**Please complete the requested information below. If a question is N/A based on the service(s) being provided please indicate as such.**

| Requested Information | Responses | Additional Information |
|---|---|---|
| **Company** | | |
| Name of the holding or parent company as registered with Secretary of State | | |
| Company/business name (if different from the parent company) | | |
| Public company? | | |
| State of Incorporation or Organization | | |
| Form of Organization (e.g., LLC, Nonstock Corporation) | | |
| Disclosure of all affiliated and non-affiliated entities associated with Contractor's proposed project team | | |
| Contractor's Organization: org chart up to the ultimate parent. | | |
| Name (Individually completing the questionnaire) | | |
| Job Title | | |
| Contact Information (email and phone number) | | |
| Contractor's website | | |
| Name of individuals who provided answers/evidence for the questionnaire) | | |
| Date of Response | | |
| **Breach Information** | | |
| Has your company suffered a data loss or security breach within the last 3 years? | | |
| If yes, please describe the loss or breach. | | |
| Have any of your Third Party Contractors suffered a data loss or security breach within the last 3 years? | | |
| If yes, please describe the loss or breach. | | |
| **Defining Scope** | | |
| Are the answers in this questionnaire for only one facility or geographic location? If yes, provide description of physical location (address, city, state, country). | | |
| Backup site physical address | | |
| Are there additional locations where systems (i.e. applications and database) and data are stored? | | |
| If yes, provide locations (address, city, state, country). | | |
| Are the answers to this questionnaire for only one specific type of service? If yes, describe the service. If not, please define all services provided as a separate questionnaire or questionnaires may need to be completed. | | |
| Are you providing or developing applications as part of the services provided. If yes, please list the applications. | | |
| **Data Request and Sharing** | | |
| Will you have access to UI/Eversource's non-public data? | | |
| Will you be storing or hosting UI/Eversource's non-public data? | | |
| Will you process UI/Eversource's non-public data? | | |
| Will you be disclosing UI/Eversource's non-public data? | | |

| Please answer the following questions based on your organization's Information Security Program or how it pertains to the scoped data. Please provide additional information in "Column D" if applicable | Response (Dropdown Response Yes, No, N/A) | Level of Maturity | Additional Information |
|---|---|---|---|
| **1. Risk Management** | | | |
| Does the Contractor act as a re-seller for any of the products or services UI/Eversource is requesting? | | | |
| Does the DevelContractoroper have a risk assessment program that has been approved by management, communicated and assigned ownership? | | | |
| **2. Security Program** | | | |
| Does the Contractor have a security program with established information security policies that have been approved by management, communicated and assigned ownership? | | | |
| Has the Contractor's program and policies been reviewed within the last year? | | | |
| Does the Contractor have a third party management program that has been approved by management, communicated and assigned ownership? | | | |
| **3. Organizational Security** | | | |
| Does the Contractor have an individual with assigned information security responsibilities? | | | |
| Does the DeveContractorloper have relationships with external parties that will have access to Scoped Systems and Data or processing facilities? | | | |
| **4. Asset Management** | | | |
| Does the Contractor have an asset management program that has been approved by management, communicated and assigned ownership? | | | |
| Does the Contractor have an information asset classification policy and is it implemented? | | | |
| **5. Human Resources Security** | | | |
| Does the Contractor have security roles defined and documented in alignment with the information security program? | | | |
| Does the Contractor execute background checks on the individual(s) who will have access to Scoped Systems or data? | | | |
| What is the frequency of the background checks performed on the Contractor's employees and all non-employees who have access to Scoped Systems/data? | | | |
| Does the Contractor have a security and privacy awareness training program in place? | | | |
| Does the Contractor have a disciplinarily process for non-compliance with information security policies? | | | |
| Does the Contractor have a user provisioning process for new, transfer and terminated users? | | | |
| **6. Physical and Environmental Security** | | | |
| Does the Contractor have a physical security program? | | | |
| Are reasonable physical security and environmental controls present in the building/data center that contain Scoped Systems and Data? | | | |
| Are visitors permitted in the Contractor's facility where the Scoped Systems and Data resides? | | | |
| Are outsourced facilities part of your Contractor management program? If yes, do they physically contain and/or have access to Scoped Systems or Data? | | | |
| **7. Communications and Operations Management** | | | |
| Does the Contractor have a change control or change management program and policy that has been approved by management, communicated and assigned ownership? | | | |
| Is there an antivirus/malware policy and program that has been approved by management, communicated and assigned ownership? | | | |
| Are system backups of Scoped Systems and Data performed? | | | |
| Are firewalls in use for both internal and external connections to the Scoped Systems or Data? | | | |
| Are vulnerability assessments, scans and/or penetration tests performed on internal or external networks? | | | |
| What external network connections exist (Internet, intranet, extranet, etc.)? | | | |
| Is wireless networking technology used? | | | |
| Is there a removable media policy (CDs, DVDs, tapes, disk drives) that has been approved by management, communicated and an owner to maintain and review the policy? | | | |
| Is Scoped Data sent or received electronically or via physical media? | | | |
| Is Scope Data encrypted in transit? | | | |
| **8. Access Control** | | | |
| Are electronic systems used to transmit, process or store Scoped Systems and Data and in a secure manner? | | | |
| Are unique user IDs used for accessing Scoped Systems and Data? | | | |
| Is multifactor authentication used before accessing the Scoped Systems and Data? | | | |
| Are separate IDs used for administrative tasks on Scoped Systems and Data? | | | |
| Is scoped data encrypted at rest? | | | |
| Are passwords required to access systems transmitting, processing or storing Scoped Systems and Data? | | | |
| Are IDs locked out after a certain amount of failed attempts? | | | |
| Is remote access permitted by Contractor employees and non-employees to Scoped Systems and Data? | | | |
| Does the Contractor have a process to notify when remote or onsite access should no longer be granted to Contractor representatives? | | | |
| **9. Information Systems Acquisition Development & Maintenance** | | | |
| Are business information systems used to transmit, process or store Scoped Systems and Data? | | | |
| Are there defined security engineering principles? | | | |
| Is application development performed on Scoped Systems? | | | |
| If yes, please provide any product roadmap information. | | | |
| Is there a formal Software Development Life Cycle (SDLC) process that includes security and privacy by design? | | | |
| Are code reviews performed before major application releases? | | | |
| Is static and dynamic scanning performed on applications? | | | |
| Are Scoped Systems and associated applications patched? | | | |
| Is there a formal verification of software integrity and authenticity of all software and patches provided by the Contractor for use in the BES Cyber System or associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS)? | | | |
| Is a web site supported, hosted or maintained that has access to Scoped Systems and Data? | | | |
| Are vulnerability tests (internal/external) performed on all applications at least annually? | | | |
| Does the Contractor have any known vulnerabilities to the specific product or service UI/Eversource is requesting? | | | |
| Does the Contractor have a process to disclose known vulnerabilities? | | | |
| Are encryption tools managed and maintained for Scoped Data? | | | |
| **10. Incident Event and Communications Management** | | | |
| Does the Contractor have an Incident Management program? | | | |
| Have there been any identified incidents related to the specific products or services UI/Eversource is requesting? | | | |
| Does the Contractor have a process to notify of Contractor-identified incidents related to the products or services provided that pose cyber security risk? | | | |
| Does the Contractor have a process to Coordinate responses to Contractor-identified incidents related to the products or services provided that pose cyber security risk? | | | |
| Is logging enabled on all Scoped Systems? | | | |
| Does logging data get sent to a Security Information and Event Management (SIEM) tool? | | | |
| **11. Business Continuity and Disaster Recovery** | | | |
| Is there a documented policy for business continuity and disaster recovery that has been approved by management, communicated and an owner to maintain and review the policy? | | | |
| Is there an annual schedule of required tests? | | | |
| Are BC/DR tests conducted at least annually? | | | |
| Is a Business Impact Analysis conducted at least annually? | | | |
| Is there insurance coverage for business interruptions or general services interruption? | | | |
| **12. Compliance** | | | |
| Is there an internal audit, risk management or compliance department with responsibility for identifying and tracking resolution of outstanding regulatory issues? | | | |
| Is there an internal compliance and ethics reporting mechanism and training program for employees to report compliance issues? | | | |
| **13. Mobile** | | | |
| Are mobile devices used to access Scoped Systems and Data? | | | |
| **14. Privacy** | | | |
| Is Scoped Data transmitted, processed, or stored that can be classified as non-public information (NPI), personally identifiable information (PII), or sensitive customer financial information? If yes, describe and list types of data | | | |
| Is Scoped Data transmitted, processed, or stored that can be classified as protected health information, electronic health records, or personal health records? If yes, identify the classifications. | | | |
| For Scoped Data, is personal information about individuals transmitted to or received from countries outside the United States? If yes, identify the countries | | | |
| For Scoped Data is there a dedicated person (or group) responsible for privacy compliance. If yes, describe. If no, explain reason | | | |
| For Scoped Data, is there a documented privacy policy or procedures to protect confidential information? | | | |
| For Scoped Data are there regular privacy risk assessments conducted? If yes, provide frequency and scope. If no, explain reason. | | | |
| Is there formal privacy awareness training for employees, contractors, and third-party users to ensure confidentiality and privacy of Scoped Data? | | | |
| Is there a formal process for reporting and responding to privacy complaints or privacy incidents for Scoped Data? If yes, describe. If no, explain reason. | | | |
| Is there a data classification and retention program for Scoped Data that identifies the data types that require additional management and governance? | | | |
| Is there a documented response program to address privacy incidents, unauthorized disclosure, unauthorized access or breach of Scoped Data? | | | |
| Is Scoped Data disclosed to third parties? If yes, describe | | | |
| Is Scoped Data disclosed to third parties outside of the U.S.? If yes, describe. | | | |
| Is there a formal coordination of controls for (i) Contractor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a Contractor(s)? | | | |
| Are there contractual controls to ensure that Scoped Data shared with third parties is limited to defined parameters for access, use and disclosure? If yes, describe the controls. If no, explain reason. | | | |
| Is there a business associate contract or applicable contractual language in place to address obligations for the privacy and security requirements of the services provided? | | | |
| Is there a documented privacy program with administrative, technical, and physical safeguards for the protection of Scoped Systems and Data? | | | |
| Is there a process for ensuring the accuracy of Scoped Data at the direction of the client? If yes, describe. If no, explain reason. | | | |
| With regard to the scoped data; is there a process to ensure that the personal information provided by an individual is limited for the purposes described in the respondent's privacy notice? If yes, describe. If no, explain reason. | | | |
| Are constituents regularly monitored for privacy compliance? If yes, describe. If no, explain reason. | | | |
| Are there documented policies, procedures, and controls to limit access based on need to know or minimum necessary for constituents? If yes, describe. | | | |
| Are enforcement mechanisms applied to constituents who violate privacy policies or confidentiality requirements? | | | |
| Are transactions for covered accounts accessed, modified, or processed, including address changes and discrepancies? If yes, describe. | | | |
| Is customer data accessed, transmitted, processed, or stored that can be classified as consumer report information provided by a consumer reporting agency? | | | |
| **15. Cloud (Is the Contractor providing, managing and/or maintaining a cloud solution?)** | | | |
| Are Cloud Services provided? If yes, what service model and deployment model is provided (select all that apply): | | | |
| Software as a Service (SaaS) | | | |
| Platform as a Service (PaaS) | | | |
| Infrastructure as a Service (IaaS) | | | |
| Private cloud | | | |
| Public cloud | | | |
| Community cloud | | | |
| Hybrid cloud | | | |
| Does Scoped Data stay within North America? | | | |

| Based on the services the 'Contractor' is performing or providing and the review of the responses within the first two tabs, the 'Contractor" will be asked to provide the following documentation with a "X" in the "Column B" | UI/Eversource Requested Document(s) |
|---|---|
| * Information Security Policies and Procedures. This should include the following (if not, provide the individual documents as necessary):<br>a) Hiring policies and practices and employment application<br>b) User Account administration policy and procedures for all supported platforms where Scoped Systems and Data are processed and network/LAN access.<br>c) Supporting documentation to indicate completion of User Entitlement reviews<br>d) Employee Non-disclosure agreement document<br>e) Information Security Incident Report policy and procedures, including all contract information<br>f) Copy of Visitor Policy and procedures<br>g) Security Log Review Policies and Procedures<br>h) Copy of third party risk management policies and procedures<br>i) Criteria/requirements when performing background checks | |
| * Copy of internal or external information security audit report/SOC2 | |
| Information technology and security organization charts (including where Respondent information security resides and the composition of any information security steering committees).<br>**Note:** Actual names of employees are not required | |
| * Physical Security policy and procedures (building and/or restricted access) | |
| * Third-party security reviews/assessments/penetration tests | |
| Legal clauses and confidentiality templates for third parties | |
| Topics covered in the security training program | |
| * Security incident handling and reporting process | |
| Network configuration diagrams for internal and external networks defined in scope.<br>**Note:** Sanitized versions of the network diagram are acceptable | |
| * System and network configuration standards | |
| * System backup policy and procedures | |
| * Offsite storage policy and procedures | |
| * Vulnerability and threat management scan policy and procedures | |
| * Application security policy | |
| * Change control policy/procedures | |
| * Access control policy/procedures | |
| * Problem management policy/procedures | |
| * Certification of proprietary encryption algorithms | |
| * Internal vulnerability assessments of systems, applications, and networks | |
| * Software development and lifecycle (SDLC) process document | |
| * Business continuity plan (BCP) and / or Disaster recovery plan | |
| * Most recent BCP/DR test dates and results | |
| * Most recent SSAE16/18/SOC2 or SOC3 audit report | |
| * Privacy policies and notices (internal, external, web); including but not limited to privacy by design, data processing agreements, data retention and privacy frameworks. | |
| * Executive Summary of certificates held. (e.g. PCI, HIPAA, ISO) | |
| * Performance Reports against contracted SLAs | |
| **Policies and Procedures.** This should include the following (if not, provide the individual documents as necessary): | |
| * Documentation of process by which the Responsible Entity will address supply chain cyber security risk management for high and medium impact BES Cyber Systems. | |
| * Documentation of the Development and Implementation of a Response Plan including: | |
| '* Documentation of Prevention of Recurrence | |
| '* Coordination of Incident Response with Company | |
| '* Notification to Affected Parties | |
| '* Unrelated Security Incidents | |
| * Access control policy/procedures including: | |
| '* Development and Implementation of Access Control Policy | |
| '*Company Authority Over Access | |
| '* Contractor Review of Access | |
| '* Notification and Revocation | |
| '* Controls for Remote Access | |
| * Disclosure by Contractors of known vulnerabilities | |
| * Verification of software integrity and authenticity of all software and patches provided by the Contractor for use in the BES Cyber System including: | |
| '*Hardware, Firmware, Software, and Patch Integrity and Authenticity | |
| '*Patching Governance | |
| '* Viruses, Firmware and Malware | |
| '* End of Life Operating Systems | |
| '* Cryptographic Requirements | |
| * Documentation of Cybersecurity Policy including: | |
| '*Return or Destruction of Company Information | |
| '*Audit Rights | |
| '* Viruses, Firmware and Malware | |
| '* End of Life Operating Systems | |
| '* Regulatory Examinations | |

| Categories of Review | UI/Eversource Analysis and Associated Risk(s) |
|---|---|
| Contractor Information | |
| Contractor Questionnaire | |
| Documentation Requests | |