective while allowing for District resources to share the workload.
- Dynamically produces procedural/departmental policy documents that reflect the requirements of your district and of state mandates.
- CyMetric does not limit the number of users who can access and interact with the platform. Unlimited district internal and external resources can use CyMetric as a part of their program execution.

- Supports custom phases of implementation for control sets. Districts can work at a pace they define with a set of controls that will form the foundation of their program while they work toward full compliance over time. This allows for setting achievable, realistic goals that districts can accomplish and report on. Beyond this, Districts can add additional controls to address any unique risk they may encounter.

MEDIUM TERM:

- When districts are ready to evaluate or assess their cyber/privacy program, CyMetric automatically assembles the controls that need to be audited in one repository eliminating the need for multiple spreadsheets. The tool also enables users to define how and what they are auditing enabling documentation of the program that is used for reporting. CyMetric produces detailed reports and highlights remediation plans for issues with the program found during the assessment process (Plan of Action and Milestone – POAM Report) along with a dashboard highlighting the status of the program.
- Districts can farm out work (control evaluation, gap analysis, policy review, etc.) to external sources to offload some of the management of their compliance program.
- If states alter the requirements of the law or indicates areas of focus for auditing the program, CyMetric updates the platform automatically to ensure districts programs are current with the latest control sets.
- Districts can enhance their individual programs with supplemental controls that address specific needs or risks they have.

LONG TERM:

- Districts can review previous audits/assessments to track their program over time looking for trends or other data points that provide insight on their program.
- In some cases, specific control assessments can be repurposed/reapplied to their audits without having to re-evaluate the control.
- Should a District need to develop compliance programs for other obligations (e.g. NY SHIELD, HIPAA, CPRA, etc.), CyMetric aligns those obligations to the controls already in place consolidating multiple programs reducing the workload to add a new obligation.
- ESAs have visibility into their component District bases to produce reports that allow for regional comparisons with their peer groups. Also, ESAs will be able to see regional trends or needs that may warrant enhanced services that can be provided by the ESA (e.g. professional development programs, new security tools to offer, etc.).

cymetric™

Don't let cybersecurity compliance place your district at risk.

Reduce District risk with CyMetric, a cloud-based delivery tool for ongoing regulatory guidance and security program management.

- Creates a common core for compliance across regions while allowing for district independence

- Automate the development of your standards, practices and procedures for your data privacy and cybersecurity program

- Enables the development of multi-year implementation models to phase in a program that supports district risk and system priorities

- Deploy, assess and evolve your program based upon your system risk, available resources and regulatory or security framework requirements

Protect personal identifiable information and sensitive data with an automated tool enabling you to ace your compliance objectives.

Visit us: www.caetra.io   Book a demo: 833.955.4900

✷ caetra.io™   Simplifying Compliance. Reducing Risk.

How does it benefit the school district?

One of the biggest challenges with any regulation or cybersecurity program is translating it into actions needed to be taken by an organization to meet the law or program requirements.

Cybersecurity frameworks like the NIST CSF, are high level models that provide guidance on security/operational areas (Identify/Protect/Detect/Respond/Recover) that organizations need to focus on in order to have a robust data security program. Frameworks generally do not provide any insight as to how to accomplish that goal – leaving districts having to guess as to how to meet the framework's goals.

CYMETRIC TAKES THE GUESSWORK OUT OF THE PROCESS

Defines processes and controls that satisfy the requirements of your cyber program

- By defining specific processes, procedures and functions (controls) that need to be put into place, CyMetric gives technology directors at the district level (or educational service agency) explicit direction in a language they can understand.

Meets requirement for system inventory to support audits
- The tool outputs system security plan documents that define the data privacy and data security program to which each district attests. All functions and capabilities have been legally vetted by nationally recognized law firm Harris Beach PLLC. to ensure the software platform satisfies the applicable laws that are licensed.

Provides assessment mechanism tool integrated into the platform
- Once districts become empowered to evaluate the implementation and status of the program at the control level, school boards can understand where risks lie and how to prioritize them with their available resources. Caetra.io, the company that provides CyMetric, also provides regulation monitoring to update and reflect any changes to the law or guidance on its implementation with respect to state privacy and data security laws.

From an educational service agency (ESA) perspective, the goal is to create a baseline standard for compliance programs across their region (in place of unique programs for each district) that can be better supported through value-added services potentially delivered from the ESA. Each district can customize their programs based upon their unique circumstances; but the core will be consistent.

How does CyMetric Work?

The essence of CyMetric is that it translates the legal requirements of any regulation or standard into discrete actions that an IT group can both understand and implement. Further, it allows the customer to measure how well their cybersecurity and privacy program is implemented so that the strength or maturity of it can be gauged. CyMetric produces a set of specific controls or processes which support not only the security requirements or supported regulations but also the unique privacy requirements of each law as well. These controls are selected from the National Institute of Standards and Technologies (NIST) SP 800-53 publication, the Center for Internet Security v8 control set or were written and validated by attorneys at a nationally recognized law firm.

CyMetric does the following:

1. Automates the definition of processes and controls that satisfy regulatory or security framework requirements eliminating the need for organization personnel or lawyers to translate the regulation or company policy documents.

2. Standardizes compliance programs on a single set of processes, procedures and controls enabling organizations to easily incorporate other compliance requirements (e.g. NY SHIELD, HIPAA, GDPR, CCPA/CPRA, CMMC) into their program if the need arises.

3. Meets the standard requirement for system inventory and data classification to support audits. CyMetric can leverage outputs from other tools that define software and hardware assets and import them into CyMetric eliminating significant amounts of data entry required to develop an asset inventory.

4. Provides a program assessment mechanism tool integrated into the platform enabling organizations to migrate away from spreadsheet-based program management.

5. Supports the dynamic nature of cybersecurity and privacy program requirements. By creating a centralized repository for all facets of the program, company programs stay current with the changing threat landscape. Updating program documentation and adjusting parameters of their security profile is managed by a few clicks of a mouse. Program evaluation content, system reports, supporting artifacts and documents are easily accessible for facts on demand.

6. Allows for establishing designed phases for program implementation so organizations can build their program in a manageable and time appropriate manner based upon available resources, budget and other factors.

7. Increases efficiency by enabling an unlimited number of users access to the tool at the organizational level. Organizations are free to leverage their internal human assets as well as external resources like consultants and third-party vendors to help manage their programs.

8. Tracks trends within the organization's cybersecurity and privacy program by enabling year-to-year comparisons of audits to see how the program is evolving and where resources need to be applied to ensure risks are being properly addressed.

STAKEHOLDERS

Every control or defined procedure is directly associated with the elements of the regulation it has mapped to. Accordingly, an organization and its many stakeholders understand not only the discrete requirements of these protection functions, but also how, when viewed as a whole, the security program is performing. Thus, for the technologists, they know exactly what they need to do to improve the program and can fully document the procedures they will use to implement each control. For stakeholders who are less technologically focused, they can see a visualization of the program arranged around the requirements of a regulation or security program they are implementing.

CyMetric also delivers all of the required elements specified in the myriad regulations imposed on organizations: asset inventory of information systems, documentation of the data types or information types stored within the organization's environment, plus assigns a risk profile to those assets. Additionally, CyMetric outputs policy and procedural documents that define organizational cybersecurity and privacy programs in support of company policies.

Lastly, CyMetric provides the mechanism to define how well the cybersecurity and privacy program has been implemented through an audit or assessment process evaluating the processes and procedures defined by the program. The outputs from the assessment process present stakeholders with insight as to what aspects of their program are well defined and where there are risks/exposures that need to be addressed. With the relative nascence of most cybersecurity and privacy mandates, should regulators, government agencies or any other entity make changes to the requirements of the law or what a company should be doing to meet the requirements of the law, Caetra.io will monitor for any such changes in the regulation and will push out updates to CyMetric customers. This will ensure that they always have the latest recommendations on how to comply with the law.

ASSESSMENT

An important design function of CyMetric is its association of controls with the unique requirements of each regulation and framework it supports. Because measuring or evaluating controls is the basis for determining compliance, this association is significant because when an organization measures the maturity of its controls, CyMetric can automatically measure the overall compliance to a regulation or security framework. Customers can assess their controls either globally across all systems or on a system by system level. This allows CyMetric to report on the organization's overall performance with respect to its compliance obligations or to the security framework it is seeking to implement. Scoring is automatically calculated and where a control has implementation issues or findings, CyMetric reports on the organization's plan for remediation as well as how that finding impacts the organization's ability to satisfy each requirement of the regulation or framework.

Other approaches to assessments are questionnaire based and solicit interviewee opinion about the organizations' ability to deliver on its responsibilities and capabilities. The primary shortcoming of this approach is that it is not based upon objective measurements of the constituent controls required by the mandate. Accordingly, when a significant cybersecurity event occurs and specific controls are identified as not being properly implemented, the organization will not be able to defend or justify its prior assessments because the individual controls were never actually measured or evaluated in accordance with best practices.

In addition to measuring and scoring the functional effectiveness of a control, the assessor can also document any findings or issues discovered regarding the control and score the severity of those issues. Further, the organization has the ability to document its remediation plan and its anticipated

closure date. All of this is then produced in an editable Plan of Action and Milestone (POAM) report. The POAM also aligns these findings with the requirements of the regulation or framework the control supports so an organization can appreciate the risks associated with the findings both from a cybersecurity standpoint and from a regulatory perspective.

POSITIVE OUTCOMES

Today's hyper-networked and highly-regulated world asks more and more of the executives that conduct business in it. Business leaders need to depend on their technology infrastructure to keep the bad actors at bay and rely on their compliance personnel to monitor the many regulations designed to protect the data they keep. CyMetric integrates the law into the software, producing controls and policies that meet the rigor required by the regulations and align with the technology infrastructure needs outlined by industry standards. CyMetric reduces the dependency on legal counsel to craft controls and policies that may be undermined or even redundant.

By leveraging CyMetric, not only to build your controls and policies but also to update them as regulations change, your compliance personnel can focus their efforts on more impactful initiatives; and your company can focus on strategic initiatives to grow the business.

Contact Us

Email: contact@caetra.io

Phone: 833.955.4900

cymetric™

Caetra.io CyMetric Risk Management Platform Overview

The essence of CyMetric is that it translates the requirements of any regulation or cyber security standard into discrete actions that an IT group can both implement and understand. Further, it allows the customer to measure how well their cybersecurity and privacy program is implemented so that the strength or maturity of it can be gauged. For the school districts and Educational Service Agencies (ESA), CyMetric prescribes a set of specific controls or processes that align to industry standard cyber frameworks like the NIST CSF and SOC2 as well as control sets like Center for Internet Security (CIS) and NIST 800-53. Additionally, the CyMetric platform also is able to provide regulatory insight on aligning with state or federal mandates focused on privacy, notification and other contemporary requirements that do not have standard controls that address them. These custom privacy and notification-oriented controls were written and validated by attorneys at our business partner, the Harris Beach PLLC law firm and integrated into the CyMetric platform ensuring that regulatory compliance is part of the solution. Any federal or state mandate or custom requirement (cyber insurance, contractual obligations, etc.) can be mapped within CyMetric providing a roadmap to meeting those business or operational requirements.

Every control or defined procedure is directly associated with either the elements of a regulation or the preferred cyber framework the organization is implementing. Accordingly, a school district and its many stakeholders understand not only the discrete requirements of these protection functions, but also how, when viewed as a whole, the security program is performing. Thus, for the technologists, they know exactly what they need to do to improve the program and can fully document the procedures they will use to implement each control. For stakeholders who are less technologically focused, they can see a visualization of the program arranged around the requirements of a regulation or cyber framework.

CyMetric delivers insight on how to comply with all of the required elements specified in state and federal privacy and cyber security laws: asset inventory of information systems, documentation of the data types or information types stored within the school districts' environment, plus assigns a risk profile to those assets. Additionally, CyMetric outputs standards/procedural documents that define districts' cybersecurity and privacy programs in support of district policies. Lastly, CyMetric provides the mechanism to define how well the cybersecurity and privacy program has been implemented through an audit or assessment process evaluating the processes and procedures defined by the program. The outputs from the assessment process present stakeholders with insight as to what aspects of their program are well defined and where there are risks/exposures that need to be addressed. With the relative nascence of cyber security and privacy laws, these mandates can be fairly fluid. Should state or federal agencies make changes to the requirements of a mandate or what an organization should

be doing to meet the requirements of the mandate, Caetra.io will monitor for any such changes in the regulation and will push out updates to CyMetric customers. This will ensure that they always have the latest recommendations on how to comply with the law.

CyMetric is currently being used by over 45 New York school districts to meet the requirements of Part 121, Education Law 2-d and the NIST CSF. In working with the various Data Protection Officers from our customer base, Caetra.io has integrated into its CyMetric platform an optional, phased implementation model for the controls required by these standards. This model is based upon a general risk assessment of the schools and an agreed upon prioritization of the controls. The phased implementation model enables districts to focus their initiatives on mission critical applications and priority controls at program initiation while building upon that model as their resources and budget permit. Districts can maximize the value of their efforts while collaborating with their colleagues in other school districts on how to best implement each control.

CyMetric streamlines cybersecurity efforts school districts.

CyMetric does the following:

- o Automates the definition of processes and controls that satisfy the regulatory requirements, cyber/privacy program objectives, cyber insurance requirements and cyber framework objectives eliminating the need for district personnel or lawyers to translate the regulation or district policy documents.

- o Standardizes compliance programs on a single set of processes, procedures and controls enabling districts to easily incorporate other compliance requirements (e.g. NY SHIELD, HIPAA) into their program if the need arises.

- o Meets the requirement for system inventory and data classification to support audits. Leveraging a Caetra.io managed inventory of over 1500 software titles, school districts select which systems they utilize in their environment which are, in turn, imported into CyMetric eliminating significant amounts of data entry required to develop an asset inventory.

- o Provides a program assessment mechanism tool integrated into the platform enabling districts to migrate away from spreadsheet-based program management.

- o Supports the dynamic nature of cybersecurity and privacy program requirements. By creating a centralized repository for all facets of the program, district programs stay current with the changing threat landscape. Updating program documentation and adjusting parameters of their security profile is managed by a few clicks of a mouse. Program evaluation content, system reports, supporting artifacts and documents are easily accessible for facts on demand.

- o Allows for establishing designed phases for program implementation so districts can build their program in a manageable and time appropriate manner based upon available resources, budget and other factors.

- o Increases efficiency by enabling an unlimited number of users access the tool at the district level. Districts are free to leverage their internal human assets as well as external resources like Education Service Agency personnel and third-party vendors to help manage their programs.

- o Tracks trends within the district cybersecurity and privacy program by enabling year-to-year comparisons of audits to see how the program is evolving and where resources need to be applied to ensure risks are being properly addressed.

CyMetric is developed from the ground up with optimal security and privacy processes in place.

Customer data security, integrity, and availability are essential elements of the CyMetric application. CyMetric is architected and designed to ensure customer data is protected from access and disclosure to unauthorized external and internal entities. As part of Caetra's continual efforts, the CyMetric application undergoes periodic 'white hat' penetration testing to identify any possible areas of weakness and to ensure they are not exploitable. Finally, the Caetra Operations team has enacted internal policies and procedures to ensure employees follow industry standards for protecting and preventing unauthorized disclosure of customer data.

The CyMetric application is built with technologies used by many Fortune 1000 companies. The application is designed and implemented using modern security design implementation patterns. Customer data is encrypted at rest and TLS is enforced on all communications from the browser to the application instance. Security certificates ensure the information cannot be decrypted or subverted by external parties.

Each quarter, the application dependencies are reviewed and updated to make certain all known security issues are addressed. In addition, new critical security issues are addressed as soon as identified and an analysis indicates how the issue impacts the platform.

The application leverages a public 3rd party cryptographic library to authenticate each user during the server-side logon process. Once a user is authenticated, an authorization token is generated and managed via an expiring JavaScript web token (jwt). The jwt and associated server-side "allow list" validates each request is authorized. Authorization is further enforced at the server and database level to limit access to relevant customer data. On user logout or session expiration, the token is invalidated and purged from the allow list.

The CyMetric software stack is hosted on Heroku's Platform as a Service (PaaS) offering. Heroku has a dedicated security team constantly monitoring and updating the platform as needed. Due to the nature of PaaS, Heroku's security policies are automatically applied to CyMetric.

In addition, CyMetric uses several Amazon Web Service (AWS) offerings to securely store certain types of customer data such as compliance report pdfs and images in an external cloud service. Further, the CyMetric application ensures that the information stored in the AWS platform is protected by implementing AWS best practices for identity and access management (IAM) and 'least privilege' authorization by enforcing the minimal level of user rights required to perform the user's role.

The CyMetric application provides strong data security built into its architecture. All customer provided compliance data is stored in a Postgres (PostgreSQL) database hosted on Heroku. Postgres is a mature relational database with strong security features utilizing industry best practices ensuring the data is secure. To ensure that customer data is protected at the customer, user, and database levels the CyMetric application uses Postgres' private schemas providing isolation of customer data, role-based access control limiting access to the database, and row level security restricting access within the database. Lastly, all Postgres database data files and backups are 'encrypted at rest' where the data is encrypted on the disk as well as in the shared buffers to ensure that the data cannot be accessed outside of the application.

Data protection and disaster recovery measures ensure that the CyMetric application and customer data will be available and recoverable in the event a catastrophic incident impacting the data center hosting CyMetric. CyMetric builds on Heroku and Amazon's native durability, availability, and disaster recovery services. This, combined with the Caetra Operations Team's recovery procedures, ensures that Caetra is able to transfer data from backups to alternative data centers and restart the application with limited manual actions.

What platforms does the product work in?

CyMetric is a cloud-based software as a service platform. As such, CyMetric works on any platform that supports a web browser.

What are the technical requirements?

CyMetric is a cloud-based application and requires no technical infrastructure, hardware or other components to be installed or put into place in order to utilize the application. CyMetric does require the use of a contemporary web browser to run effectively. The web browsers currently supported by CyMetric are:

- Google Chrome
- Microsoft Edge
- Apple Safari
- Mozilla Firefox

Browsers should be running the most recent versions provided by the manufacturer to maximize security and browser capability.

Part E – Signature Forms: Caetra.io, Inc.

AEPA 025-F
Cyber Security and Training

Uniform Guidance "EDGAR" Certification Form
2 CFR Part 200

When a purchasing agency seeks to procure goods and services using funds under a federal grant or contract, specific federal laws, regulations, and requirements may apply in addition to those under state law. This includes, but is not limited to, the procurement standards of the Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards, 2 CFR 200, referred to as the "Uniform Guidance" or new "EDGAR". All Respondents submitting proposals must complete this EDGAR Certification form regarding the Respondent's willingness and ability to comply with certain requirements, which may apply to specific agency purchases using federal grant funds.

For each of the items below, the Respondent will certify its agreement and ability to comply, where applicable, by having the Respondent's authorized representative check, initial the applicable boxes, and sign the acknowledgment at the end of this form. If a Respondent fails to complete any item of this form, AEPA will consider and may list the response, as the Respondents are unable to comply. A "No" response to any of the items below may influence the ability of a purchasing agency to purchase from the Respondent using federal funds.

1. Violation of Contract Terms and Conditions

Provisions regarding Respondent default are included in AEPA's terms and conditions. Any contract award will be subject to such terms and conditions, as well as any additional terms and conditions in any purchase order, ancillary agency contract, or construction contract agreed upon by the Respondent and the purchasing agency, which must be consistent with and protect the purchasing agency at least to the same extent as AEPA's terms and conditions. The remedies under the contract are in addition to any other remedies that may be available under law or in equity.

2. Termination for Cause of Convenience

For a participating agency purchase or contract in excess of $10,000 made using federal funds, you agree that the following term and condition shall apply:

The participating agency may terminate or cancel any purchase order under this contract at any time, with or without cause, by providing seven (7) business days in advance written notice to the Respondent. If this agreement is terminated in accordance with this paragraph, the participating agency shall only be required to pay Respondent for goods and services delivered to the participating agency prior to the termination and not otherwise returned in accordance with the Respondent's return policy. If the participating agency has paid the Respondent for goods and services provided as the date of termination, Respondent shall immediately refund such payment(s).

If an alternate provision for termination of a participating agency's purchase for cause and convenience, including how it will be affected and the basis for settlement, is in the participating agency's purchase order, ancillary agreement or construction contract agreed to by the Respondent, the participating agency's provision shall control.

3. Equal Employment Opportunity

Except as otherwise provided under 41 CFR Part 60, all participating agency purchases or contract that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 shall be deemed to include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 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."

The equal opportunity clause provided under 41 CFR 60-1.4(b) is hereby incorporated by reference. Respondent agrees that such provision applies to any participating agency purchase or contract that meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 and Respondent agrees that it shall comply with such provision.

4. Davis Bacon Act

When required by Federal program legislation, Respondent agrees that, for all participating agency contracts for the construction, alteration, or repair (including painting and decorating) of public buildings or public works, in excess of $2,000, Respondent shall comply 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, Respondent is required to pay wages

to laborers and mechanics at a rate not less than the prevailing wages specific in a wage determinate made by the Secretary of Labor. Also, Respondent shall pay wages not less than once a week.

Current prevailing wage determinations issued by the Department of Labor are available at www.wdol.gov. Respondent agrees that, for any purchase to which this requirement applies, the award of the purchase to the Respondent is conditioned upon Respondent's acceptance of wage determination.

Respondent further agrees that is shall also comply 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 construction completion, or repair of public work, to give up any part of the compensation to which he is otherwise entitled under his contract of employment, shall be defined under this titled or imprisoned not more than five (5) years, or both.

5. Contract Work Hours and Safety Standards Act

Where applicable, for all participating agency purchases in excess of $100,000 that involve the employment of mechanics or laborers, Respondent agrees to comply 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, Respondent is required to compute the wages of every mechanic and laborer based on a standard workweek of 40 hours. Work in excess of the standard workweek 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 workweek. The requirements of the 40 U.S.C. 3704 applies to construction work and provides that no laborer or mechanic must be required to work in surroundings or under working conditions that are unsanitary, hazardous, or dangerous. These requirements do not apply to the purchase of supplies, materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

6. Right to Inventions Made Under a Contract or Agreement

If the participating agency's federal award meets the definition of "funding agreement" under 37 CFR 401.2(a) and the recipient or sub-recipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance or experiments, developmental or research work under the "funding agreement," the recipient or sub-recipient 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.

7. Clean Air Act and Federal Water Pollution Control Act

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). When required, Respondent agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act and the Federal Water Pollution Control Act.

8. Debarment and Suspension

Debarment and Suspension (Executive Orders 12549 and 12689), a contract award (see 2 CFR 180.222) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR Part 1966 Comp. p. 189) and 12689 (3 CFR Part 1989 Comp. p. 235), "Debarment and Suspension." SAM exclusions contain 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. Respondent certifies that the Respondent is not currently listed and further agrees to immediately notify AEPA and all participating agencies with pending purchases or seeking to purchase from the Respondent if Respondent is later listed on the government-wide exclusions in SAM, or is debarred, suspended, or otherwise excluded by agencies or declared ineligible under state statutory or regulatory authority other than Executive Order 12549.

9. Byrd Anti-Lobbying Amendment

Byrd Anti-Lobbying Amendment (31 U.S.C. 1352), Respondents 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 take place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

10. Procurement of Recovered Materials

For participating agency purchases utilizing Federal funds, Respondent agrees to comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act where applicable and provide such information and certifications as a participating agency may require to confirm estimates and otherwise comply. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery, and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

11. Profit as a Separate Element of Price

For purchases using federal funds in excess of $150,000, a participating agency may be required to negotiate profit as a separate element of the price. See 2 CFRR 200.323(b). When required by a participating agency, Respondent agrees to provide information and negotiate with the participating agency regarding profit as a separate element of the price for a particular purchase. However, Respondent agrees that the total price, including profit, charged by the Respondent to the participating agency shall not exceed the awarded pricing, including any applicable discount, under the Respondent's contract with AEPA.

12. General Compliance with Participating Agencies

In addition to the foregoing specific requirements, Respondent agrees, in accepting any purchase order from a participating agency, it shall make a good faith effort to work with a participating agency to provide such information and to satisfy requirements as may apply to a particular purchase or purchases including, but not limited to, applicable record keeping and record retention requirements as noted in the Federal Acquisition Regulation, FAR 4.703(a).

13. Governing Law; Forum Selection.

Respondent acknowledges and agrees that any legal action or proceeding in which the Association of Educational Purchasing Agencies, Inc. ("AEPA"), is a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the Commonwealth of Kentucky, and must be brought and determined in the state courts of the Commonwealth of Kentucky in Warren County, Kentucky, or the United States Western District of Kentucky (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

Respondent further acknowledges and agrees that any legal action or proceeding in which a party includes a participating agency, but does not include AEPA as a party, that in any way relates to this solicitation, any contract award or the services provided thereunder, any other document executed in connection herewith, or for recognition and enforcement of any judgment in respect hereof brought by Respondent, a participating agency, or other party hereto, or its successors or assigns, will be governed by, construed and interpreted by the laws of the state in which the participating agency is domiciled, and must be brought and determined in the state in which the participating agency is domiciled (and may not be brought or determined in any other forum or jurisdiction), and each party hereto submits with regard to any action or proceeding for itself and in respect of its property, generally and unconditionally, to the sole and exclusive jurisdiction of the aforesaid courts and waives any further objection.

By initialing the table (1-13) and signing below, I certify that the information in this form is true, complete and accurate and I am authorized by my business to make this certification and all consents and agreements contained herein.

Respondent Certification (By Item)	Respondent Certification: YES, I agree	Initial
1. Violation of Contract Terms and Conditions	YES, I AGREE	MAC
2. Termination for Cause of Convenience	YES, I AGREE	MAC
3. Equal Employment Opportunity	YES, I AGREE	MAC
4. Davis-Bacon Act	YES, I AGREE	MAC
5. Contract Work Hours and Safety Standards Act	YES, I AGREE	MAC
6. Right to Inventions Made Under a Contract or Agreement	YES, I AGREE	MAC
7. Clean Air Act and Federal Water Pollution Control Act	YES, I AGREE	MAC
8. Debarment and Suspension	YES, I AGREE.	MAC
9. Byrd Anti-Lobbying Amendment	YES, I AGREE	MAC
10. Procurement of Recovered Materials	YES, I AGREE	MAC
11. Profit as a Separate Element of Price	YES, I AGREE	MAC
12. General Compliance with Participating Agencies	YES, I AGREE	MAC
13. Governing Law; Forum Selection.	YES, I AGREE	MAC

CAETRA.IO, INC.
Name of Business

Signature of Authorized Representative

MICHAEL A. COMPISI
Printed Name

9/16/2024
Date

Instructions: This form must be signed by the business's authorized representative and notarized below. If awarded, the Respondent is required to produce a copy of this document for each Member Agency with which it contracts.

1. The undersigned, is duly authorized to represent the persons, business and corporations joining and participating in the submission of the foregoing bid (such persons, business and corporations hereinafter being referred to as the Respondent), being duly sworn, on his/her oath, states that to the best of his/her belief and knowledge no person, business or corporation, nor any person duly representing the same joining and participating in the submission of the foregoing bid, has directly or indirectly entered into any agreement or arrangement with any other Respondents, or with any official of the **Member Agency**, or any employee thereof, or any person, business or corporation under contract with the **Member Agency** whereby the Respondent, in order to induce the acceptance of the foregoing bid by the **Member Agency**, has paid, or is to pay to any other Respondent, or to any of the aforementioned persons, anything of value whatever, and that the Respondent has not, directly nor indirectly entered into any arrangement, or agreement, with any other Respondent or Respondents which tends to or does lessen or destroy free competition in the letting of the contract sought for by the foregoing bid.

2. This is to certify that the Respondent, or any person on his/her behalf, has not agreed, connived, or colluded to produce a deceptive show of competition in the manner of the bidding, or award of the referenced contract.

3. This is to certify that neither I, nor to the best of my knowledge, information and belief, the Respondent, nor any officer, director, partner, member or associate of the Respondent, nor any of its employees directly involved in obtaining contracts with the **Member Agency**, or any subdivision of the state has been convicted of false pretenses, attempted false pretenses, or conspiracy to commit false pretenses, bribery, attempted bribery or conspiracy to bribe under the laws of any state or federal government for acts or omissions after January 1, 1985.

4. This is to certify that the Respondent or any person on his behalf has examined and understands the terms, conditions, the scope of work and specifications, and other documents of this solicitation and that any and all exceptions have been noted in writing and have been included with the bid submittal.

5. This is to certify that if awarded a contract, the Respondent will provide the equipment, commodities, and/or services to members and affiliate members of the Agency in accordance with the terms, conditions, the scope of work and specifications and other documents of this solicitation in the following pages of this bid.

6. This is to certify that the Respondent is authorized by the manufacturer(s) to sell all proposed products on a national basis.

7. This is to certify that we have completed, reviewed, approved, and have included all information that is required of these bid forms.

MICHAEL A. COMPISI
Authorized Representative (Please print or type)

99 GARNSEY RD
Mailing Address

PRESIDENT
Title (Please print or type)

PITTSFORD NY 14534
City, State, Zip

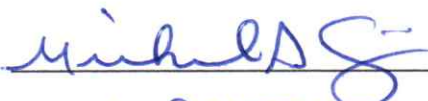*(signature)*
Signature of Authorized Representative

9/16/2024
Date

Acceptance of Solicitation & Contract

Instructions: PART I of this form is to be completed by the Respondent and signed by its Authorized Representative. PART II will be completed by the AEPA Member Agency only upon the occasion of the bid award. If approved by AEPA, the Respondent is required to produce a copy of the document for each of the AEPA Member Agency with which it contracts.

PART I: RESPONDENT

In compliance with the Published Solicitation (IFB OR RFP), the undersigned warrants that I/we have examined all Instructions to Respondents, associated documents, and being familiar with all of the conditions of the solicitation, hereby offer and agree to furnish all labor, materials, supplies, and equipment incurred in compliance with all terms, conditions, specifications, and amendments associated with this IFB OR RFP and any written exceptions to the bid. The signature also certifies understanding and compliance with the certification requirements of the AEPA Member Agency's Terms and Conditions and/or Special Terms and Conditions. The undersigned understands that their competence, ability, capacity and obligations to offer and provide the proposed tangible personal property, professional services, construction services, and other services on behalf of the Vendor Partner as well as other factors of interest to the AEPA Member Agency as stated in the evaluation section, will be a consideration in making the award.

Business Name	CAETRA.IO, INC	**Date**	9/15/2024
Address	99 GARNSEY RD	**City, State Zip**	PITTSFORD NY 14534
Contact Person	MICHAEL COMPISI	**Title**	PRESIDENT
Authorized Signature	_(signature)_	**Title**	PRESIDENT
Email	MCOMPISI@CAETRA.IO	**Phone**	585.955.4905

PART II: AWARDING MEMBER AGENCY

Your bid response for the above-identified bid is hereby accepted. As a Vendor Partner, you are now bound to offer and provide the products and services identified within this solicitation, your response, and approved by AEPA, including all terms, conditions, specifications, exceptions, and amendments. As a Vendor Partner, you are hereby not to commence any billable work or provide any products or services under this contract until an executed purchase order is received from the AEPA Member Agency or Participating Entities. This contract intends to constitute the final and complete agreement between the AEPA Member Agency and Vendor Partner, and no other agreements, oral or otherwise, regarding the subject matter of this contract, shall bind any of the parties hereto. No change or modification of this contract shall be valid unless in writing and signed by both parties to this contract. If any provision of this contract is deemed invalid or illegal by any appropriate court of law, the remainder of this contract shall not be affected thereby. The initial term of this contract shall be for up to fifteen (15) months and will commence on the date indicated below and continue until February 28, 2026 unless terminated, canceled, or extended. By mutual written agreement the contract may be extended for three (3) additional 12-month periods after this initial contract term. In the event the AEPA Board does not recommend renewal of the contract, or the contract expires, it may be extended for up to six (6) months by an AEPA state.

Awarding Agency _____

Authorized Representative _____

Awarded this	**day of**		**Contract Number**
Contract to commence (Member Agency to select)		3/1/2025	**Or**

Solicitation Checklist

Instructions: Utilize the checklist below, reviewing to confirm that all the required documents have been uploaded to Public Purchase, in their _**specified/required format**_, by the due date and time listed for this solicitation. _**Submissions not following the specified/required format may result in being marked non-responsive and may not be considered for evaluation.**_ Respondents are reminded that failure to follow, comply with, and adhere to the enclosed instructions of this solicitation may result in their response being deemed non-responsive. AEPA, its Member Agencies, affiliate agencies, and authorized representatives are not responsible for bid proposals that are incomplete, unreadable, or received after the solicitation deadline submission date.

"x"	**Document Title, Uploaded to Bonfire** *(Respondent must submit documents in the required title/format)*	**Format of Uploaded Document**	**Notes**
	Bid Bond – if Required, see Part A if applicable.	Upload PDF copy of the bid security.	The original bid security must be received by Lakes Country Service Cooperative by due date and time.
	Part C – State-Specific Forms – *Name of Responding Company*	Single, Scanned PDF	**New Jersey Only Requirement.** Signatures Required.
X	**Part D - Questionnaire – *Name of Responding Company*** Includes: ● Company Information ● Service Questionnaire ● Exceptions ● Deviations	Single, Scanned PDF	**Required.**
X	**Part E – Signature Forms – *Name of Responding Company*** Includes: ● Uniform Guidance "EDGAR" Certification ● Solicitation Affidavit ● Acceptance of Solicitation & Contract	Single, Scanned PDF	**Required.** Signatures required.
X	**Part F – Pricing Schedule – *Name of Responding Company***	Excel Workbook	**Required.**
X	**Price List and/or Catalog – *Name of Responding Company***	Upload PDF	**Required.**
X	**Exhibit A – Marketing Plan – *Name of Responding Company***	Scanned PDF	**Optional.** Form not provided by AEPA, Respondent Created