

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

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?				

Propose of the beginning and control based on your organization's bidemention browly. **Propose of the beginning of the begi				
The time of the control of the contr	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	(Dropdown Response Yes,		
See the Conference on the sea of an extraction region for the last that payment is required for a second se	1. Risk Management	No, N/A)	Level of Maturity	Additional Information
And the Common and th	Does the DevelContractoroper have a risk assessment program that has been approved by management, communicated and			
The second country of performance and performance for companies of the com	2 Security Program			
A Comment of the Comm	management, communicated and assigned ownership? Has the Contractor's program and policies been reviewed within the last year? Does the Contractor by us, a third park, management program that have been approved by management, communicated and			
See the Company has an extended of management amounts are extended in the company of the company	assigned ownership? 3. Organizational Security			
The first of controls of the control	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			
Section of Company and Association of the Company of Co	4. Asset Management			
Some the Company of the control of t	assigned ownership?			
Some to Compare American Services and Compare American Services and American Services an	Does the Contractor have security roles defined and documented in alignment with the information security program?			
Such to Common the an extensional recommend control process. The Authority State Common State Co	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?			
Control Contro	Does the Contractor have a disciplinarily process for non-compliance with information security policies?			
An experiment of the Company of Company of Company of System, the Player of Company of System is the Company of System of System of Company of System is the Company of System o	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?			
Subcrete Services of Services The ten Contractive Services of Ser	and Data?			
See the Contraction to an animal for contraction and contraction of the contraction of th	Are visitors permitted in the Contractor's facility where the Scooed Systems and Data resides? Are outsourced facilities part of your Contractor management program? If yes, do they physically contain and/or have access 15 Contract Outstand Delta Contractor Contractor management program? If yes, do they physically contain and/or have access			
Sections of Communication and Section Communication Commun	7. Communications and Operations Management Does the Contractor have a change control or change management program and policy that has been approved by			
As comment in selection of finance flowers and other continued. As electrical content of the comment of the co	management, communicated and assigned ownership? Is there an antivirus/malware policy and program that has been approved by management, communicated and assigned			
An exhaust antendencia more process of the process	ownership? Are system backups of Scoped Systems and Data performed?			
Survivous controllors benchedous years. 3. Solone Data series or manufact of communication of the base term proposed by manufactured and a series of the base term proposed by manufactured and the base of the b	Are vulnerability assessments, scans and/or penetration tests performed on internal or external networks? What external network connections exist (Internet, intranet, extranet, etc.)?			
Solve Description and Property in Equipment (1997) And description contents of the content, across by the property of the sent of the sen	Is wireless networking technology used? Is there a removable media policy (CDs, DVDs, tapes, disk drives) that has been approved by management, communicated			
A Access Control of the Treatment and Control of the Security Control of the S	and an owner to maintain and review the policy? Is Scoped Data sent or received electronically or via physical media?			
The management of the section of the common of found from any of facility of the common of the commo	8. Access Control Are electronic systems used to transmit, process or store Scoped Systems and Data and in a secure manner?	_		
Successful an exceptional of many common transmission, accordance in studies (Control of the Control of the Con	Is multifactor authentication used before accessing the Scoped Systems and Data?			
An Chit cold of an after a contain, minored of finded amongs? The control of Complete Programs is record by minored to cold on any of the programs of Chant's control of the Complete Programs of Cha	is scoped data encrypted at rest?			
Close to Economic hand a pociose to residy when remain or order access should be beginned. Maintenance An electronic Street and the Street St	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?			
As between schematic systems, and on because, services a retrie flored forgetters and fellow and applications of the state	Does the Contractor have a process to notify when remote or onsite access should no longer be granted to Contractor representatives?			
As accordance in continuents conformed and Society (SECE) in consess that includes security and created by the continuents of t	Are business information systems used to transmit, process or store Scoped Systems and Data?			
Man code in section and control and decision in a constraint of the control and code in a constraint of the code in a code in	Is application development performed on Scoped Systems? If yes, please provide any product roadmap information.			
And Second Sections and association accolations contributed by the Contractor for using the BES Cycle of Section or associated Rectinating Systems (EACMS) Propriet Access Coreal Sections (ACM). The BES Cycle of Section of the BES Cycle of Section of the BES Cycle of Section (ACM). And the BES Cycle of Section of the BES Cycle of Section of the BES Cycle of Section (ACM). And subscription the section of the BES Cycle of Section (ACM). And subscription the section of the BES Cycle of Section (ACM). And subscription the BES Cycle of Section (ACM). And subscription the BES Cycle of Section (ACM). And subscription (ACM). And subscripti	Are code reviews performed before major application releases?			
in the 185 Cycler System or associated Electronic Access Control of Microbiolog Systems and Data? An uniform state of the Control of Microbiolog Systems and Data? An uniform state of the Control of Microbiolog Systems and Data? An uniform state of the Control of Microbiolog Systems and Data? An uniform state of the Control of Microbiolog Systems and Data? An uniform state of the Control of Microbiolog Systems and Data? An uniform state of the Control of Microbiolog Systems and Data? An uniform state of Systems and Systems and Data? An uniform state of Systems and Systems and Data? An uniform state of Systems and Systems and Data Systems and Data Systems and Data Systems and Systems an	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			
An outbroadpility tests internal internal conformed on all analysis in the second process to Cornicion and Vision of American (Control Date) Ass excended to the management of the Control Date of the Contro	in the BES Cyber System or associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS)?			
Obes the Contraction have a process to disclose from unbranched files? In the Contraction have an incident Measurement success? In the Contraction have a process to Contraction Measurement success to the products or extension products or a success for the contraction of the success of the contraction of the success	Are vulnerability tests (internal/external) performed on all applications at least annually?			
Contractor has the Contractor has a Street for Section of Contractor has a process to relate to the products or a process to relate to the products of the products or a process to relate to the products of the products of the process to relate to the products of th	Does the Contractor have a process to disclose known vulnerabilities?			
Some motive accounts male. In common words accounts and account and account accounts and account accounts account and account accounts account and account accounts account account account and account accounts account acco	10. Incident Event and Communications Management Does the Contractor have an incident Management program?			
Does the Contractor have a process to Countries requires to Contractor-Sential contractor-Sential Contractors (Contractors) Designations of the contractors (Contractors) Designations (Contractors	Have there been any identified incidents related to the specific products or services LWEversource is requesting? Does the Contractor have a process to notify of Contractor-identified incidents related to the products or services provided that			
Obes location data not earl to a Scientify Information and West Memoratement (SEM bod?) In these a documentary policy for business certainly and disaster recovery that has been approved by management, communicated and an owner to maintain and reviews the action? In the an annual Activity of the Communication of the Commu	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 there is documented policy for business continuity and disaster recovery that has been approved by management, continuity and active content or marketina desire the society. And BCDF tests conducted at least annually? And BCDF tests conducted at least annually? And BCDF tests conducted at least annually? And the second provided of the second provided annual second provided provided annual second provided provided annual second provided provided provided annual second provided pr	Is logging enabled on all Scoped Systems? Does loading data get sent to a Security Information and Event Management (SIEM) tool?			
A three as annual achieval of a least annuals of the common of the commo	Is there a documented policy for business continuity and disaster recovery that has been approved by management,			
In these measures coverage for because stempoters or general excess intemporary. 12 Consideration 13 Consideration 14 Consideration requisitory issues? 15 Consideration 15 Consideration 16 contained on requisitory issues? 16 contained on requisitory issues? 18 Consideration 18 Consideration	Is there an annual schedule of required tests? Are BC/DR tests conducted at least annually?			
is there are internal audit, risk management or compliance department with responsibility for identifying and tracking recording of continued to compliance and orders reporting mechanism and training program for employees to report compliance and compliance and continued compliance and orders reporting mechanism and training program for employees to report compliance and continued and contin	Is there insurance coverage for business interruptions or general services interruption?			
Is there are informal compliance and efficie reporting mechanism and training programs for employees to report compliance between the control of the control	is there an internal audit, risk management or compliance department with responsibility for identifying and tracking resolution			
As mobile devices used to access Scoped Systems and District Scoped Data returnishing processed or store that can be a second to the store of the s	Is there an internal compliance and ethics reporting mechanism and training program for employees to report compliance issues?			
Is Scoped Data transmitted, processed, or stored that can be desaffed as non-public information (NPI), personally identifiable Scoped Data transmitted, processed, or stored that can be classified as protected Pealer Information, (NPI), personally identifiable Scoped Data transmitted, processed, or stored that can be classified as protected Pealer Information, (NPI), personally information, 1997, personal transmitted into indebulant transmitted to or received from countries custode the United States? For Scoped Data is the tree a declarated person for group) improved the privacy complaines. If yes, describe. If no, explain States. For Scoped Data is the tree a declarated person for group) improved the privacy complaines. If yes, describe. If no, explain States. For Scoped Data are there explain privacy risk assessmentes conductors? If yes, provide Insequency and scope. If no, explain States. For Scoped Data are there explain privacy risk assessmentes conductors? If yes, provide Insequency and scope. If no, explain States. For Scoped Data are there explain privacy risk assessmentes conductors? If yes, provide Insequency and scope. If no, explain States. For Scoped Data are there explain privacy risk assessmentes conductors? If yes, provide Insequency and scope. If no, explain States. For Scoped Data are there explain privacy risk assessmentes conductors? If yes, provide Insequency and scope If no, explain Scoped Data declarates and reterrois program for Scoped Data and stendards privacy incidents or privacy incidents for Scoped Data? If yes, Is there as Scoped Data declarates in build parties I yes, describe. Scoped Data declarates to the grant parties? If yes, describe. Scoped Data declarates to the grant parties? If yes, describe. Scoped Data declarates to the grant parties? If yes, describe. Scoped Data declarates to the grant parties? If yes, describe. Scoped Data declarates to the grant parties of the parties of	Are mobile devices used to access Scoped Systems and Data?			
In Scored Data instructional, processed, or stored that can be described as protected health information, electronic health ### Coopport Data, is prevent information should be the Ministry of the Coopport of the Coopport of Scored Data in State and American Health of the Coopport of Scored Data in State and American Health of Scored Data in Scored Data in State and American Health of Scored Data in State in State and American Health of Scored Data in State in Scored Data in Scored Data in Scored Data in State in Scored Data	is Scoped Data transmitted, processed, or stored that can be classified as non-public information (NPI), personally identifiable			
Less, desirable, the countries. "Or Scope Olbas is these a declarated person (or group) responsible for privacy compliance. If yes, describe, If no, explain Far Scopeo Olbas is there a declarated person (or group) responsible for privacy compliance. If yes, describe, If no, explain Far Scope Olbas is there a declarated person (or group) responsible for privacy compliance, If yes, provide frequency and scope, If no, explain is these formal privacy awareness training for employees, contractors, and their party users to ensure confidentially and ordinaries of Scope Olbas and the seasons and contractions of Scope Olbas and the seasons and contractions of Scope Olbas and the seasons and contractions and described ordinaries of Scope Olbas and the seasons and the seasons of Scope Olbas And the seasons and the seasons of Scope Olbas And the seasons and the seasons of Scope Olbas And the Scope Olbas And the Scope Olbas And the Scope Olbas And the Scop	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.			
Association of the control process of the process of the control pro	If yes, identify the countries.			
Section and privacy assumes training for employees, contactors, and third pathy users to ensure confidentiality and desirated formed bearing. In these is formal process for reporting and responding to privacy compliants or privacy incidents for Scoped Data? Yee, describe. If no septial responding to privacy promptines are privacy incidents for Scoped Data? Yee, describe and process of the pro	reason			
some of Scored Dail? In these a formal process in reporting and responding to privacy compliants or privacy incidents for Scoped Data? It yes, In these a data classification and reterrition program for Scoped Data and derivatives the data types that require additional management and appropriate or program to address privacy products, unauthorized disclosure, unautho	reason.			
describe. If no, explain reason. In there a data classication and reletrion program for Scoped Data that identifies the data types that require additional In there a data classication and reletrion program for Scoped Data that identifies the data types that require additional In these a documented response program to address princy incident, unsubflorided disclosure, unsubflorided access or hashand of Scored Data disclosured by the state of	privacy of Scoped Data?			
In there is documented response program to address prinsivy incidents, unsulhnotized disclosure, unsulhnotized access or busines documented response program to address prinsivy incidents, unsulhnotized disclosure, unsulhnotized access or business. The program of the program o	describe. If no, explain reason. Is there a data classification and retention program for Scoped Data that identifies the data types that require additional			
In Scored Data dischards its mind garless? If yes, describe. Second Data dischards in their charge of the U.S. If yes, describe. Second Data dischards on their carties revised of the U.S. If yes, describe. Second Data dischards on their carties revisited of the U.S. If yes, describe. As the reconstruction of their carties revised of their carties of their parties in limited to defined parameters for access, us, as and declinated? If yes, describe the controls, if no, explain research, as and edischard? If yes, describe the controls, if no, explain research explains research and their carties of the services produced in the services pr	Is there a documented response program to address privacy incidents, unauthorized disclosure, unauthorized access or			
access with a Contractorist? Access with a Contractorist? Access with a Contractorist? Access with a Contractorist? Access with a Contractorist was a contract with initing parties in limited to defined parameters for access, in them as business associate contracts or applicable contractual languages in place to address obligations for the privacy and social access with a contract or applicable contractual languages in place to address obligations for the privacy and social access with a contract or applicable contractual languages in place to address obligations for the privacy and social access with a contract or applicable contractual languages in place to address obligations for the privacy and social access with a contract or ac	Is Scoped Data disclosed to third parties? If yes, describe			
use and decisionary? If yes, describe the controls, If no explain reason. If there is burners and control explains of specials controls used in singulary in place to address obligations for the privacy and its there is a burners and a documented privacy program with administrative, technical, and physicial safeguands for the protection of Scoped Sections and Data". Sections and Data". With regard to the scoped data: is there a porcess to ensure that the personal information provided by an individual initiated by the proposed sections of the client? If yes, describe. If no, explain exacts. With regard to the scoped data: is there as process to ensure that the personal information provided by an individual initiated by the proposed shortfeet in the reasonativity privacy individual? If yes, describe. If yes, describe it no explain exacts. As these documentary droves, processed and controls to lints accessed, thereof yes the control of	access with a Contractor(s)?			
Security requirements of the services provided? In these a process provided privacy program with administrative, technical, and physical safeguants for the protection of Scoped In these as process for ensuring the accuracy of Scoped Data at the direction of the client? If yes, describe, If no, opplain The process for ensuring the accuracy of Scoped Data at the direction of the client? If yes, describe, If no, opplain The process described in the respondent is privacy included by an included by an included at instead for the purposes described in the respondent is privacy included. If yes, describe, If no, opplain reason. An excessionate instantive monitored for sense for exeminative that is a constitution of the process of the control of th	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			
Sections and Chat? In these a process for resuring the accuracy of Scoped Data at the direction of the client? If yes, describe, If no, explain the three a process for resuring the accuracy of Scoped Data at the direction of the client? If yes, describe, If no, explain With regard to the scoped data; as there a process to resurve that the purposes developed the resurrence of the purposes developed the three spreaders produced part of the scoped data; the purpose developed the process to resurve that the purpose developed the process to resurve the purpose developed the purpose devel	security requirements of the services provided? Is there a documented privacy program with administrative, technical, and physical safeguards for the protection of Scoped			
for the purposes described in the respondent's prince or indirect in the companion respon. Application of the prince of the purposes described in the respondent prince or indirect in the companion of the prince described in the prince of t	Systems and Data?			
As constituents anotable, monitored for entires controllators? If you, describe, I'm, esobles reason. As the documental produces, procedure, and controls to lint access based on need to trove or informum necessary for a second product of the control and				
constituents' If was, discribe. constituents' If was, discribe. An extraction of the constituent was violent princip colors or confidentially manimisments' and destruction of the constituents was violent princip colors. If was, discribe. If was, discribe.	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			
Jas. describe. 1. southerer data accessed, transmitted, processed, or stored that can be classified as consumer report information provided 1. southerer data accessed, transmitted, processed, or stored that can be classified as consumer report information provided 1. southerer as a consecutive of the constructor enrollers, managine anotic maintainine a closed solution? 1. southerer as a Sergee (Saski) 1. s	constituents? If ves. describe. Are enforcement mechanisms applied to constituents who violate privacy policies or confidentiality requirements?			
to's a consumer recordine sector // 18. Could filthe Contractor serviding, managing and/or maintaining a cloud solution?! An Could Services provided? If ve, what service model and deployment model is provided tester all that apply? Software as a Service (Past) Pastion as a Service (Past) Person Could Pe	ves describe			
Am Cloud Services provided If I've, what service model and deployment model is provided fastert all that apply? Software as a Service (Past) Pastoma as a Service (Past) Person Cloud Service (Service	by a consumer reporting agency? 16. Cloud (Is the Contractor providing, managing and/or maintaining a cloud solution?)			
Inflastructure as Service (tasS) Protest cloud Public cloud Public cloud Community cloud	Are Cloud Services provided? If yes, what service model and deployment model is provided (select all that apply): Software as a Service (SaaS)			
Public cloud Community cloud	Infrastructure as a Service (laaS)			
Hybrid cloud Does Scoped Data stay within North America?	Public cloud Community cloud			
	Hybrid cloud Does Scoped Data stay within North America?			



EVERS@URCE

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" - Information Security Policies and Procedures. This should include the following (if not, provide the individual documents as necessary): a) Histing policies and practices and employment application b) User Account administration policy and procedures for all supported platforms where Scoped Systems and Data are processed and network. All Access. c) Supporting documentation to indicate completion of User Entitlement reviews d) Information Security indicates and network. All Access. d) Information Security indicates and Procedures e) Information Security indicates and Procedures e) Security Log Review Policies and procedures e) Security Log Review Policies and Procedures e) Capy of Internal or external information security suddit reports (SC2 Information technology and security organization charts (including where Respondent information security reades and the composition of any information security sudding and procedures of the security reades and the composition of any information security sudding and procedures of the security reades and the composition of any information security sudding and procedures of the security including and reporting process. - Physical Security policy and grocensus Residual Security policy and grocensus Residual Security social security social in the security including and reporting process - Residual Security policy and grocedures and security sudding and reporting process - Residual Security policy and procedures - System and retrock configuration standards - System backup policy and procedures - System backup policy and procedures - System backup policy and procedures - Problem manugement policy procedures - Problem manugement policy procedures - Problem manugement policy procedures - Sortions development and liepsempant scan policy and procedures - Pro	An Avangid company	
will be asked to provide the following documentation with a "X" in the "Column B" * Information Security Policies and Procedures. This should include the following (if not, provide the individual documents as necessary): a) Hiding policies and practices and employment application b) User Account administration policy and procedures for all supported platforms where Scoped Systems and Data are processed and network. All Access. c) Supporting documentation to indicate completion of User Entitlement reviews d) Employee Mondisclosions aggreement document e) Information Security Inodent Report policy and procedures, including all contract information c) Copy of Vistor Policy and procedures d) Security Log Review Policies and Procedures d) Core of Vistor Policy and procedures d) Critical 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 securities and the composition of any Information security security access and confidentialises of any the Composition of any Information security security access and confidentialises of any Information security security access and confidentialises of any Information security security access and confidentialises of any Information security security access and confidentialise properting procedures (Sulfained Papertine) **Psycal Society policy and reporting procedures **Society includent handling and reporting process **Network configuration diagrams for internal and external retworks defined in scope. **Note: Sentined versions of the retwork diagram as acceptable **Society includent handling and reporting process **Note: Sentined versions of the retwork diagram as acceptable **Vulnerability and Prest management scon policy and procedures **Vulnerability and Prest management policy/procedures **Problem management policy/procedures **Problem management policy/procedures **Pulneras scalary policy and proc	Based on the services the 'Contractor' is performing or providing and	
* Information Security Policies and Procedures. This should include the following (if not, provide the individual documents as necessarsy): a) Hiring policies and practices and employment application b) User Account administration policy and procedures for all supported platforms where Scoped Systems and Data are processed and network/LAN access. a) Supporting documentation is indicate completion of User Entitlement reviews a) Structure of Data are processed and network/LAN access. b) Corpy of Vistor Policy and procedures c) Security Log Review Policies and Procedures c) Corpy of Vistor Policy and procedures c) Corpy of Vistor Policy and procedures c) Corpy of Vistor Policy and procedures c) Criticital/requirements when performing background checks d) Criticital/requirements when performing background checks c) Criticital checks and the composition of any information security resides and the composition of any information security resident residence and composition of any information security resident residence and composition of any information security residence and composition of any in		UI/Eversource Requested
individual documents as necessary): a) Hiding policies and practices and employment application b) User Account administration policy and procedures for all supported platforms where Scoped Systems and Data are processed and network IAN access. c) Supporting documentation to indicate completion of User Entitlement reviews d) Employee Non-disclosure agreement document d) Employee Non-disclosure agreement d) Export of third party risk management policies and proceedures l) Copy of Internal or external information security suggested and the composition of any information security stering committees. Copy of Internal or external information security stering committees). Note: Actual names of employees are not required Pyhysical Security policy and procedures (building and/or restricted access) Third-party security reviews/assessments/penetration tests Legal closues and confidentially templotes for third parties Topics covered in the security triating program Security incident harding and reporting process Network configuration diagrams for internal and external networks defined in scope. Security incident harding and reporting process Network configuration diagrams for internal and external networks defined in scope. System and relevant configuration standards System backup policy and procedures System backup policy and procedures Typical control policy/procedures Typical control policy/procedures Typical control poli		
a) Hiring policies and practices and employment application b) User Account administration policy and procedures for all supported platforms where Scoped Systems and Data are processed and network/LAN access c) Supporting documentation to indicate completion of User Entitlement reviews d) Employee Non-disclosure agreement document d) Employee Non-disclosure agreement document d) Information Security incident Report policy and procedures d) Security (c) Review Policies and Propodutes d) Security (c) Review Policies and Propodutes d) Security (c) Review Policies and Propodutes d) Criterial-requirements when performing background checks c) Capy 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 settlenges). Note: Actual names of employees are not required Note: Actual names of employees are not required composition of a property organization charts (including where Respondent information security security reviews security reviews security reviews and the composition of any information security settlenges. Note: Actual names of employees are not required composition of a property organization charts (including where Respondent information security security reviews security reviews security reviews security reviews security reviews and the composition of any information security security reviews security reviews and the security security reviews security reviews and the security organization disparate for third parties c) Topics covered in the security training program c) Security incident handling and reporting process Networks Confidentially semplates for third parties c) Topics covered in the security training program c) Security incident handling and reporting process Networks Confidentially semplates for third parties c) System and network configuration standards c) System backup policy and procedures c) System and network configuration s	* Information Security Policies and Procedures. This should include the following (if not, provide the	
b) User Account administration policy and procedures for all supported platforms where Scoped Systems and Data are processed and network[AN access.] c) Supporting documentation to indicate completion of User Entitlement reviews d) Employee Non-disclosure agreement document e) Information Security Incident Report policy and procedures e) (Copy of Visitor Policy and procedures (policy and procedures policy pr	**	
c) Supporting documentation to indicate completion of User Entitlement reviews d) Employee Non-disclosure agreement document e) Information Security Incident Report policy and procedures g) Security Log Review Policies and Procedures g) Security Log Review Policies and Procedures g) Security Log Review Policies and Procedures g) Criteria/requirements when performing background checks g) Criteria/requirements go check go g) Criteria/requirements g) Criteria/requirements g) g) Criteria/requirements go confidentiality remplates for third parties g) Criteria/requirements g) Criteria/requirements g) g) Criteria/requirements g) Criteria/requirements g) Criteria/requirements g) g) Criteria/re		
e) Information Security Incident Report policy and procedures including all contract information () Copy of Visitor Policy and procedures () Corteria/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 registers) and the composition of any information security steering committees). Note: Actual armses of employees are not required **Physical Security policy and procedures fluiding and/or restricted access) **Third-party security reviews/assessments/penetration tests Legal clauses and conflidentiality templates for third parties Topics covered in the security flaming program *Security incident handling and reporting process Notes: Santitized versions of the network diagram are acceptable *System and network configuration standards *System backup policy and procedures *Unherability and retoration security process *Offsite storage policy and procedures *Unherability and threat management scan policy and procedures *Unherability and threat management scan policy and procedures *Application security policy *Change control policy/procedures *Problem management policy/procedures *Problem management policy/procedures *Problem management policy/procedures *Problem management policy/procedures *Software development and lifecyle (SDLC) process document *Business contriou lylan (BCP) and 7 or Disaster recovery plan *Most recent BCP/DR test dates and results *Most recent BCP/DR test dates and results *Provacy policies and rotices (internal, external, veb); including but not limited to privacy by design, data processing agreements, data retention and privacy internation of a Response Plan including: *Documentation of Proversion of Received Process of Contraction of Tractical Process of Co	· ·	
() Copy of Visitor Policy and procedures () Security Log Review Policies and Procedures () Criteria-loguirements 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). Note: Actual names of employees are not required Physical Security policy and procedures (building and/or restricted access) **Third-party security review-assessments/persertation tests Legal clauses and conidentiality 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. Note: Santized versions of the network diagram are acceptable **System and network configuration standards **System and network configuration standards **System and network configuration standards **System policy and procedures **Offisite storage policy and procedures **Offisite storage policy and procedures **Vulnerability and threat management scan policy and procedures **Problem management policy/procedures **Proving management policy		
in) Copy of third party risk management policies and procedures 1) 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). Note: Actual names of employees are not required * Physical Security policy and procedures (building and/or restricted access) * Third-party security reviews/assessments/persertation 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. * Note: Sanitized versions of the network diagram are acceptable * System and network configuration standards * System and network configuration standards * System and network configuration standards * System security policy and procedures * Universibility and threat management scan policy and procedures * Universibility and threat management scan policy and procedures * Application security policy * Problem management policy/procedures * Problem management policy/procedures * Certification of proprietary encryption algorithms * Territorial universibility assessments of systems, applications, and networks * Software development and lifecycle (SDLC) process document * Business continuity plan (ECP) and / or Dissaster recovery plan * Most recent SCP/DR test dates and results * Most recent SAET6(18) SCC2 or SCC3 audit report * Provacy policies and notices (internal, external, web); including but not limited to privacy by design, data procedures, data retention and privacy frameworks. * Executive SIAMEN SAET6(18) SCC2 or SCC3 audit report * Provacy policies and Procedures. This should include the following (if not, provide the individual documents as necessary): * Documentation of Proces	f) Copy of Visitor Policy and procedures	
**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). **Note: Actual names of employees are not required **Physical Security policy and procedures (building and/or restricted access) **Third-party security review/sasessements/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 disparants for internal and external networks defined in scope. **Network configuration disparants for internal and external networks defined in scope. **Network configuration disparants for internal and external networks defined in scope. **Network configuration disparants for internal and external networks defined in scope. **Network configuration disparants for internal and external networks defined in scope. **Network configuration disparants for internal and external networks defined in scope. **Network configuration disparants for internal and external networks defined in scope. **Network configuration disparants for internal and external networks defined in scope. **Note: Sanitized versions of the network diagram are acceptable **System backup opicicy and procedures **Application security policy procedures **Application security policy procedures **Problem management policy/procedures **Proble	5, , S	
Information technology and security organization charts (including where Respondent information security resides and the composition of any information security steering committees). Note: Actual names of employees are not required *Physical Security policy and procedures (building and/or restricted access) *Third-party security review/sassessments/penetration tests Legal clauses and confidentiality templates for third parties Topies covered in the security training program *Security incident handling and reporting process Network configuration diagrams for internal and external networks defined in scope. Note: Sanitized versions of the network diagram are acceptable *System and network configuration standards *System backup policy and procedures *Official storage policy and procedures *Application security policy *Change control policy/procedures *Access control policy/procedures *Certification of proprietary encryption algorithms Internal vulnerability assessments of systems, applications, and networks *Software development and lifecycle (SDLC) process document *Business continuity plain (BCP) and 7 or Disaster recovery plan *Most recent SSAE 16/18/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 (in 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 the Development and Implementation of Acces		
security resides and the composition of any information security steering committees). 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. Note: Santized versions of the network diagram are acceptable *System and network configuration standards *System backup policy and procedures *Offsite storage policy and procedures *Offsite storage policy and procedures *Application security policy *Change control policy/procedures *Access control policy/procedures *Access control policy/procedures *Certification of proprietary encryption algorithms *Internal vulnerability assessments of systems, asplications, and networks *Software development and lifecycle (SDLC) process document *Business contriluty plan (BCP) and / or Disaster recovery plan *Most recent BCP/DR test dates and results *Most recent BCP/DR test dates and results *Most recent BCP/DR test dates and results *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 *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 Prevention of Recurrence *Conditation of Indicated Response with Company *Notification to Affected Parties *Contractor Review of Access *Other Contractor Review of Access *Notification and Reviews of Access *Notification and Reviews of Access *Notification and Reviews of Access *Notification and Revie		
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. Note: Santitized versions of the network diagram are acceptable * System and network configuration standards * System backup policy and procedures * Offsite storage policy and procedures * Offsite storage policy and procedures * Uninerability and threat management scan policy and procedures * Application security policy * Change control policy/procedures * Access control policy/procedures * Access control 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 7 or Disaster recovery plan * Most recent BCP/DR test dates and results * Most recent BCP/DR test dates and results * Most recent SSAE fish (SOC or SOCs) 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 Prevention of Recurrence * Coordination of Indicated Response with Company * Notification to Affected Parties * Unrelated Security Incidents * Access control policy/procedures including: * Documentation of Prevention of Recurrence * Contriactor Review of Access * Notification to Affected Parties * Controls for Remote Access * Disclos		
*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. Note: Santitized versions of the network diagram are acceptable *System backup policy and procedures *Offsite storage policy proced		
Topics covered in the security training program 'Security incident handling and reporting process Network configuration diagrams for internal and external networks defined in scope. Note: Sanitized versions of the network diagram are acceptable 'System and network configuration standards 'System backup policy and procedures 'Offsite storage policy and procedures 'Uninerability and threat management scan policy and procedures 'Application security policy 'Change control policy/procedures 'Access control policy/procedures 'Access control 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 SCP/DR test dates and results 'Most recent SCP/DR contices (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. PCL 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 Prevention of Recurrence 'Coordination of Incident Response with Company 'Notification to Affected Parties 'Unrelated Security Incidents 'Access control policy/procedures including: 'Documentation of Prevention of Recurrence 'Coordination of Incident Response with Company 'Notification to Affected Parties 'Unrelated Security Incidents 'Access control policy/procedures including: 'Contractor Review of Access 'Notification of Access Control Policy 'Company Authority Over Access 'Notification of Remote Access 'Notification of Remote Access 'Notification of Remote Access 'Notification of Remote Access 'Dol	* Third-party security reviews/assessments/penetration tests	
* Security incident handling and reporting process Network configuration internal and external networks defined in scope. Note: Sanitized versions of the network diagram are acceptable * System and network configuration standards * System backup policy and procedures * Offsite storage 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 * Problem management policy-procedures * Problem management policy-procedures * Certification of prorpitalizy-procedures * 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 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 anecessary): * 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 Prevention of Recurrence * Coordination of Incident Response with Company * Notification to Affected Parties * Unrelated Security Incidents * Access control policy/procedures including: * Documentation of Prevention of Recurrence * Contractor Review of Access * Notification and Revocation * Controls for Remote Access * Notification and Revocation * Controls for Remote Access * Disclosure by Contractors of known vulnerabilities		
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 * Application security policy/procedures * Problem management 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/RISOC2 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 Prevention of Recurrence * Coordination of Incident Response with Company * Notification to Affected Parties * Unrelated Security Incidents * Coordination and Implementation of Access Control Policy **Company Authority Over Access * Controls for Remote Access * Ontrols for Remote Access * Ontrols for Remote Access * Documentation of Provention of Response Plan including: * Controls for Remote Access * Controls for Remote Access * Controls for Remote Access * Documentation of Response Access * Notification and Revocation * Controls for Remote Access	* Security incident handling and reporting process	
* System and network configuration standards * System backup policy and procedures * Offsite storage policy and procedures * Vulnerability and threat management scan policy and procedures * Vulnerability and threat management scan policy and procedures * Application security policy * Change control policy/procedures * Problem management 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 continuty plan (BCP) and or Disaster recovery plan * Most recent BCP/DR test dates and results * Most recent BCP/DR test dates and results * Most recent BSAE16/18/SOC2 or SOC3 audit report * Privacy policies and notices (internat, externat, 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 Process by which the Responsible Entity will address supply chain cyber security risk management for high and medium impact BES Cyber Systems. * 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 ** Contractor Review of Access ** Disclosure by Contractors of known vulnerabilities		
* 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 BCR/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 a 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 Acfected Parties * Unrelated Security Incidents * Access control policy/procedures including: * Development and implementation of Access Control Policy **Company Authority Over Access * Contractor Review of Access * Disclosure by Contractors of known vulnerabilities	* System and network configuration standards	
* Application security policy * Change control policy/procedures * Access control policy/procedures * Problem management 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 BSAE16/18/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 a 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 Incident Response with Company ** Notification to Affected Parties ** Unrelated Security Incidents * Access control policy/procedures including: ** Development and Implementation of Access ** Contractor Review of Access ** Otortactor Review of Access ** Otortactor Review of Access ** Contractor Review of Access ** Disclosure by Contractors of Known vulnerabilities		
* 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 BSAE16/18/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		
* 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 * Access control policy/procedures including: * Development and Implementation of Access Control Policy **Company Authority Over Access ** Contractor Review of Access ** Contractor Review of Access ** Contractor Review of Access ** Octorios for Remote Access ** Octorios for Remote Access ** Disclosure by Contractors of known vulnerabilities	* Change control 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 BSAE16/18/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 ** Notification and Revocation ** Controls for Remote Access ** Disclosure by Contractors of Known vulnerabilities		
* 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 ** Outractor Review of Access ** Notification and Revocation ** Contractor Remote Access ** Disclosure by Contractors of known vulnerabilities	* Certification of proprietary encryption algorithms	
* 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 ** Development and Revocation ** Controst for Remote Access * Disclosure by Contractors of known vulnerabilities	* Software development and lifecycle (SDLC) process document	
* 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 * Notification and Revocation * Contractor Review of Access * Notification and Revocation * Controls for Remote Access * Disclosure by Contractors of known vulnerabilities		
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 "* Contractor Review of Access "* Controls for Remote Access * Disclosure by Contractors of known vulnerabilities	* Most recent SSAE16/18/SOC2 or SOC3 audit report	
* 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 * 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		
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	* Executive Summary of certificates held. (e.g. PCI, HIPAA, ISO)	
* 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		
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		
** 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 ** Disclosure by Contractors of known vulnerabilities ** Disclosure by Contractors of known vulnerabilities	risk management for high and medium impact BES Cyber Systems.	
** 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		
* 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	'* Coordination of Incident Response with Company	
The Development and Implementation of Access Control Policy The Company Authority Over Access The Contractor Review of Access The Notification and Revocation The Controls for Remote Access The Disclosure by Contractors of Known vulnerabilities	'* Unrelated Security Incidents	
**Company Authority Over Access ** Contractor Review of Access ** Notification and Revocation ** Controls for Remote Access * Disclosure by Contractors of known vulnerabilities		
1* Notification and Revocation 1* Controls for Remote Access * Disclosure by Contractors of known vulnerabilities	'*Company Authority Over Access	
* Controls for Remote Access * Disclosure by Contractors of known vulnerabilities		
	'* Controls for Remote Access	
	* 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	'*Hardware, Firmware, Software, and Patch Integrity and Authenticity	
*Patching Governance * Viruses, Firmware and Malware		
* End of Life Operating Systems	* End of Life Operating Systems	
* Cryptographic Requirements * Documentation of Cybersecurity Policy including:	* Documentation of Cybersecurity Policy including:	
*Return or Destruction of Company Information *Audit Rights		
1* Viruses, Firmware and Malware	'* Viruses, Firmware and Malware	
1* End of Life Operating Systems 1* Regulatory Examinations	** End of Life Operating Systems ** Regulatory Examinations	

W UI An Avengrid company EVERS⊕URCE	
Categories of Review	UI/Eversource Analysis and Associated Risk(s)
Contractor Information	
Contractor Questionnaire	
Documentation Requests	