**Communication Exchange Use Case**

**Description:** (Proposed changes/additions/deletions are in red)

This use cases identifies categories of information to be electronically exchanged between a DER Aggregator and a Distribution Utility to carryout transactions for sales of distribution grid services that fall under state or local jurisdiction. The goal is to identify the cybersecurity protections that may be needed to secure necessary commercial communications and determine if supporting NAESB Business Practice Standards should be considered. The NAESB Base Contract for the Sale and Purchase of Distributed Grid Services from DER Aggregations includes provisions for parties to use secure electronic communications (ECS) to exchange applicable information, such as transaction confirmations and invoices, under the contract.

**Potential Data Exchanges:**

| ***Electronic Communication Exchange*** | ***Data Owner/Controller*** | ***Receiving Party*** | ***Cybersecurity Considerations*** | ***Communication Protocols*** | ***Comments*** |
| --- | --- | --- | --- | --- | --- |
| **Billing and Payment Information Communications** | Distribution Utility | Aggregator | * Confidentiality of sensitive information, including entity identifiers and account information * ~~Disruptive activities (e.g., denial of service)~~ * Availability of communications infrastructure * Integrity of data * Identification and authentication of parties (X.509 v3 certs for authentication) * Authorization of parties * ~~Reliable~~ Validated delivery of message, including a time stamp * Expected duration of cybersecurity protection (e.g., key size) (Need to distinguish between symmetric and asymmetric cryptography. Symmetric may require longer key sizes when quantum computing is a reality. The asymmetric quantum algorithms have been defined by NIST.) | * REQ.21 ESPI * Secure FTP / SSH / HTTPS * HTTPS posts * FTP * EDI / VAN * SD WAN * TLS * IPSec * VPN | * May be variety of implementations that are not consistent * Uniformity and consistency in standards use * Standardized approach creates efficiency and benefits stakeholder |
| Aggregator | Distribution Utility |
| **System/Outage InformationCommunications (this should be included as part of availability requirements)** | ~~Distribution Utility~~ | ~~Aggregator~~ | * ~~Availability of communications infrastructure~~ * ~~Integrity of data~~ * ~~Confidentiality of sensitive information, including entity identifiers and account information~~ * ~~Disruptive activities (e.g., denial of service)~~ * ~~Timeliness and time sensitivity (e.g., timestamps)~~ * ~~Authentication of parties ??~~ * ~~Authorization of parties ??~~ * ~~Reliable delivery of message~~ * ~~Expected duration of cybersecurity protection (e.g., key size). ??~~ | * ~~REQ.21 ESPI~~ * ~~Secure FTP / SSH / HTTPS~~ * ~~HTTPS posts~~ * ~~FTP~~ * ~~EDI / VAN~~ * ~~SD WAN~~ | * ~~Investigate real-time versus non-retail communication differences and cybersecurity needs~~ * ~~Need understanding of business requirements~~ |
| ~~Aggregator~~ | ~~Distribution Utility~~ |
| **Aggregation ~~Information~~ Data Communications** | Aggregator | Distribution Utility | * Availability of communications infrastructure * Integrity of data * Confidentiality of sensitive information, including entity identifiers and account information * Timeliness and time sensitivity (e.g., timestamps) * ~~Disruptive activities (e.g., denial of service)~~ * Identification and authentication of parties (X.509 v3 certs for authentication) * Authorization of parties * ~~Reliable~~ Validated delivery of message, including a time stamp * Expected duration of cybersecurity protection (e.g., key size) (Need to distinguish between symmetric and asymmetric cryptography. Symmetric may require longer key sizes when quantum computing is a reality. The asymmetric quantum algorithms have been defined by NIST.) | * REQ.21 ESPI * Secure FTP / SSH / HTTPS * HTTPS posts * FTP * EDI / VAN * SD WAN * TLS * IPSec * VPN | * Investigate real-time versus non-retail communication differences and cybersecurity needs * Need understanding of business requirements |
| **Aggregation Data Communications** | ~~Aggregator~~ Distribution Utility | ~~Distribution Utility~~ Aggregator | * Availability of communications infrastructure * Integrity of data * Confidentiality of sensitive information, including entity identifiers and account information * Timeliness and time sensitivity (e.g., timestamps) * ~~Disruptive activities (e.g., denial of service)~~ * Identification and authentication of parties (X.509 v3 certs for authentication) * Authorization of parties * Reliable delivery of message (how is this different from data integrity and communications availability?) * Expected duration of cybersecurity protection (e.g., key size) (Need to distinguish between symmetric and asymmetric cryptography. Symmetric may require longer key sizes when quantum computing is a reality. The asymmetric quantum algorithms have been defined by NIST.) | * REQ.21 ESPI * Secure FTP / SSH / HTTPS * HTTPS posts * FTP * EDI / VAN * SD WAN * TLS * IPSec * VPN | * Investigate real-time versus non-retail communication differences and cybersecurity needs * Need understanding of business requirements |