PUGET SOUND ENERGY

2022 Distributed Energy Resources RFP:

Exhibit K. Requirements List

Number	Functional Area	Capability	Aggregator	Direct Connect	Requirement	Must Have	Nice to Have	Future
1.01	Business	Capitalization	✓	✓	Respondent must meet PSE's minimum capitalization requirements	✓		
1.02	Business	Co-branding	✓		Respondent must use PSE branding or co-branding to clearly demonstrate the role of PSE in the project.	✓		
1.03	Business	Co-branding	✓		Respondent must use PSE branding or co-branding when sending notifications to customers	✓		
1.04	Business	Customer	✓		Respondent must provide information on customer complaints received regarding DER products and services	✓		
1.05	Business	Customer	✓		Respondent must have a customer consent and authorization process.		✓	
1.06	Business	Customer	✓		Respondent shall specify how event notification will be sent to PSE customers	✓		
1.07	Business	Customer	✓		Respondent shall specify communication options and/or recommendations for interfacing with customers	✓		
1.08	Business	Customer	✓		Respondent shall indicate how PSE customer interests will be considered when dispatching an event	✓		
1.90	Business	Customer	✓		Respondent shall have the capability to include GHG carbon reduction as part of their reports		✓	
1.10	Business	DER Types	✓	✓	Respondent must provide CETA compliant resource(s)	✓		
1.11	Business	DER Types	✓		Respondent is requested to be able to leverage different DER sub-types to meet commitments. For example, if a Respondent is intending to aggregate batteries PSE requests the Respondent be able to interface with different types of batteries (ex. Tesla, Generac, etc)		✓	
1.12	Business	Disclosure for information use	✓		Respondent must provide clear disclosure to the customer at sign-up regarding the purposes for obtaining their information and with whom the information will be shared.		✓	
1.13	Business	Opt-out	✓		PSE prefers the Respondent provide the ability for customers to opt out of a called event. Respondent to provide a description of the process for opting out.	✓		
1.14	Business	Performance	✓	✓	Respondents proposing dispatchable resources must provide detailed event performance measurements and perform EM&V. Respondent shall specificy what EM&V and baseline capabilities they have.	✓		
1.15	Business	Performance	✓	✓	Respondent must acknowledge that PSE may implement financial penalties for non-performance of kW / kWh targets	✓		
1.16	Business	Performance	✓	✓	Respondent is requested to provide information on how they have handled prior non-performance penalties.		✓	

Number	Functional Area	Capability	Aggregator	Direct Connect	Requirement	Must Have	Nice to Have	Future
1.17	Business	Performance	✓	✓	Respondent must be able to guarantee load flexibility MW reduction by month, day, and hour basis during the event		✓	
1.18	Business	Planned outage	✓	✓	Respondent must provide PSE 7 days advanced notice for any planned DER outage	✓		
1.19	Business	Planned outage	✓	✓	Respondent must provide 7 days advanced notice for any DER testing	✓		
1.20	Business	Rate schedule	✓		Respondent must have the ability to have rate schedules managed by the VPP	✓		
1.21	Business	Record maintenance	✓		Respondent must have a protocol for managing customer consent, including for how long verifiable proof of consent is retained.		✓	
1.22	Business	Record maintenance	✓		Respondent must have a protocol for managing shared customer information. Ex if a customer leaves the aggregator, how long will their customer information be retained in the aggregator's system.	✓		
1.23	Business	Record maintenance	✓		Respondent must allow customers to be able to revoke authorization/consent and withdraw from participation	✓		
1.24	Business	Regulation compliance	✓		Respondent must comply with all applicable laws and regulations, and support PSE's compliance with applicable privacy laws and regulations, including WAC 480-100-153 and WAC 480-90-153.	✓		
1.25	Business	Sale of information	✓		Respondent must not sell any customer information obtained from PSE or from the customer through PSE programs	✓		
1.26	Business	Settlement	✓	✓	Respondent must support settlement process with both DER owners and PSE	✓		
1.27	Business	Use Cases	✓		Respondent shall have the capability to provide stacked services and have the flexibility to meet PSE's evolving needs			✓
2.01	Engineering	Asset Management	✓	✓	Respondent must provide the physical location and, when available, the feeder the DER is connected to PSE for incorporation into GIS system for DER > 25 kVA (see also requirement 6.04)	✓		
2.02	Engineering	Asset Management	✓	✓	Respondent must provide DER nameplate information to PSE for DER > 25 kVA	✓		
2.03	Engineering	Asset Management	✓	✓	Respondent requested to provide geographical information (LAT/LON) to feed into the VPP's geographical/mapping interface	✓		
2.04	Engineering	Communications		✓	Respondent requested to validate that the DER can communicate through LTE cellular and send IEEE 2030.5 controls. What LTE cellular carrier is being proposed? What cellular carriers have you used in the past? Where was this done? What equipment (i.e., battery controller, inverter, both) does the IEEE 2030.5 signal control?		✓	

Number	Functional Area	Capability	Aggregator	Direct Connect	Requirement	Must Have	Nice to Have	Future
2.05	Engineering	Grid Operation		✓	Respondent must meet the interconnection requirements set forth in: -PSE's Tariff Schedule 152 - Interconnection with Electric Generators (https://www.pse.com/-/media/Project/PSE/Portal/Rate-documents/Electric/elec_sch_152.pdf) -IEEE 1547-2018: Standard for Interconnection and Interoperatbility of Distributed Energy Resources with Associated Electric Power System Interfaces (https://standards.ieee.org/products-services/standards-related/pdf/electric-power-systems.html), and -PSE's Technical Specification and Operating Procedures for Interconnection of Generation Facilities Not Subject to FERC Jurisdiction (https://www.oasis.oati.com/woa/docs/PSEI/PSEIdocs/PSE-ET-160.70_NonFERC_19Aug07.pdf)	✓		
2.06	Engineering	Inverter	✓	✓	Respondent must provide DER inverter specifications to PSE for DER >= 25 kVA including, but not limited to: -Rated AC output power, current, and voltage; -Power factor range of adjustability; -Available voltage and frequency protective elements; -Available grid support functions (anti-islanding, voltage ride through, voltage support, etc.); -Available communication protocols; -Grid standard (IEEE 1547 and UL1741) compliance information	✓		
2.07	Engineering	Inverter	✓	✓	Respondent requested to provide DER inverter specifications to PSE for DER < 25 kVA including, but not limited to: -Rated AC output power, current, and voltage; -Power factor range of adjustability; -Available voltage and frequency protective elements; -Available grid support functions (anti-islanding, voltage ride through, voltage support, etc.); -Available communication protocols; -Grid standard (IEEE 1547 and UL1741) compliance information		✓	
2.08	Engineering	Safety standards	✓	✓	Respondent must ensure that all proposed resource must comply with all existing Puget Sound Energy, WA state, and national safety standards	✓		

Number	Functional Area	Capability	Aggregator	Direct Connect	Requirement	Must Have	Nice to Have	Future
2.09	Engineering	Standards	✓	✓	Respondent must adhere to all applicable PSE interconnection processes and comply with all applicable PSE technical specifications	✓		
2.10	Engineering	Voltage level		✓	Respondent must specify the voltage level for DER interconnection in kV.	✓		
2.11	Engineering	Voltage level		✓	Respondent must indicate the interconnected DER output capacity in kVA and kW	✓		
3.01	IT	Compliance	✓		Respondent must be certified and include proof of a current SOC2 audit for SaaS and Cloud software implementations. On premise Respondents do not need an SOC2 audit. Respondents who are in the process of a SOC2 audit will be considered if a letter is provided from their auditor stating they are in a SOC2 audit and have an estimated completion date by July 1, 2022.	✓		
3.02	IT	Compliance	✓	✓	Respondent must comply with NERC CIP-003-8 R2 if total power is greater than 75MVA and connection voltage is greater than or equal to 100kV, this includes the following: •Cyber Security Awareness (Reinforce, at least once every 15 calendar months, cyber security practices) •Physical Security Controls (Control physical access to cyber assets) •Electronic Access Controls (Permit only necessary electronic access) •Cyber Security Incident Response (Have a Cyber Security Incident Response Plan, test at least once every 36 months & update if needed within 180 days of a test or actual incident) •Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation (Plan for using transient cyber assets and removable media on applicable cyber assets to mitigate risk of introducing malicious code)	✓		
3.03	IT	Cybersecurity	✓		Respondent must meet industry best practices for security standards set by NIST-IR 7628	✓		
3.04	IT	Cybersecurity	✓		Respondent must encrypt data in motion using TLS 1.2+	✓		
3.05	IT	Cybersecurity	✓		Respondent must encrypt data at rest using AES-256 or better	✓		
3.06	IT	Cybersecurity	✓		Respondent must support standard approaches for network connectivity to the Respondent platform, including firewall rules on both sides, IP restrictions to PSE's external IP range, and VPN connectivity for connections back to PSE OT systems, amongst others. Details will be determined during the design phase of the implementation project	✓		

Number	Functional Area	Capability	Aggregator	Direct Connect	Requirement	Must Have	Nice to Have	Future
3.07	IT	Cybersecurity	✓		Respondent shall provide cyber security features, including but not limited to: authentication, encryption, access control, event and communication logging, monitoring and alarming to protect the system from unauthorized modification or use	✓		
3.08	IT	Cybersecurity	✓		Respondent shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time and through-put (including during the Site Acceptance Testing (SAT) when connected to existing equipment)	✓		
3.09	IT	Cybersecurity	✓	✓	Respondent shall remove or disable all software components that are not required for the operation and maintenance of the device prior to the Factory Acceptance Testing (FAT). The Respondent shall provide documentation on what is removed and/or disabled	✓		
3.10	IT	Cybersecurity	✓	✓	Respondent shall provide, within a pre-negotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security	✓		
3.11	IT	Cybersecurity	✓	✓	Respondent shall certify that its systems and products have undergone cyber security testing by leading and independent government sanctioned organizations	✓		
3.12	IT	Cybersecurity	✓	✓	After contract award, the Respondent shall provide notification of known security vulnerabilities affecting the Respondent supplied or required operating system, application and critical third-party software within a pre-negotiated period after public disclosure	✓		
3.13	IT	Cybersecurity	✓	✓	After contract award, the Respondent shall provide notification of a patch(es) affecting security within a pre-negotiated period, as identified in the patch management process. The Respondent shall apply, test and validate the appropriate updates and/or workarounds on a baseline reference system before distribution. Mitigation of these vulnerabilities shall occur within a pre-negotiated period	✓		
3.14	IT	Cybersecurity	✓		After contract award, the Respondent shall provide firewalls and firewall rule sets between network zones or provide firewall rule sets if the firewalls are not provided by the Respondent. The Respondent shall provide firewall rule sets and/or other equivalent documentation. The basis of the rule set shall be “deny all,” with exceptions explicitly identified by the Respondent. Note that this information is deemed business sensitive and shall be protected as such	✓		

Number	Functional Area	Capability	Aggregator	Direct Connect	Requirement	Must Have	Nice to Have	Future
3.15	IT	Cybersecurity	✓		After contract award, the Respondent shall provide detailed information on all communications (including protocols) required through a firewall, whether inbound or outbound, and identify each network device initiating a communication in accordance with the corresponding rule sets	✓		
3.16	IT	Cybersecurity	✓		Respondent shall not permit user credentials to be transmitted in clear text. The Respondent shall provide the strongest encryption method commensurate with the technology platform and response time constraints. The Respondent shall not allow applications to retain login information between sessions, provide any auto-fill functionality during login or allow anonymous logins. The Respondent shall provide user account-based logout and timeout settings	✓		
3.17	IT	Cybersecurity	✓		Respondent shall provide a configurable account password management system that allows for selection of password length, frequency of change, setting of required password complexity, number of login attempts, inactive session logout and denial of repeated or recycled use of the same password	✓		
3.18	IT	Cybersecurity	✓		Respondent shall not store passwords electronically or in Respondent-supplied hardcopy documentation in clear text unless the media is physically protected. The Respondent shall control configuration interface access to the account management system. The Respondent shall provide a mechanism for rollback of security authentication policies during emergency system recovery or other abnormal operations where system availability would be negatively impacted by normal security procedures	✓		
3.19	IT	Cybersecurity	✓		Respondent shall provide a system whereby account activity is logged and is auditable both from a management (policy) and operational (account use activity) perspective. The Respondent shall time stamp and control access to audit trails and log files. The Respondent shall ensure audit logging does not adversely impact system performance requirements	✓		
3.20	IT	Cybersecurity	✓		Respondent shall provide for user accounts with configurable access and permissions associated with the defined user role. The Respondent shall adhere to least privileged permission schemes for all user accounts and application-to-application communications	✓		

Number	Functional Area	Capability	Aggregator	Direct Connect	Requirement	Must Have	Nice to Have	Future
3.21	IT	Cybersecurity	✓		Respondent shall verify that a user cannot escalate privileges, under any circumstances, without logging into a higher-privileged role first. The Respondent shall provide a mechanism for changing user(s) role (e.g. group) associations. After contract award, the Respondent shall provide documentation defining access and security permissions, user accounts, applications and communication paths with associated roles	✓		
3.22	IT	Cybersecurity	✓		Respondent shall provide a Single Sign-On (SSO) such that Role-based Access Control (RBAC) enforcement is equivalent to that enforced as a result of direct login. This system should be RBAC capable. The Respondent shall provide documentation on configuring such a system and documentation showing equivalent results in running validation tests against the direct login and the SSO. The Respondent shall protect key files and Access Control Lists (ACLs) used by the SSO system from non-administrative user read, write and delete access. Note that SSO must resolve individual user's logins to each application	✓		
3.23	IT	Cybersecurity	✓		The Respondent shall have and provide documentation of a written flaw remediation process for all software they develop. The Respondent shall provide appropriate software updates and/or workarounds to mitigate all vulnerabilities associated with the flaw within a pre-negotiated period.	✓		
3.24	IT	Cybersecurity	✓		After contract award, when the Respondent is made aware of or discovers any flaws, the Respondent shall provide notification of such flaws affecting security of Respondent-supplied software within a pre-negotiated period. Notification shall include, but is not limited to, detailed documentation describing the flaw with security impact, root cause, corrective actions, etc. (This language is typically found in a quality assurance document, but is included here for completeness.)	✓		
3.25	IT	Cybersecurity	✓		Respondent's aggregation system must track and maintain third-party penetration tests	✓		
3.26	IT	Cybersecurity	✓		Respondent's aggregation system must log all events, including security-related event status with an accurate timestamp.	✓		
3.27	IT	Cybersecurity	✓		Respondent's aggregation system must not require read/write/execute access to filesystems outside its web root folder and must not execute OS-level commands based off of user input	✓		
3.28	IT	Cybersecurity	✓		Respondent's aggregation system must physically or logically separate PSE's data from other of Respondent's customers' data	✓		

Number	Functional Area	Capability	Aggregator	Direct Connect	Requirement	Must Have	Nice to Have	Future
3.29	IT	Cybersecurity	✓		Respondent's aggregation system must secure API access and system connectivity (e.g., API keys, SSH keys)	✓		
3.30	IT	Cybersecurity	✓		Respondent's aggregation system must support single sign-on using SAML 2.0.	✓		
3.31	IT	Data security	✓		Respondent must ensure data security for all usage, metering, settlement, and customer information in the context of PSE's Security Addendum (Consultant or Hosted).	✓		
3.32	IT	Data security	✓	✓	Respondent must comply with PSE's Security Addendum (Consultant or Hosted) for data security requirements.	✓		
3.33	IT	Data security	✓		Respondent must secure customer data and describe the manner in which this data is secured.	✓		
3.34	IT	Deployment	✓		Respondent to indicate preferred pattern of solution. PSE's preference is for SaaS solution, but will consider other deployment patterns. If not SaaS, please provide details on architecture		✓	
3.35	IT	High Availability	✓		Respondent must support a high-availability architecture. Please describe your product's architecture to support a high level of reliability. What is your committed level of product up-time?		✓	
3.36	IT	High Availability	✓		Respondent shall support high availability operations with redundant infrastructure and communications along with continuous automated monitoring, alerting and automated failover	✓		
3.37	IT	High Availability	✓		Respondent must support reliable connections to SaaS and cloud-hosted software. Please describe best practices for integration of your software to the PSE VPP.	✓		
3.38	IT	Integration	✓		Respondent requested to be capable of communicating over AMI, Cellular, and Broadband networks utilizing standards-based and proprietary protocols to communicate with DER		✓	
3.39	IT	Integration	✓		Respondent must be able to integrate DER monitoring, control, and dispatch to PSE VPP using Open ADR 2.0	✓		
3.40	IT	Integration	✓		Respondent must have the ability to interface with and be controlled by the PSE VPP	✓		
3.41	IT	Integration	✓	✓	For VPP interfacing resources, Respondent is requested to provide a list of presently operational VPP interfaces and a separate list of VPP interfaces that have only been piloted.	✓		
3.42	IT	Integration	✓		Respondent must support a programmatic interface to the PSE VPP implementation	✓		
3.43	IT	Offshore	✓		Respondent must use datacenters located in the US for SaaS or Cloud	✓		

Number	Functional Area	Capability	Aggregator	Direct Connect	Requirement	Must Have	Nice to Have	Future
3.44	IT	Security	✓	✓	Respondent must comply with PSE's Security Addendum (Consultant or Hosted) with respect to contractor management.	✓		
3.45	IT	Standards	✓		Respondent is requested that the system shall have capability to be configured as a OpenADR V2.0b VTN		✓	
3.46	IT	Standards	✓	✓	Respondent requested that system be capable of fully complying with and capable of communicating over the following standards and communication protocols: IEEE 2030.5, DNP3 SCADA protocol devices, Modbus SCADA protocol devices, SunSpec Smart Inverter Profile (Modbus or DNP3), MESA Storage Profile (Modbus or DNP3), ICCP		✓	
3.47	IT	Standards	✓		Respondent is requested to have the capability to be dispatched via open standards or non-proprietary protocols. Please describe preferred and outline any other feasible mechanisms for dispatch of DER assets.		✓	
4.01	Load Office	DER Control		✓	Respondent must have the ability to be managed by, interface with, and directly be controlled by the PSE VPP for solar deployments >=0.5MW and <2MW and FOTM BESS <2MW	✓		
4.02	Load Office	Dispatch	✓	✓	Respondent must have the capability to indicate resource availability for dispatch	✓		
4.03	Load Office	Forecasting	✓	✓	Respondent required to have the capability to provide generation capacity up to 48 hours in advance	✓		
4.04	Load Office	Forecasting	✓	✓	Respondent requested to have the capability to provide generation capacity up to 7 days in advance		✓	
4.05	Load Office	Price	✓		Respondent must provide price of dispatch with generation forecast	✓		
5.01	Operations	Alarms	✓	✓	Respondent requested to have the ability to provide DER alarms to the VPP (ie loss of connectivity, loss of communication)		✓	
5.02	Operations	Control	✓		Respondent must have the ability to be enabled and disabled by the VPP	✓		
5.03	Operations	Control	✓	✓	Respondent requested to have the capability to respond to real time control from the VPP			✓
5.04	Operations	Control	✓	✓	Respondent must enable control of DER assets from the VPP on a 15 second interval	✓		
5.05	Operations	Data interval	✓	✓	Respondent requested to provide consumption and production data at 15 second intervals to the VPP	✓		
5.06	Operations	Event response	✓	✓	Respondent must be able to provide confirmation of opt-out of events to the VPP	✓		
5.07	Operations	Event response	✓	✓	Respondent must be able to receive event notifications from the VPP	✓		

Number	Functional Area	Capability	Aggregator	Direct Connect	Requirement	Must Have	Nice to Have	Future
5.08	Operations	Event response	✓	✓	Respondent must be able to respond to day-ahead events. Respondent shall describe their notification requirements in order to successfully respond to an event, including minimum advanced notice time interval.	✓		
5.09	Operations	Event response	✓	✓	Respondent requested to have the capability to respond to hour-ahead events		✓	
5.10	Operations	Ride-through		✓	Respondent must ensure that inverters ride-through momentary outages according to standard IEEE 1547 -2018, standard CA-21, and standard UL-1741.	✓		
5.11	Operations	SCADA		✓	Respondent shall specify experience in communicating via IEEE 2030.5; Respondent should specify the equipments controlled by the IEEE signal		✓	
5.12	Operations	SCADA		✓	Respondent is required, for direct connect DER, to provide interconnection architecture (building upon included diagrams and including more detail) that shows the connectivity with meter, DER, utility service point, transformer highlighting the energy flow, and the communication standards used to communicate between the devices.	✓		
5.13	Operations	SCADA	✓		Respondent is required, for Aggregated DER, to provide interconnection architecture (building upon included diagrams and including more detail) that shows the connectivity with meter, DER, utility service point, transformer highlighting the energy flow, and the communication standards used to communicate between the devices. Additionally, Respondent is requested to provide integration mechanism and cybersecurity controls around integration to the PSE VPP.	✓		
5.14	Operations	SCADA		✓	Respondent must provide a persistent connection to DER for monitoring, control, and metering purposes to the PSE SCADA system for DER > 25 kVA	✓		
5.15	Operations	SCADA		✓	Respondent requested to provide communication status of the DER monitoring, control, dispatch link to the VPP		✓	
5.16	Operations	SCADA		✓	Respondent must be able to curtail DER when instructed by PSE for DER > 25kVA	✓		
5.17	Operations	SCADA		✓	Respondent is requested to provide digital and analog points for SCADA connected DER > 25 kVA		✓	
5.18	Operations	SCADA	✓	✓	Respondent requested to provide DER status, performance, and configuration data to the VPP		✓	
5.19	Operations	VPP	✓		Respondent shall have the capability to dispatch an event if communication is lost to VPP	✓		
5.20	Operations	VPP	✓		Respondent shall have the capability to issue acknowledgement signals to VPP indicating a certain command or request has been received	✓		

Number	Functional Area	Capability	Aggregator	Direct Connect	Requirement	Must Have	Nice to Have	Future
5.21	Operations	VPP	✓		Respondent shall specificy their methodology for handling multiple events or how different DERs will be bid for a specific program			✓
5.22	Operations	Maintenance	✓	✓	For any response with a PSE ownership option, Respondent shall provide equipment maintenance requirements	✓		
6.01	Planning	Forecast	✓	✓	Respondent shall provide to PSE annually updated 8760 DER forecast and normative load shapes for DERs >=500kVA.	✓		
6.02	Planning	Forecast	✓		Respondent requested to provide regression-based DER growth models for 2 year time period		✓	
6.03	Planning	Forecast	✓		Respondent requested to provide a time-based DER growth and availability model for 2 years		✓	