Insurance Brokerage Request for Proposal Summary

RFP Release Date: 5/11/2022
Bidder Questions Due: 5/24/2022
Answers Posted: 06/01/2022
Proposals Due: 06/15/2022

Vermont Energy Investment Corporation (VEIC) is a mission-driven, non-profit leader in the design and delivery of decarbonization programs and services for residents, businesses, and industrial customers across the United States. VEIC is seeking proposals from qualified insurance brokerage companies to provide a full range of insurance brokerage services, as described briefly below, and described in further detail in **the Scope of Work**.

- Assist VEIC in identifying and analyzing its loss exposures on an ongoing basis.
- Assist VEIC in procuring insurance policies and/or renewing existing insurance policies to meet its extensive contractual requirements.
- Provide VEIC with an insurance coverage summary annually detailing its policies, terms, carriers, premiums, deductibles, and any other pertinent information.
- Assist VEIC with routine insurance audits to ensure a successful outcome.
- Assist VEIC with filing and handling claims that may arise.
- Review minimum insurance requirements for new business and obtaining additional coverage, endorsements, or limits to meet contractual requirements.
- Provide ongoing support and counsel regarding VEIC's insurance needs and operations including producing certificates of insurance, answering insurance coverage questions, and advising on emerging risks in the market.
- Provide training and education as needed to various internal stakeholders which may include its Board of Directors, Senior Leadership Team, and program staff.
- Provide any other services customarily provided by an insurance broker.

Responses to this Request for Proposals (RFP) must be delivered electronically to VEIC by **5 p.m. EDT on Wednesday, June 15, 2022**. VEIC will not accept proposals submitted after **5 p.m.** EDT. Please submit your proposal electronically via e-mail to: **legal@veic.org** with **"RFP Proposal for Insurance Brokerage Services"** in the subject line.

VEIC will respond to individual questions regarding this RFP only as follows: VEIC will receive questions regarding requirements and scope of work up to **5 p.m. EDT Tuesday, May 24, 2022,** via e-mail only, to **legal@veic.org with "Insurance Brokerage Services Question" in the subject line.** When appropriate, please refer to the RFP page number and Section Heading for ease of

navigation and response. VEIC will post answers on the VEIC website no later than **Wednesday, June 1, 2022**. VEIC will not address questions submitted after **May 24, 2022**.

Background

Vermont Energy Investment Corporation

VEIC is a mission-driven, nonprofit organization dedicated to reducing the economic and environmental costs of energy use. It carries out its mission, in part, by design and delivery of decarbonization programs and services for residents, businesses, and industrial customers across the United States. Founded in 1986, VEIC is nationally and internationally recognized for advancing energy efficiency, energy conservation, and renewable energy programs and projects across the United States, Canada, and Europe. VEIC employs 290 professionals and is headquartered in Winooski, Vermont. It also has presence in several states, including an office in Washington, DC. For additional information, please see: VEIC Website: **www.VEIC.org**

Scope of Work, Schedule, and Contract

RFP and Implementation Schedule

Table 1. VEIC will attempt to adhere to the following schedule but reserves the right to adjust the below schedule as needed.

RFP release	May 11, 2022
Bidders Questions Due	May 24, 2022
Answers posted	June 1, 2022
Proposals due	June 15, 2022
Bidder selected	July 15, 2022
Contract negotiations and signature	August 1, 2022
Performance Period	September 15, 2022 – Sept. 15, 2025

Scope of Work

The primary goals and objectives of this RFP are to:

- Obtain the services of an insurance brokerage company licensed to act as VEIC's Broker of Record and assist VEIC with all aspects of risk transfer as further described below.
- Obtain the best mix of insurance coverages at the least possible cost for VEIC and in compliance with its risk tolerance, all applicable laws and contractual requirements, including but not necessarily limited to, VEIC's existing coverage which includes *commercial general liability, business automobile liability, workers' compensation, stop gap coverage in certain states, employer's liability, foreign liability, cyber liability, professional liability (errors & omissions), pollution liability, crime (3rd party indemnity), sexual/physical abuse and molestation, directors and officers, fiduciary liability umbrella or excess liability, and disability & paid leave where required by law, including New York.*

- Facilitate communication between VEIC and its selected insurance carriers. VEIC anticipates selecting one qualified bidder through this RFP process and entering into a professional services agreement for a three-year period, subject to annual option periods.

The Scope of Work:

- **Assisting VEIC in identifying and analyzing its loss exposures on an ongoing basis.** This work may include, but is not necessarily limited to, working closely with various stakeholders across the organization to understand VEIC's current business operations, contractual obligations, its loss history, risk tolerance, current risk management practices, advising the organization on any potential vulnerabilities and/or opportunities for improvement, and recommending any necessary changes to the terms, conditions, or coverage limits to ensure VEIC has obtained adequate and affordable coverage. VEIC expects this to include at least one annual meeting with VEIC's senior leadership team and quarterly check-ins with a member(s) of its Legal team responsible for managing the work contemplated under this RFP.
- **Assisting VEIC in procuring comprehensive insurance policies and/or renewing existing insurance policies with reputable and financially responsible insurance carriers at the least cost.** The majority of VEIC's existing policies have a September 1 – August 31st effective period. The services contemplated under this RFP will likely transition to the successful bidder once coverage for the 2022-2023 period is bound. However, in the following year (2023-2024) and annually during the Performance Period, this work will include renewing VEIC's policies, which will involve soliciting applications from insurers, completing the applications with any routine or standard information prior to delivering the applications to VEIC, working closely with VEIC to coordinate and complete the applications, reviewing the applications for completeness, obtaining clarity when needed from insurers or underwriters, negotiating coverage options and premiums on behalf of VEIC, presenting multiple quotations and advising VEIC on the insurer's coverage options, operations, claims handling and related services, binding coverage, and reviewing all policies, binders, and endorsements to assure all wording is complete and accurate before submitting to VEIC.
- **Providing VEIC with an insurance coverage summary annually** detailing its policies, terms, carriers, premiums, detailed billing schedule, deductibles, and any other pertinent information.
- **Assisting VEIC with routine insurance audits to ensure a successful outcome.** This work will include gaining a deep understanding of the business to ensure VEIC is accurately estimating exposures and helping to coordinate and schedule the audit and facilitate insurance carrier data requests as needed.
- **Assisting VEIC with filing and handling claims that may arise.** This work may include collecting information, providing guidance on which carrier(s) or policy(ies) may provide coverage, submitting claims, answering any questions that may arise during the claim process, monitoring the claims to ensure proper

handling, and monitoring VEIC's overall claims activity to ensure VEIC always has adequate coverage.

- **Reviewing proposed minimum insurance requirements for new business,** providing guidance, and obtaining additional coverage, endorsements, or limits as needed to meet contractual requirements.
- **Providing ongoing support to VEIC on issuance and management of Certificates of Insurance** including producing certificates of insurance for VEIC's certificate holders, maintaining a system including a repository and log of COIs that have been issued to external parties on behalf of VEIC, and tracking COI renewal schedules to meet contractual obligations.
- **Providing ongoing support and counsel regarding VEIC's general insurance needs and operations** including answering insurance coverage questions and advising on emerging risks in the market.
- **Providing training and education as needed** to various internal stakeholders which may include its Board of Directors, Senior Leadership Team, and program staff. This work may include on-site or remote trainings, access to e-learning tools and/or resources through your company or the insurers with whom your firm works.
- Providing any other services customarily provided by an insurance broker.

Preparing and Delivering a Proposal

For ease and efficiency of review, VEIC has specified the requirements for submitting a proposal to this RFP. Bidders must follow, and be responsive to, ALL requirements of this RFP. Proposals should be clear and concise, presented in the form of a written response with sections and sub-headings. Proposals that are not in the required format or incomplete may be disqualified at VEIC's sole discretion.

Bidders are required to propose, and will be scored upon, the individual criteria summarized in Table 2. Every bidder is required to include a Bid Summary Table based on Table 2 below with the specific value or information they propose for each of the listed criteria. The Bid Summary Table shall be presented as part of the narrative summary. (The values that the bidder provides in the Bid Summary Table are its proposed values, which will not be binding on VEIC. VEIC, in its sole discretion, will determine the final values to be awarded to each bidder.)

Table 2: Response Summary, Evaluation Criteria and Points

Scoring Category/Criteria	Description	Max Points
Company Information and Executive Summary	• Executive Summary • References • Company Data	10
Team Qualifications and Experience	• The team's knowledge, experience, and ability to successfully complete the Scope of Work. • Subject matter expertise, work experience, training, licenses and/or other credentials of key employees.	15
Scope of Work	• Approach to the Scope of Work. • Implementation plan and timeline.	25
Commercial Lines Access	• List of all the commercial lines your company has access to that coincide with VEIC's existing coverage listed above and the insurers that you maintain relationships with for each line of coverage.	15
Commission Disclosure and Broker Fees	• Full disclosure of any expected commissions to be earned by your company associated with our account, any broker fees that would be paid separately by VEIC through a professional services agreement, proposed payment terms, and an annual not-to-exceed amount for the Scope of Work. Preference will be awarded to bidders that provide the most comprehensive services at	18

	the least cost.	
Resources and Tools	• Any resources and/or tools that are provided by your company or the insurers you work with related to the Scope of Work. For example, website portal for securely transferring documents, resource databases, e-learning tools, or electronic management systems for certificates of insurance.	17
TOTAL		**100**

Proposal Requirements

A. **Company Information and Executive Summary: (**2 pages maximum) This section of the proposal must include the following:

1. **Company Info:** Name of the business, contact person, and contact information including full legal name, address, telephone, mobile telephone number, e-mail address, and website address, as applicable.
2. **Executive Summary**: a brief description of your company and its core values, the type of business entity (sole proprietorship, corporation, LLC, or other), a description of the types of organizations your company generally supports (demographics such as employee size, geographic location/dispersion, market, complexity, etc.), how your company differs from your competitors, and your company's knowledge and experience with insurance carriers.
3. **References**: Please provide at least two current client references and two former client references. For each reference, please include the name, point of contact, address, telephone number, email address, and a brief synopsis of the services rendered, length of relationship and demographics.
4. **Company Data**: If available, please provide your client retention rate over the last three years, workforce and/or supplier diversity data (e.g., gender, race, age, etc.), and any other pertinent data such as your average turnaround time for routine services such as producing certificates of insurance.

B. **Team Qualifications and Experience:** (5 pages maximum): This section of the proposal must demonstrate your team's knowledge, experience, and ability to successfully complete the Scope of Work. Please provide the names and contact information of the primary contact and the resumes for any key employees who will be assigned to our account. Describe their subject matter expertise, work experience, any relevant training(s), licenses and/or other credentials, and the role they will play with our account.

C. **Scope of Work:** This section of the proposal must include a narrative outlining your approach to the Scope of Work, implementation plan and timeline, and include proposed values or summary information for each of the scoring criteria listed in Table 2 above.

D. **Commercial Lines Access:** This section of the proposal must include a full list of all the commercial lines your company has access to that coincide with VEIC's existing coverage listed above and the insurers that you maintain relationships with for each line of coverage.

E. **Commission Disclosure and Broker Fees**: This section of the proposal should include full disclosure of any expected commissions to be earned by your company associated with our account, any broker fees that would paid separately by VEIC through a professional services agreement, proposed payment terms, and an annual not-to-exceed amount for the Scope of Work.

F. **Resources and Tools:** This section of the proposal should include any resources and/or tools that are provided by your company or the insurers you work with related to the Scope of Work. For example, website portal for securely transferring documents, resource databases, e-learning tools, or electronic management systems for certificates of insurance.

G. **Binding Transmittal Letter** (1 page maximum): Your proposal must include a binding transmittal letter signed by a party authorized to obligate the bidder to the services described in your proposal. The letter must clearly identify the person authorized to serve as the organization's representative for future communications regarding the response. The letter must state that the proposal is valid for 90 days.

H. **Certificate of Insurance.** Bidder must supply a current certificate of insurance showing evidence of Commercial General Liability, Automotive Liability and Professional Liability coverage. The successful bidder will also be required to provide a final certificate of insurance before commencement of any services. VEIC anticipates requiring the successful bidder to always maintain while providing the services the following:

Insurance Policies	Limits
Commercial General Liability	$1m per occurrence/$2m aggregate
Automotive Liability	$1m per occurrence single limit for bodily injuries and property damage
Workers' Compensation	Statutory mandates
Employer's Liability	$500k per accident; $500k per disease; $500k policy disease limit
Professional Liability Insurance (Errors & Omissions)	$1m per occurrence/$2m aggregate
Umbrella or Excess Liability Insurance	$1m per occurrence/$2m aggregate.

I. Disclosure of any pertinent litigation
   a. Bidder must disclose if any claims have been filed against their company for errors and omissions and/or if any complaints have been filed against a current or former employee for violating any rules and regulations associated with their license. If applicable, please include the number of claims and/or complaints and a general description of the nature of the claims and/or complaints. Employee-specific information should not be provided.
   b. Bidder must disclose any past or pending judgments, lawsuits, actions, bankruptcies or regulatory decisions or information that may adversely affect the bidder's ability to meet any requirements of this RFP, the professional services agreement or the bidder's proposal. Bidder agrees to provide a detailed description of any of the above events and the applicable case number in its proposal.
   c. This disclosure obligation is an on-going material obligation that applies from the date of proposal submission through the expiration of any resulting professional services award. Failure to disclose pertinent litigation may result in the disqualification of Bidder's proposal.

J. Information Security Requirements: Please review the Information Security Requirements listed in Appendix A and provide a complete Information Security Questionnaire (available for download with this RFP) with your response. Any exceptions or request to negotiate terms should be included in your proposal.

Limitation

This RFP does not commit VEIC to award a contract or to pay any costs incurred in the preparation or submission of proposals. VEIC reserves the right to reject any or all proposals received in response to this RFP, to negotiate with any qualified bidder or to cancel in part or in its entirety the RFP, if any of these actions is deemed by VEIC in its sole discretion to be in VEIC's best interest.

Appendix A - Information Security Requirements

VEIC

VENDOR INFORMATION SECURITY REQUIREMENTS

Vermont Energy Investment Corporation and its individual operating companies, divisions, subsidiaries and affiliates (collectively, "VEIC") must ensure that access to its information systems, networks, facilities and other resources (collectively, "VEIC Systems") and its data is appropriately controlled and that these resources are adequately protected. This includes access by vendors, other third parties and their respective employees, agents, subcontractors and representatives (collectively, "Vendors" and each individually, a "Vendor").

This Vendor Information Security Requirements document (this "VISR") sets forth the obligations that apply to Vendors that receive access to (i) VEIC Systems, (ii) VEIC Data (as defined below) and/or (iii) VEIC premises in connection with receipt of access to VEIC Systems and/or VEIC Data, when engaged in business with any VEIC entity (such entity, "Company"). This VISR supplements the terms and conditions set out in any agreement between Company and Vendor to which this VISR is attached or that otherwise incorporates this VISR by reference (the "Agreement"). VEIC Systems and VEIC Data are confidential information of VEIC. For purposes of this VISR, "VEIC Data" means personally identifiable information / personal information of VEIC's customers or associates, protected health information, payment card information, and any other confidential or restricted information or data of VEIC that if disclosed to the public or unauthorized parties (including competitors) is likely to cause significant harm or competitive disadvantage to VEIC (e.g., trade secrets, marketing plans, financial information, budgets, IP (internet protocol) addresses and IP ranges, strategic plans, employee compensation and performance information).

1. General Obligations

If Vendor is provided with access to VEIC Data or VEIC Systems as part of its engagement with Company, Vendor shall for the entire duration of the engagement:

b) maintain at all times a comprehensive and formally documented information security program that: (i) is based on a reputable information security standard; (ii) complies with applicable laws and regulations and; (iii) includes appropriate administrative, technical, physical, organizational and operational safeguards and other security measures designed to:

- establish minimum required standards related to the safeguarding of Vendor data and VEIC Data contained in both paper and electronic records;
- protect the security and confidentiality of Vendor data and VEIC Data in a manner consistent with applicable industry standards;

- protect against any anticipated threats or hazards to the security or integrity of Vendor data and VEIC Data; and
- protect against unauthorized processing, loss, use, disclosure or acquisition of or access to any Vendor data or VEIC Data; and upon Company's request, provide a summary or overview of this security program and/or a written confirmation that an assessment of Vendor's information security program has been conducted by an independent assessor and that any discovered program deficiencies have been remediated;

c) cooperate with security audits/assessments/testing as may be periodically requested by Company (and no more than annually unless a problem is identified) upon prior written notice to Vendor, to be performed by or on behalf of Company to confirm Vendor's compliance with this VISR; provided that such audits/assessments shall be conducted at a time(s) mutually agreed by the parties, during Vendor's normal business operations, in a manner minimally disruptive to Vendor's business, and subject to reasonable confidentiality requirements consistent with the confidentiality provisions in the Agreement);

d) ensure that Vendor personnel or representatives that receive access to VEIC Data are competent, properly trained in information security matters and understand Vendor's obligations under this VISR;

e) ensure that Vendor personnel are assigned unique authentication credentials, such as user names, passwords, digital certificates, tokens and smartcards, for access to VEIC Data, and that these credentials are handled with the utmost care and confidentiality to prevent unauthorized disclosure or misuse;

f) ensure that, unless expressly authorized in writing by Company, no VEIC Data shall be permanently stored on laptops that are not equipped with full hard drive encryption, and that no VEIC Data is stored on or accessed by USB drives, mobile devices, or any other portable storage media belonging to Vendor or Vendor personnel;

g) grant access to VEIC Data only on a need to know basis, and not distribute such VEIC Data outside the purpose of the engagement;

h) have effective and up-to-date endpoint protection in place, which includes capabilities for dynamic exploit protection, dynamic malware protection, mitigation, remediation and forensics, on all Vendor systems that are used to access VEIC Data;

i) upon termination of the engagement, upon request of Company, or at any such other time as may be required by applicable law, securely return, securely destroy or render unreadable or undecipherable all VEIC Data provided to Vendor that remains in Vendor's possession or control, and provide Company with a written certification that such return or alternate action has occurred;

j) notify Company of any unauthorized use of, disclosure of, or access to VEIC Systems or VEIC Data, or any failure to comply with this VISR, promptly and in no event more than twenty-four (24) hours after Vendor confirms such prohibited activity and shall

cooperate with Company in taking necessary or advisable corrective actions.

k) handle all Confidential Information in accordance with all applicable laws and contractual obligations. In the event that the Vendor, pursuant to applicable law or regulation or legal process, is requested or required to disclose VEIC Data, the Vendor shall provide the Company with prompt notice of such requirement in order to enable the Vendor to confer with the Company concerning the steps that may be taken to reduce the extent of VEIC Data that must be disclosed and/or to enable the Company to seek an appropriate protective order or other remedy reducing the extent of VEIC Data that must be disclosed. In any event, the Vendor shall disclose only such VEIC Data that the Vendor is advised by legal counsel is legally required to be disclosed in order to comply with such applicable law or regulation or legal process (as such may be affected by any protective order or other remedy obtained by the Company) and shall use reasonable efforts to ensure that all VEIC Data is so disclosed will be accorded confidential treatment.

Access to VEIC Systems

Compliance with this section of the VISR is required for the entire duration of the engagement if Vendor is provided access to VEIC Systems. In these situations, Vendor shall:

a) ensure that requests to grant Vendor access to VEIC Systems follow approved, formal processes and adhere to the "least privileged access principle" (i.e., access to information resources must be limited to only those individuals whose job requires such access, and access to information resources must be prevented unless explicitly allowed);

b) ensure that all remote access to VEIC Data by Vendor personnel or representatives is secured using multi factor authentication via a secure method or another authentication mechanism as agreed upon with VEIC;

c) ensure that Vendor personnel shall not attempt to gain access to any VEIC Systems that are not specifically related to fulfilling the purpose of the engagement;

d) ensure that system access provided to Vendor personnel is promptly terminated (i) upon termination of the engagement with Vendor, (ii) when Vendor personnel change functions and no longer require access, (iii) when Vendor personnel are no longer assigned to Company's account or, (iv) when for any reason, access is no longer required; and

e) accept and agree that, if and while Vendor personnel are using any VEIC Systems, system activity (e.g. system events, unauthorized log-in attempts or unauthorized transmissions of confidential information) may be subject to monitoring, to protect Company information assets, to the extent allowed by law and pursuant to all reasonable security instructions and VEIC policies or guidelines.

Access to VEIC Premises

Compliance with this section of the VISR is required for the entire duration of the engagement if Vendor is provided physical access to any non-public areas in Company's location or premises and receive access to VEIC Systems or VEIC Data. In these situations, Vendor shall and shall ensure that Vendor personnel will:

a) comply with guidance and policies provided by the Company, verbally or in writing, with regard to building safety and security, while working on site at Company's premises;
b) not attempt to gain access to any Company facilities or areas within those facilities that are not specifically related to fulfilling the purpose of the engagement;
c) treat security and identification devices (such as access badges) provided to them by Company with the utmost care and confidentiality to prevent unauthorized access;
d) ensure that Vendor personnel shall have available a valid photo ID at all times while on Company premises and shall present such identification upon request of Company personnel; and
e) refrain from interfering with VEIC's network and infrastructure or causing any damage or threat to such network and infrastructure.

Housing Services, Hosting Services and Cloud Services

Compliance with this section of the VISR is required for the entire duration of the engagement if Vendor provides facilities that host Company infrastructure (e.g., data centers), provides facilities and infrastructure for Company to manage and store its data, provides facilities and infrastructure to host supplier-provided IT solutions, or provides professional services that support the deployment and ongoing management of externally-hosted (not within Company facilities) information resources. If Vendor is providing any of these services to Company, Vendor shall:

a) comply with the SOC2 control framework and regulations, or a similar control framework with at least an equal security standard;
b) periodically provide Company (at least annually) with an unqualified SOC 2 (Type II) examination in accordance with the AICPA AT Section 101, or any successor or equivalent standards, by qualified, independent auditors engaged and compensated by Vendor, covering Vendor's controls and systems relating specifically to all aspects of the services provided ("SOC 2 Report"); and
c) provide security operational integration such as logs, monitoring and remediation, for integration with VEIC's SOC requirements.

Developing or Maintaining Software

Compliance with this section of the VISR is required for the entire duration of the engagement if Vendor develops and/or maintains software for Company as part of the engagement. In these situations, Vendor shall:

a) maintain a secure Systems Development Life Cycle (or "SDLC") process, including at a minimum:
   i. evidence of a secure code review process;
   ii. periodic application penetration test executed by a specialized third party;
   iii. a procedure that results in timely resolution of all discovered high and medium risk vulnerabilities (using the Common Vulnerability Scoring System (or "CVSS"); and
   iv. a security checkpoint in change management.

b) apply the following measures in accordance with industry best practices:
   i. patch management;
   ii. vulnerability assessment;
   iii. strong access control; and
   iv. system hardening.

c) provide to Company, upon request (in the event of an incident or no more than annually), evidence that periodic application penetration tests are performed and discovered vulnerabilities are remediated; and

d) periodically (no more than annually) provide Company with an ISO or similar certification reflecting the compliance of Vendor with the above obligations.

Maintaining Hardware

Compliance with this section of the VISR is required for the entire duration of the engagement if Vendor maintains hardware for Company as part of the engagement. In these situations, Vendor shall apply the following measures with respect to the hardware and peripherals it provides and/or maintains:

a) hardware hardening according to industry best-practices or VEIC instructions; and

b) industry standard-based security or prevention measures (anti-tampering, air gapping etc.).

Privileged Access

Compliance with this section of the VISR is required for the entire duration of the engagement if Vendor

(i) manages IT systems (hardware or software) for VEIC or (ii) is responsible for any aspect of Identity and Access Management (IAM) related to VEIC systems, including Privileged Access controls. For purposes of clarity, this Section 7 will apply only if Vendor is providing services pursuant to Sections 4, 5 or 6 above. "Privileged Access" is defined as access that provides a capability to alter the properties, behavior, or control of an information resource, change system control parameters, alter other users' access to data, or bypass or change system and security controls. In these situations, Vendor shall:

a) Maintain and disseminate to Vendor employees a written access control policy based on reputable industry standards and the least privileged access principle.
b) Include formal instructions for the following in Vendor's IAM procedures:
    i. Approval for, creation of and providing entitlements for privileged accounts;
    ii. Removal of Privileged Access upon termination of the engagement with Vendor, when Vendor personnel change functions and no longer require access, when Vendor personnel are no longer assigned to the VEIC account or, for any reason, Privileged Access is no longer required.
c) Maintain a recertification cycle (validation of permissions granted) for privileged accounts that includes:
    i. Maintaining a list of Vendor personnel with Privileged Access to VEIC Systems or other IT resources that support VEIC Systems or operations;
    ii. Reviewing Vendor personnel's access rights at regular intervals (at least quarterly) and after any changes, such as promotion, demotion, or termination of employment;
    iii. Taking immediate action to correct any discrepancies discovered during this review; and
    iv. Upon request by Company, providing reporting related to this review.
d) Monitor and adequately log creation of and changes to privileged accounts for systems used by, accessed by, or in-place to support Company and, upon discovery of anomalies, notify Company.
e) Monitor and adequately log all actions performed by Vendor personnel with Privileged Access to systems used by, accessed by or in-place to support Company, report any anomalies to Company and, upon request, provide a history of all system management actions performed by Vendor personnel that could impact the confidentiality, integrity or availability of services or systems.
f) Implement procedures for emergency access (e.g., a "break glass" account) and ensure that passwords are properly secured and changed after each use.

g) Ensure that all Vendor personnel (including technical and functional support personnel, operators, network administrators, system programmers, and database administrators) have an individually- assigned unique identifier (user ID) that can be traced to the accountable individual.

h) Implement controls to ensure secure log-on procedures, quality passwords, a secure authentication method, and session time-outs for inactive sessions at the network, operating system and database level.

i) Ensure that non-personal accounts (e.g., Admin or Root, service accounts, batch accounts, and back-up accounts) cannot be used by an individual for system access.

j) Where technically feasible, integrate solutions provided by Vendor with the VEIC privileged access management (PAM) solution.