DDQ Question Number	Question
DDQ-A.01	What is your organization's name?
DDQ-A.02	Who is your point of business contact from Eversource?
DDQ-A.03	What is the type of solution and/or service your organization is providing to Eversource?
DDQ-A.04	Will your organization be providing cloud hosting (IaaS)?
DDQ-A.05	Will your organization operate or host Eversource applications?
DDQ-A.06	Will your organization install or service Eversource applications or systems?
DDQ-A.07	Will your organization require access to Eversource employee or customer Personally Identifiable Information (PII) data?
DDQ-A.08	Will your organization require physical access to secured Eversource computer facilities?
DDQ-A.09	Will your organization transmit files to or from Eversource?
DDQ-A.10	Does your organization utilize a third-party for infrastructure (or other) hosting related to delivery of your product or service? Please identify hosting provider (e.g. AWS, GCP, or Microsoft Azure)
DDQ-A.11	Please list all third parties, where they are located, and the type of hosting solution (e.g., SaaS) they provide.
DDQ-A.12	Eversource requires that its data must be stored and processed only within the United States. If your organization cannot comply with this requirement, please detail where your company would store and process Eversource data.
DDQ-A.13	If remote access to Eversource is required, please confirm that you will comply with Eversource security policies and settings for remote access. (CIP-013 R1.2.6)
DDQ-A.14	The Department of Homeland Security (DHS) now has a program for software and hardware manufacturers to voluntarily agree to following the “Secure by Design” guidance. Has your company signed on to this practice?
DDQ-B.01	Is your organization certified in an industry accepted control standard (e.g. SOC 2 Type 2, ISO 9000, PCI)?
DDQ-B.02	Would your organization allow/consider a third-party assessment/attestation of your controls?
DDQ-B.03	Does your organization have processes and procedures for monitoring compliance against your internal security policies and/or external regulatory security requirements (e.g. NERC, SOX, PCI, etc.)?
DDQ-B.04	Does your organization have a written Information Security policy, sponsored and approved by senior management, published and available to all employees?
DDQ-B.04-Attachment	If yes, please provide.
DDQ-B.05	Is your organization's Information Security policy and program modeled after an industry framework (e.g. ISO, COBIT, NIST, etc.)?
DDQ-B.06	Is your organization's Information Security Policy reviewed and updated periodically?
DDQ-B.07	Does your organization's Information Security policy include a formal process to address changes in privacy laws/regulations and regulatory guidance?
DDQ-B.08	Are existing employees required to periodically sign-off on your organization's Information Security policy?
DDQ-B.09	Are your employees notified, and required to acknowledge, when changes or updates are made to the Information Security policy and/or procedures?
DDQ-B.10	Are new employees required to sign-off that they understand and agree to your organization's policies, including the Information Security policy?
DDQ-B.11	Does your organization's Information Security policy include an "acceptable use" policy that must be signed by all employees?
DDQ-B.11-Attachment	If yes, please provide.
DDQ-C.01	Does your organization's conduct background checks (e.g. credit, criminal, drug, employment checks, etc.) for all employees?

DDQ Question Number	Question
DDQ-C.02	Does your organization's have a formal Information Security Awareness program developed and implemented for all employees?
DDQ-C.03	Does your organization's employees receive Information Security awareness training at regular intervals?
DDQ-C.04	Are employees asked to sign a confidentiality or non-disclosure agreement as part of their terms and conditions of employment?
DDQ-C.05	Are employees asked to sign a confidentiality or non-disclosure agreement as part of their terms and conditions of leaving the company?
DDQ-C.06	Are contractors and part-time/temporary employees bound by your organization's Information Security policy, and confidentiality and/or non-disclosure agreements?
DDQ-C.07	Does your organization utilize (or plan to utilize) offshore resources as part of your overall delivery strategy?
DDQ-D.01	Does your organization have written policies/procedures/guidelines for maintaining and monitoring the security of customer data?
DDQ-D.01-Attachment	If yes, please provide.
DDQ-D.02	Does your organization employ encryption technologies or other controls to protect client data while stored on your information systems?
DDQ-D.03	Does your organization employ hard disk encryption technologies (e.g. whole disk, file level, etc.) on your desktops and laptops?
DDQ-D.04	Will Eversource data be co-mingled with data from other clients?
DDQ-D.05	Does your organization data masking capabilities at the database level to obscure/replace sensitive data elements?
DDQ-D.06	Does your organization employ encryption controls for client data that contains Personally Identifiable Information (PII)?
DDQ-D.07	Does your organization employ additional security controls for access to client data that contains Personally Identifiable Information (PII)?
DDQ-D.08	What secure data transfer does your organization support?
DDQ-D.09	Does your organization store backup media at an on-site location that is separate from your computing facilities?
DDQ-D.10	Does your organization take measures to ensure that backup media containing client data is protected from unauthorized access and misuse?
DDQ-D.11	Does your organization send backup media off-site for archiving?
DDQ-D.12	Does your organization periodically test backup media to ensure data completeness and consistency, and to ensure that data can be restored within a defined timeframe?
DDQ-D.13	Will Eversource data be stored for longer than the contract period?
DDQ-D.14	Does your organization have policies and procedures in regards to the disposal of customer information?
DDQ-D.14-Attachment	If yes, please provide
DDQ-E.01	What does your application perform for data validation for inbound data to identify common attacks (e.g. SQL Injection, XSS)?
DDQ-E.02	Does your application perform data validation/filtering for outbound data to ensure that sensitive information (e.g. username or password) is not presented back to the end-user following data validation errors?
DDQ-E.03	Does your application perform both client-side and server-side data validation?
DDQ-E.04	Does your application employ encryption technologies to protect customer data during transit?
DDQ-E.05	Does your application support role-based access models for user access, with specific permissions assigned to each role?
DDQ-E.06	Does your application implement password enforcement policies, such as minimum length, complexity, expiration, reuse restrictions (within a predefined period of time)?

DDQ Question Number	Question
DDQ-E.07	After how many failed authentication attempts is a user locked out?
DDQ-E.08	What utility is used in your application to integrate with LDAP (e.g. Active Directory) or other directory service for authentication and/or authorization?
DDQ-E.09	Does your application have the ability to integrate with federated single sign-on solutions/protocols (i.e. OKTA? using SAML)?
DDQ-E.10	Does your organization have a formal Software Development Lifecycle (SDLC) program or methodology?
DDQ-E.11	Does your application enforce a session time-out and/or lockout that would be triggered after a pre-defined amount of user inactivity?
DDQ-E.12	Does your application implement user login/session functionality?
DDQ-E.13	Does your application provide an audit trail linking users to specific data transactions?
DDQ-E.14	What anti-virus protection tools are utilized on the servers on which your applications run?
DDQ-E.15	Describe (including time parameteres) your organizations process for communicating application or product vulnerability information to Eversource? Will you allow Eversource to notify E-ISAC and other utilities of vulnerabilities identified by Eversource after notifying your company? (CIP-013 R1.2.4)
DDQ-E.16	Please provide documentation regarding your process for ensuring integrity and authenticaticity of the software's supply chain.
DDQ-E.17	Provide your organization's product support contact information (phone, email) and provide support hours.
DDQ-E.18	Describe your organization's Problem Reporting process. What's the response and resolution time for critical / high severity issues?
DDQ-F.01	What product does your organization utilize for antivirus software on all employee desktops, laptops, and servers that are running the Windows operating system?
DDQ-F.02	How often does your organization update the antivirus signatures?
DDQ-F.03	Does your organization's antivirus software run full system scans on a periodic basis?
DDQ-F.04	Does your organization's antivirus software include spyware detection and protection?
DDQ-F.05	Does your organization restrict administrative access to desktops and laptops?
DDQ-F.06	Does your organization leverage Data-Loss Prevention (DLP) or Host-Based Intrusion Detection/Prevention (HIDS/HIPS) solutions?
DDQ-F.07	Does your organization have documented standard security configurations (i.e. hardening standards) for each system type? For all your critical infrastructure, are you following CIS standards
DDQ-F.08	Are your organization's systems configured to capture and log successful and failed user authentication (login) attempts and user authorization failures?
DDQ-F.09	How long does your organization retain system log files to assist in access control monitoring and security investigations?
DDQ-F.10	Does your organization enforce strict change management controls (including appropriate review, approval, and testing) for changes to production applications and servers?
DDQ-F.11	Does your organization have a formal Asset Management policy?
DDQ-F.11-Attachment	If so, please provide detail or attach policy.
DDQ-F.12	Does your organization have a formal Configuration Management program that covers the development and maintenance of standard server/device configurations (e.g. hardening standards)?
DDQ-F.12-Attachment	If so, please provide.
DDQ-F.13	Does your organization maintain separate test and development environments and facilities that are isolated from production ?
DDQ-G.01	Describe your organizations employment of firewalls (types used, as well as how they are deployed and managed) to protect the systems that may/will support Eversource data? .
DDQ-G.02	What network-based IDS/IPS tools does your organization employ to monitor traffic for malicious content?

DDQ Question Number	Question
DDQ-G.03	Does your organization utilize network segmentation (physical or logical) on a client-by-client basis?
DDQ-G.04	What utlilities does your organization use to protect all email traffic originating from untrusted networks for viruses and other malware?
DDQ-G.05	Does your organization's systems provide protection/encryption for sensitive data (e.g. login credentials, sensitive personal information) during network transit?
DDQ-G.06	What utilities does your organization employ for encryption technologies or other controls to safeguard confidentiality and integrity of client data being accessed over public networks (e.g. the internet)?
DDQ-G.07	What does your organization support for email encryption (SMTP/TLS or other)?
DDQ-G.08	How does your organization monitor for unauthorized network connection points such as wireless access points, modems, etc.?
DDQ-G.09	Will your organization require access to the Eversource network environment?
DDQ-G.10	Does your organization employ wireless networks within your data processing facilities?
DDQ-G.11	Does your organization enforce host integrity checks that only allow endpoint devices that have adequate security controls (e.g. antivirus, up-to-date OS patches, etc.) to connect to your network?
DDQ-H.01	Is there an Internet-accessible self-service portal available that allows clients to configure security settings and view access logs, security events and alerts?
DDQ-H.02	Are cloud hosting services subcontracted?
DDQ-I.01	Does your organization have a formal and documented process for employee and customer account management that includes provisioning, password requirements, access controls, and deprovisioning?
DDQ-I.02	Does your organization change default system account names and passwords across all systems?
DDQ-I.03	Does your organization provide your personnel with guidelines for selecting and maintaining secure passwords requiring the use of a combination of upper-case letters, lower-case letters, numbers, and non-alphanumeric symbols? Password length requirement? Minimum password length requirement?
DDQ-I.04	Do your organization's systems enforce a maximum password age, password strength requirements , the use of a combination of upper-case letters, lower-case letters, numbers, and non-alphanumeric symbols as well as the use of the account or user ID as part of the password?
DDQ-I.05	Do your organization's systems have a password history functionality enabled such that passwords cannot be reused within a predefined period of time?
DDQ-I.06	Do your organization's systems have a process to ensure that access privileges are immediately revoked for employees leaving the company or moving to a new job role ? Does this process include notification to Eversource when on-site or remote computer access to Eversource is no longer required? Please describe and provide the acceptable time for revocation as well as notification to Eversource. (CIP-013 R1.2.3)
DDQ-I.07	Does your organization ensure that all users have a unique user ID, and that user accounts are not shared among multiple people (with the exception of privileged administrative accounts)?
DDQ-I.08	Where shared user accounts are used (e.g. administrator account), does your organization employ compensating controls to maintain user accountability?
DDQ-I.09	Do your organization's systems enforce user account lock-out after a specified number of incorrect authentication attempts?
DDQ-I.10	How do your organization's systems provide protection (encryption/hashing) for stored passwords?
DDQ-I.11	Does your organization use any system scripts that may have user or system passwords hard coded in them?

DDQ Question Number	Question
DDQ-I.12	Do your organization's systems (e.g. servers, employee workstations, etc.) enforce a session time-out and/or lockout that would be triggered after a pre-defined amount of user inactivity?
DDQ-I.13	Do your organization's systems (e.g. Servers, Databases, etc.) support role-based access models for user access, with specific permissions assigned to each role?
DDQ-I.14	Do your organization's access control mechanisms block access by default and provide access using a least-privileges methodology?
DDQ-I.15	Does your organization review access rights on a periodic basis for both internal employees and clients? How often are these reviews completed (Monthly, Bi-Monthly, Quarterly)?
DDQ-I.15-Date Picker	When was the last review completed?
DDQ-I.16	Does your organization utilize Two-Factor Authentication controls for employees accessing your internal network from remote locations?
DDQ-I.17	Please describe how your organization's administrators access the systems that will/may support Eversource. Is server access allowed only from within your organization's internal network, or do you allow access from remote locations? If remote access is allowed, please describe.
DDQ-I.18	Does your organization implement segregation-of-duties controls to reduce opportunities for unauthorized modification or misuse of information or services?
DDQ-I.19	Does your organization employ physical security controls (e.g. card-controlled entry doors, security guards, etc.) to protect your data processing facilities?
DDQ-J.01	Are privacy awareness training obligations extended to your organization's vendors (e.g., subcontractors)?
DDQ-J.02	Does the process to respond to an individual's access request include the personal information that has been shared with vendors, subcontractors, and/or service providers?
DDQ-J.03	Do your organization's vendors, (e.g., subcontractors, sub-processors, sub-service organizations) have access to, receive, or process client scoped data?
DDQ-J.04	Has client consent been obtained for any usage of fourth-parties, subcontractors, sub-processors or sub-service organizations?
DDQ-J.05	Is a contract maintained with such parties to require each to adhere to the same legal and contractual requirements that are required by your organization?
DDQ-J.06	Does your organization have documented policies, procedures or mechanisms to provide notice, and if required obtain consent for any new, or changed usage of vendors, subcontractors, sub-processors, or sub-service organizations?
DDQ-J.07	If there is a vendor involved in the delivery of your organization's application or service, does your contract with that party include requirements for privacy, security, service level agreements, and non-disclosure agreements?
DDQ-J.08	If there is a vendor involved in the delivery of your organization's application or service, does your agreement with that party include provisions for performing a risk assessment or audit to ensure they have appropriate security controls in place?
DDQ-J.08-Attachment	Please provide a copy of your organization's policy
DDQ-J.09	Are vendors required to notify your organization of any exceptions to policies, procedures or compliance matters that might require escalation to Eversource legal and/or compliance?
DDQ-K.01	Does your organization have a formal and documented Incident Response plan for handling security incidents that addresses incident management responsibilities, evidence preservation, chain-of-custody procedures and coordination with Eversource? Does the plan include notification to Eversource ? (CIP-013 R1.2.1, R1.2.2).
DDQ-K.02	Does your organization perform monthly vulnerability scanning against both internal and client-related systems?
DDQ-K.03	Does your organization have a formal process for identifying threats and vulnerabilities (either through early detection alerts, vulnerability scans, etc.) and tracking remediation?

DDQ Question Number	Question
DDQ-K.04	Does your organization perform periodic penetration tests against your Internet-facing network performed by a third party?
DDQ-K.04-Attachment	If yes, please provide the executive summary of the most recent penetration test.
DDQ-K.05	Does your organization have auditing/logging enabled for all systems?
DDQ-K.06	Are your organization's systems configured to capture and log activity performed by system administrators or users with elevated privileges?
DDQ-K.07	Do audited events include data attributes for date and time of the event, type of event, username/user ID associated with the event, hostname or IP address of the system affected, key details about the event?
DDQ-K.08	Are your organization's servers configured to synchronize their time/clocks to a common source?
DDQ-K.09	Does your organization have processes and procedures for reviewing security events (e.g. audit log reviews)?
DDQ-K.10	Does your organization have a Security Information and Event Management (SIEM) technology in place for storing security logs long-term, monitoring and correlating security events, and alerting on specific events?
DDQ-K.11	Would your organization support activities by Eversource to conduct intrusion testing or audits against those systems that house or process Eversource data at your site?
DDQ-K.12	Does your organization have documented processes for patch management to ensure that security-related patches (e.g. desktops, laptops, server OS, Database, Application, etc.) are addressed within a reasonable timeframe? Please describe.
DDQ-K.13	Does your organization's business continuity plan include appropriate risk management and business impact analysis activities to identify recovery priorities?
DDQ-K.14	Does your organization conduct regular testing and review of your business continuity plans to ensure their continuing effectiveness?
DDQ-L.01	Are there formal, documented disaster recovery procedures and business continuity programs that are sponsored and approved by senior management on a periodic basis?
DDQ-L.01-Attachment	If so, please provide.
DDQ-L.02	Is your organization's disaster recovery location more than 100 miles from the production data center?
DDQ-L.03	Does your organization's formal disaster recovery procedures include specific actions to be taken in response to a data center disruptive event for each data center (internal and external) supporting the products and/or services specified in the scope of this assessment?
DDQ-L.04	Do your organization's formal disaster recovery procedures address the recovery of critical networks and systems?
DDQ-L.05	Does the recovery of critical networks and systems include backup types (e.g., physical, and/or virtual)?
DDQ-L.06	Does the recovery of critical networks and systems include backup levels (full, incremental, or differential)?
DDQ-L.07	Does the recovery of critical networks and systems include update and retention cycle frequencies?
DDQ-L.08	Does the recovery of critical networks and systems include software and hardware compatibility reviews?
DDQ-L.09	Does the recovery of critical networks and systems include data transmission protocols?
DDQ-L.10	Does the recovery of critical networks and systems include data repository maintenance?
DDQ-L.11	Are procedures defined for restoring backlogged activity or lost transactions to identify how transaction records will be brought current within expected recovery time frames?
DDQ-L.12	How often to you perform DR tests? Are the DR tests full/incremental, tabletop, or live?
DDQ-L.13	Does your company have Cyber Insurance?

DDQ Question Number	Question
DDQ-M.01	Will our data be shared or used within the platform in any way with a generative AI platform/tool?
DDQ-M.02	Is AI a third party tool or developed in-house?
DDQ-M.03	What individuals and companies have access to prompts submitted to the tool? Does the AI feature rely on a third party, a model provider, or a local model?
DDQ-M.04	Does the AI tool consume or in any way use external input? What would happen if prompt injection payloads were inserted into them? What impact could that have?
DDQ-M.05	Can the tool take consequential actions, such as changes to files, users, or other objects?
DDQ-M.06	Does the AI tool have any features with the potential for traditional vulnerabilities to occur (such as SSRF, IDOR, and XSS mentioned above)? For example, is the prompt or output rendered where XSS might be possible? Does web fetching functionality allow hitting internal hosts or cloud metadata IP?
DDQ-N.01	Are you operating or manufacturing in any countires of interest (Russia, China, North Korea, and Iran)?
DDQ-N.02	Does the company have any foreign ownership?