Avista Corporation

Exhibit H: Demand Reponse Detailed Proposal Information Template

Resource Description Provide responses that best describe the control, hosting, and dispatchability of the resource

What is the resource control method?	
Where is the software hosted?	

Estimated Breakdown of Program Costs by Category

Provide an estimated breakdown of annual program costs for providing capacity by category using the tables below. Provided costs are to be provided in the units described below for each program cost category.

Program Startup Costs	Unit	
2026	($/kW)	
2027	($/kW)	
2028	($/kW)	
2029	($/kW)	
2030	($/kW)	

Program Administrative Costs	Unit	
2026	($/kW-year)	
2027	($/kW-year)	
2028	($/kW-year)	
2029	($/kW-year)	
2030	($/kW-year)	

Program Marketing Costs	Unit	
2026	($/new participant)	
2027	($/new participant)	
2028	($/new participant)	
2029	($/new participant)	
2030	($/new participant)	

Customer Incentive Payments for Events	Unit	
2026	($/kW-event)	
2027	($/kW-event)	
2028	($/kW-event)	
2029	($/kW-event)	
2030	($/kW-event)	

Requirements and Details

Note: not being able to meet the requirements listed below will not automatically eliminate a respondent.
If a requirement cannot be met, provide an explanation in the Vendor Comments section of capabilities.

Functional Area/Ca	Requirement	Priority	Select: Comply or Not Comply	Vendor Comments
Business/Customer/Aggregator	Respondent must have a customer consent and authorization process.	Nice to have		
Business/Co-branding/Aggregator	Respondent must use Avista branding or co-branding when sending notifications to customers for programs with the potential for Avista ownership. For programs that will not be owned by Avista, Avista branding or co-branding is preferred, but if that option is not technically possible please explain alternative.	Must Have		
Business/Customer/Aggregator	Respondent shall specify how event notification will be sent to Avista customers	Must Have		
Business/DR-types/Aggregator	Respondent is requested to be able to leverage different DR sub-types to meet commitments. For example, if a Respondent is intending to aggregate batteries Avista requests the Respondent be able to interface with different types of batteries (ex. Tesla, Generac, etc.)	Nice to have		
Business/Performance/All	Respondents proposing dispatchable resources must provide detailed event performance measurements and perform M&V. Respondent shall specify what M&V and baseline capabilities they have.	Must Have		

Business/Performance/All	Respondent must acknowledge that Avista may implement financial penalties for non-performance of kW / kWh targets	Must Have		
Business/Planned outage/All	Respondent must provide Avista 7 days advanced notice for any planned DR system outage	Must Have		
Business/Planned outage/All	Respondent must provide 7 days advanced notice for any DR system testing	Must Have		
Business/Record maintenance/Aggregator	Respondent must have a protocol for managing customer consent, including for how long verifiable proof of consent is retained.	Nice to have		
Business/Record maintenance/Aggregator	Respondent must have a protocol for managing shared customer information. Example, if a customer leaves the aggregator, how long will their customer information be retained in the aggregator's system.	Must Have		
Business/Record maintenance/Aggregator	Respondent must allow customers to be able to revoke authorization/consent and withdraw from participation	Must Have		
Business/Sale of information/Aggregator	Respondent must not sell any customer information obtained from Avista or from the customer through Avista programs	Must Have		
Business/Compliance/All	Respondent must comply with all applicable laws and regulations. Respondent must ensure that all proposed resources comply with all applicable Avista, applicable state jurisdiction and national safety standards. As applicable, respondent must support Avista's compliance with privacy laws and regulations including WAC 480-100-153 and WAC 480-90-153.	Must Have		
Business/Settlement/All	Respondent must support settlement process with both DR participants and Avista	Must Have		
Engineering/Asset Management/All	Respondent must provide the physical location of the DR resource allowing Avista to match it with the distribution feeder it is connected to. It is assumed and expected that the vendor/supplier of the project will provide the GIS data to Avista in electronic form to be consumed or entered into our CCB CIS and GIS systems.	Must Have		
Engineering/Asset Management/All	Respondent must provide DR nameplate if applicable, resource availability, response information to Avista. This information needs to be provided at individual DR level for DR > 25kVa if applicable and aggregated (at least down to feeder level) for smaller resources.	Must Have		
Engineering/Asset Management/All	Respondent must provide Avista with the ability to send dispatch and control commands to individual DRs > 25 kVa and to geographically aggregated resources (at least down to feeder level) for smaller resources	Must Have		
Engineering/Communications/All	Respondent requested to be capable of communicating using the following as applicable to their solution: -Networks: AMI, LTE cellular, Broadband Respondent requested to describe experience with: -IEEE 2030.5: Describe communications experience with IEEE 2030.5 and specify equipments (i.e. battery controller, etc.) controlled by the IEEE signal -LTE Cellular: What cellular carrier is being proposed and what carriers have you used in the past? Where was this done?	Must Have		
Engineering/Communications/Direct Connect	Respondent requested to validate that the DR can communicate through LTE cellular or fiber connections using real-time data with IEEE 2030.5 or DNP 3.0 communication standards if applicable. Supplier to specify which cellular carrier is being proposed? Please provide what cellular carriers have you used in the past? Where was this done? If applicable, what PCS (Power Control System) and Inverter equipment did you communicate with (i.e., battery controller, inverter, both) ? What diagnostics were used if communication failures occurred?	Must Have		

Engineering/Grid Operation/All	Respondent must adhere to all applicable Avista interconnection processes, comply with all applicable Avista technical specifications and open industry communication standards, including the interconnection requirements set forth in: -Avista's Tariff Schedule 65 - Interconnection with Electric Generators (https://www.myavista.com/about-us/our-rates-and-tariffs/washington-electric/WA_65.pdf) -IEEE 1547-2018: Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power System Interfaces (https://standards.ieee.org/products-services/standards-related/pdf/electric-power-systems.html), and -Avista's Technical Specification and Operating Procedures for Interconnection of Generation Facilities (https://www.myavista.com/about-us/construction-services/transmissions-services)	Must Have		
Engineering/Inverter/All	Respondent must provide DR inverter specifications to Avista for customer battery systems 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	Must Have		
IT/Compliance/Aggregator	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 within six (6) months of contract signing.	Must Have		
IT/Cybersecurity/Aggregator	Respondent must meet industry best practices for security standards set by NIST-IR 7628	Must Have		
IT/Cybersecurity/Aggregator	Respondent must encrypt data in motion using TLS 1.2+	Must Have		
IT/Cybersecurity/Aggregator	Respondent must encrypt data at rest using AES-256 or better	Must Have		
IT/Cybersecurity/Aggregator	Respondent must support standard approaches for network connectivity to the Respondent platform, including firewall rules on both sides, IP restrictions to Avista's external IP range, and VPN connectivity for connections back to Avista OT systems, amongst others. Details will be determined during the design phase of the implementation project	Must Have		
IT/Cybersecurity/Aggregator	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	Must Have		
IT/Cybersecurity/Aggregator	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)	Must Have		
IT/Cybersecurity/All	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	Must Have		
IT/Cybersecurity/All	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	Must Have		
IT/Cybersecurity/All	Respondent shall certify that its systems and products have undergone cyber security testing by leading and independent government sanctioned organizations	Must Have		
IT/Cybersecurity/All	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	Must Have		

IT/Cybersecurity/All	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	Must Have		
IT/Cybersecurity/Aggregator	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	Must Have		
IT/Cybersecurity/Aggregator	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	Must Have		
IT/Cybersecurity/Aggregator	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	Must Have		
IT/Cybersecurity/Aggregator	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	Must Have		
IT/Cybersecurity/Aggregator	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	Must Have		
IT/Cybersecurity/Aggregator	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	Must Have		
IT/Cybersecurity/Aggregator	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	Must Have		
IT/Cybersecurity/Aggregator	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	Must Have		
IT/Cybersecurity/Aggregator	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.	Must Have		

IT/Cybersecurity/Aggregator	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.)	Must Have			
IT/Cybersecurity/Aggregator	Respondent's aggregation system must track and maintain third-party penetration tests	Must Have			
IT/Cybersecurity/Aggregator	Respondent's aggregation system must log all events, including security-related event status with an accurate timestamp.	Must Have			
IT/Cybersecurity/Aggregator	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	Must Have			
IT/Cybersecurity/Aggregator	Respondent's aggregation system must physically or logically separate Avista's data from other of Respondent's customers' data	Must Have			
IT/Cybersecurity/Aggregator	Respondent's aggregation system must secure API access and system connectivity (e.g., API keys, SSH keys)	Must Have			
IT/Cybersecurity/Aggregator	Respondent's aggregation system must support single sign-on using SAML 2.0.	Must Have			
IT/Data Security/All	Respondent must comply with Avista's Security Addendum (Consultant or Hosted) and ensure data security for all relevant usage, metering, settlement, and customer information.	Must Have			
IT/Data Security/Aggregator	Respondent must secure customer data and describe the manner in which this data is secured.	Must Have			
IT/Deployment/Aggregator	Respondent to indicate preferred pattern of solution. Avista's preference is for SaaS solution, but will consider other deployment patterns. If not SaaS, please provide details on architecture.	Nice to Have			
IT/High Availability/Aggregator	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? Is your VEN system capable of meeting a 99.9% availability SLA ?	Must Have			
IT/High Availability/Aggregator	Respondent shall support high availability operations with redundant infrastructure and communications along with continuous automated monitoring, alerting and automated failover	Must Have			
IT/Integration/Aggregator	Please describe best practices for integration of your software to the an utility hosted Virtual Power Plant (VPP).	Nice to Have			
IT/Offshore/Aggregator	Respondent must use datacenters located in the US for SaaS or Cloud	Must Have			
IT/Standards/Aggregator	Supplier / Respondent may be requested that their DR system has the capability to be configured as a OpenADR VEN. Avista desires to have two way real time data communication between it's platform and Aggregator platform using OpenADR 2.0b.	Nice to Have			

IT/Standards/All	Avista requires common interoperability standards be used for BESS solutions. These standards and communication protocols shall be as follows: * IEEE 2030.5 * DNP3.0 * Modbus TCP The above communication protocols shall provide open interoperability and real-time communication to the PCS control system and components which the Smart Inverter is part of the controls equipment. Security with the Smart Inverter shall also include: Avista security requirements, and other agreed to security infrastruction, Digital Certificates and authority, encryption, authentication, authorization, identities, and client identification with the above communications. The requested Standard shall provide a DR and Device Information Data Model to collect, read, and write data to the Smart Inverter. This shall consist of the inverter profile, monitoring power production data (kWH, kW, Delivered, Received, charging ramp rates, alarms, charging schedules, events, over/under voltage, over/under current, Frequency, and all power-voltage imbalances). It shall also provide connect and disconnect functions, High/low voltage ride through, Volt-Var, and PF control functions. Avista requires reporting data capabilities as well with Real and Reactive Power, Volts, Amps, Hz, and PF for all 3 phases + Neutral including Averages.	Nice to Have		
IT/Standards/Aggregator	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 DR assets.	Nice to Have		
IT/Standards/All	Supplier/Respondent must have the ability with their PCS system (Power Control System) for BESS to support both direct and indirect control with rate and charging schedules. This can be managed by an Aggregator using open protocols such as IEEE-2030.5 or DNP 3.0 but must coordinate and integrate with Avista via OpenADR 2.0b as a VEN. If direct control is use by Avista then the supplier shall support Avista standards of IT/OT communications direct to the energy storage controller.	Must Have		
Load Office/Dispatch/All	Supplier/Respondent must have the capability with its DR site controls, communication to aggregators and DR Management System to indicate resource availability, readiness, and equipment states of all components at the DR to dispatch the DR resource.	Must Have		
Load Office/Forecasting/All	Respondent required to have the capability to provide capacity up to 48 hours in advance	Must Have		
Load Office/Forecasting/All	Respondent requested to have the capability to provide capacity up to 7 days in advance	Nice to Have		
Load Office/Price/Aggregator	Respondent must provide price of dispatch with forecast	Must Have		
Operations/Alarms/All	The Supplier/Respondent shall have the ability to provide DR controls which manage all states, alarms and events to Avista with their solution. This shall include watch dog timers for communication, loss of end-points or loss of physical or communication to the site. If the communications is lost the communications shall retry to establish communications. If communications is lost an alert and alarm shall occur. All states and events shall also be managed so that root cause analysis can be determined to what caused the failure.	Nice to Have		
Operations/Control/Aggregator	Respondent must have the ability to be enabled and disabled by Avista	Must Have		
Operations/Control/All	Supplier/ Respondent shall have the capability to respond to real time control from Avista (source) to the DR PCS controls (site). Communications shall have the ability to perform read request, respond and write data including all PCS configuration controller data.	Nice to Have		

Operations/Control/All	Supplier/Respondent must be capable of enabling control of the DER site from Avista through their solution. The interval between control command request and response back to Avista should be less than 15 seconds. Avista ultimately desires to have 5 second or better response time from request to response from the DR.	Nice to Have			
Operations/Data interval/All	Supplier/Respondent must be capable of enabling processes for the DR site to be managed from Avista for all data collection with DR Asset Production Resource data if applicable.	Must Have			
Operations/Event response/All	Respondent's time window for providing full capacity for a dispatched event, which Avista notifies an hour ahead, is how large (within a minute, five mins, etc.…)?	Must Have			
Operations/Event response/All	Respondent must be able to provide confirmation of opt-out of events to Avista	Must Have			
Operations/Event response/All	Respondent must be able to receive event notifications from Avista	Must Have			
Operations/Event response/All	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.	Must Have			
Operations/Event response/All	Respondent requested to have the capability to respond to hour-ahead events	Nice to Have			
Operations/SCADA/Direct Connect	Respondent is required, for direct connect DR, to provide interconnection architecture (building upon included diagrams and including more detail) that shows the connectivity with meter, DR, utility service point, transformer highlighting the energy flow, and the communication standards used to communicate between the devices.	Nice to Have			
Operations/SCADA/Direct Connect	Respondent may be requested to provide other details of communications and DR asset performance with their solution through the interview stage if applicable.	Nice to Have			
Operations/Maintenance/All	For any response with an Avista ownership option, Respondent shall provide equipment maintenance requirements	Must Have			
Planning/Forecast/Aggregator	Respondent requested to provide regression-based DR growth models for 2 year time period	Nice to Have			
Planning/Forecast/Aggregator	Respondent requested to provide a time-based DR growth and availability model for 2 years	Nice to Have			