NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

System Requirements Document

Transmission System Information Networks (TSIN) Registry Rewrite

Version 1.0
August 22, 2006

A New Jersey Nonprofit Corporation

Phone 609-452-8060 ■ Fax 609-452-9550 ■ URL www.nerc.com

Revision History

Date	Version	Description	Author
December 13, 2005	0.3	Initial Version	JISWG
February 13, 2006	0.4	Addition of Glossary	JISWG
May 25, 2006	1.0	Changes to address Industry Comment	JISWG

Table of Contents

1 Introduction

This System Requirements Document describes the content and requirements for a central repository (or Registry) of information that the electric industry needs in order to achieve both reliability and commercial interaction. The Registry must incorporate all existing functionality provided by the current TSIN Registry 1.7 and accommodate new industry requirements to support OASIS, NERC e-tag, and other applications. Data residing in the Registry must be authenticated before being published for use.

The Joint Interchange Scheduling Working Group, in cooperation with NERC staff, will oversee the development and implementation of the Registry.

1.1 Requirements Overview

The following is a brief summary of the existing regulatory and industry application requirements for information to be made available through a central registry:

- NAESB Business Practices Standards; Order 638
  - Entity Code
  - Entity DUNS
  - Transmission service attributes
  - Ancillary service attributes
  - Points of Receipt and Delivery (PORs/PODs)
- NAESB Standards and Communications Protocols for Open Access Same Time Information Systems (OASIS); Order 889-B, Order 605
  - OASIS Node Location (URL)
  - OTHER_CURTAILMENT_PRIORITY
  - PROCEDURE_NAME
  - PROCEDURE_LEVEL
  - REQUEST_TYPE
  - SECURITY_TYPE
  - SYSTEM_ATTRIBUTE
- NERC Reliability Standards and the NERC e-tag specification:
  - Tag Service Location (Agent/Authority/Approval/Forwarding URLs)
  - PSE Code
  - CA Code
  - TSP Code
  - SC Code
  - PORs/PODs
  - Sources/Sinks

The current TSIN Registry 1.7 definition accommodates most of these requirements.

The following are new Industry initiatives that could benefit from a central registry of information:

- NERC Functional Model
  - Functions performed by an entity (e.g., BA, TSP, etc.)
  - Certification of entity to perform function(s)
- NAESB Wholesale Electric Quadrant (WEC) Public Key Infrastructure (PKI)
  - Authorized Certification Authorities (CA)
  - Qualified CA Object Identifiers (OIDs)
  - CA Root Certificate Public Key

- e-tag Transaction Path Validation
  - TSP POR/POD Path and Scheduling Entity Association
  - TSP Path Adjacency
  - Source to TSP POR Adjacency
  - TSP POD to Sink Adjacency
- Seams Coordination and IDC Granularity
  - Book of Flowgates
  - AFC coordination data
  - Source/sink zones

These current and future Registry requirements are summarized in the following subsections according to the general functionality that will be required to be supported.

1.1.1 Registry Identifier

The Registry must include identifying information related to its publication, format, and applicability. Such information might include:

- Schema version
- Publication date/time
- Activation date/time

Schema version would reference an agreed to enumeration of revisions to the Registry, or might reference a specific XSD, if the Registry is published in an XSD form. Publication date would be when this version of the Registry was created and made available. Activation date would be when this specific version of the Registry was to take effect.

Additional information may be included to provide assurance that the Registry is authentic and has not been altered. This information might include a "digest" of the Registry, digitally signed by the registry administrator, such that any corruption or modification of Registry information could be detected. This mechanism will be determined during the detailed design phase of the Registry project.

1.1.2 Entities (Companies)

Entity (Company) registration is one of the key functions of the current Registry and will be extended in the new Registry. Key attributes that are required for entity registration and integration with existing applications include:

- Entity Name
- Entity Location(s)
- Entity Contact(s)
- Entity Identifier(s)
- Entity Code(s)
- Entity-to-Entity Relationship(s)
- Entity Role(s) (Functions)
- Entity Certification(s)

The Registry must support the registration of the full business entity name and primary place of business. Entity registration must provide for the entry of effective start and end date/times. These dates may be in the future to take effect on, but not before, the specified start date/time.

The ability to support a one-to-many relationship between a given registered entity and each of the attributes for location, contact information, identifiers, codes, affiliations and roles must be provided.

Entity location information will consist of a street address for the entity. Contact information will be classified by the contact type. Contact types will be defined in the Registry by the registry administrator.

For example, there may be administrative contacts, technical support contacts, emergency (24x7) contacts, etc. Contact types will be associated with the specific entity roles. The registry administrator may require that certain contact types be populated. The Registry implementation should enforce this requirement as part of automated data validation and constraint verification. Entity identifier would minimally support the registration of the entity's DUNS number required by the OASIS application. Various other industry recognized standard identifiers may be used in the future. The system design should anticipate the need to accommodate additional identifiers.

Entity code information is important to both the OASIS and the e-tag specifications. OASIS codes are the entity code itself. E-tag codes are the registered tag PSE codes currently consisting of the entity code with an appended tag desk code. (Note for additional description on entity codes)Current requirements must be supported, but other restrictions should be relaxed with the only requirement that entity code must be unique at any given point in time, and once assigned should have limited ability to be re-used by another entity, e.g., only in the case of an acquisition/merger or divestiture. The ability to require and enforce an authorized third party (i.e. Registry administrator or designee)[1] approval of registered entity codes must be included in the Registry.

Entity-to-entity relationships must be supported to provide a trace of entity acquisitions/mergers and or divestitures, as well as inter-entity affiliations. Entity affiliations are required by the OASIS application to identify the merchant affiliates of each transmission provider.

Entity roles or functions must be extended from the limited set supported by the current TSIN Registry 1.7 to support the registration of entities performing the various functions defined by the NERC Functional Model. Registration of an entity role/function should provide the ability for third party (i.e. Registry administrator or designee) approval or "certification" that the entity has in fact been qualified to perform that function. The ability to enable or disable the requirement for third party approval of a registered entity role is required. (Flag: "or information" will be added where appropriate.) The following are the initial set of entity roles to be considered in the Registry:

- Current O/SE (Operations) associated entity roles
  - RA — Reliability Authority/Coordinator (formerly Security Coordinator)
  - BA — Balancing Authority (formerly Control Area)
  - MO — Market Operator
  - TO — Transmission Operator
  - TSP — Transmission Service Provider
- Current TC/PSE (Merchant) associated entity roles
  - TC — Transmission Customer (i.e., OASIS customer code)
  - PSE — Purchasing Selling Entity (i.e., Tagging desk code)
  - LSE — Load Serving Entity (implies PSE)
  - GPE — Generation Providing Entity (implies PSE)
- Additional Entity Roles
  - Registry Administrator
  - ASP — Application Service Provider
  - PKICA — PKI Certification Authority
  - PKIPA — PKI Policy Authority
  - ERO — Electric Reliability Organization
  - RRO — Regional Reliability Organization
  - IMM — Independent Market Monitor
  - Other

[1] Note that "third party" identification depends on the type of information being registered.

The distinction of an entity being either an O/SE or TC/PSE should be retained for backward compatibility only. The key registration requirement is that an entity may register one or more entity codes. Each of those entity codes may be associated with one or more entity roles. The combination of entity code and entity role determines the context within certain actions that may be performed or granted. For example, in e-tagging, the entity code allowed to appear in association with a source must be designated as having the entity role of GPE to be valid in the context of that tag.

1.1.3 Clients (Users)

The Registry must support at least a rudimentary set of client/user registration functions to minimally identify who is able to access and update the Registry itself. There may also be requirements that certain applications will require the Registry to provide client authentication credentials, e.g., a Tag Agent client certificate registration.

The Registry must also provide a central repository to identify client credentials (e.g., certificate distinguished name, etc…) issued by all the authorized PKI certification authorities. This provides value for application system administrators in that they would not have to provide tools to access all the various PKI certificate repositories to gather this information. [2]The specific information to be retained in The Registry has not been finalized.

Typical information that would be registered for a client would include:

- User's entity
- User name
- User credential(s)

User credentials may include different types of credentials, but would minimally support the x.509 certificate information for one or more certificates issued to that client. The Registry must support a one-to-many relationship between a client and their credentials. Certificate credentials require information from the certificate subject field and certificate issuer field for uniqueness.

1.1.4 Security

The NAESB WEC PKI Certificate Policy and Authorized Certification Authority Accreditation and Certification program will identify those certification authority service providers that are authorized to issue certificates under the NAESB policy.

These certification authority service providers would be registered as an entity with the appropriate role of PKICA. An NAESB Policy Authority would be required to approve/certify these registrations before they are to be "trusted". Who will serve as the Policy Authority has not been determined. The following additional information will be registered for each authorized certification authority:

- Certificate Issuer(s)

The certificate issuers identify an attributes that can be embedded in the certificates issued by this authorized certification authority.

1.1.5 Applications

The Registry must support the registration of specific applications and will require the registration of specific "enumerated" data types or attributes. This requirement is particularly true for OASIS. FERC and NAESB Business Practice Standards enumerate specific transmission and ancillary service attributes and additional data elements that may be "registered" by a transmission provider.

[2] Note that The Registry must support the application validation identified in the electric industry PKI standard (NAESB PKI standards under development).

Applications may also require the identification or location of the server/service provided for the application. OASIS requires the registration of the OASIS node location (URL) for each transmission provider; e-tag requires the registration of the location (URL) for each of the tag services required to be provided by TSPs, CAs, and PSEs.

Each application that requires registration of specific information would appear in the Registry. Application "registration" is envisioned to be part of the base data established by the registry administrator. The specific application attributes would then be registered by either the industry at-large, or specific entities.

1.1.5.1 Application Services

The Registry currently supports registration of various application services by the Uniform Resource Locator (URL) that is used to access that service/application. This includes:

- OASIS Nodes
- Tag Agent Services
- Tag Authority Services
- Tag Approval Services
- Tag Forwarding Services

It is expected that additional services may be registered in the future. Such information might include locations for web services related service URLs, XML schema, WSDL, or UDDI locators.

Application services are envisioned to be registered and maintained by those entities that support/provide the service (e.g., entity type of ASP). Contact information should be provided for each service (e.g., twenty-four hour support, administrative, etc.). Many potential entities could subscribe or use these services. The Registry must support an entity's registration as a user/subscriber to a specific registered service. The Registry will need to support a many-to-many relationship between services and entities.

The Registry must support mapping between application services and the applications they support. The exact nature of this association must recognize the following types of existing relationships:

- Application = e-tag
  - Service = Tag Agent URL
  - Service = Tag Authority URL
  - Service = Tag Approval URL
  - Service = Tag Forwarder URL
- Application = OASIS
  - Service = OASIS URL
- Application = IDC
  - Service = IDC URL

1.1.5.2 Application Attributes

Each application appearing in the Registry may require the definition of unique registered attributes. OASIS requires such information for the transmission service attributes for data elements TS_CLASS, TS_TYPE, SERVICE_INCREMENT, etc. The e-tag application also requires definition of product codes and curtailment priorities.

Capabilities must be provided for a Registry administrator or designee to review and "approve" registration of attributes.

The basic information that is required to be captured related to application attributes would include:

- Application (name or identifier)

- Application Attribute (e.g., TS_CLASS, etc.)
- Application Attribute Value (e.g., FIRM, etc.)
- Registering Entity
- Approval Entity

1.1.6 Topology

The Registry must support the registration and association between physical, commercial, and reliability topology information for use in a variety of applications.

These applications would include:

- Definition of metered areas (balancing areas) controlled by registered balancing authorities (BAs)
- Definition of the metered areas (balancing areas) overseen by registered Reliability authorities/coordinators (RA) (reliability areas)
- Definition of metered areas participating in a centralized market overseen by a registered market operator (MO) (market areas)
- Contract path or e-tag path adjacencies between transmission providers (TSPs), and scheduling entities (SEs)
- Location of commercial service points (PORs, PODs, sources, or sinks) with respect to commercial markets and with respect to reliability related areas (BAs/RAs)
- Mapping of commercial service points to reliability or network modeled elements recognized by reliability applications (e.g., OASIS POR/PODs mapped to IDC flowgates or MMWG elements)

OASIS and e-tag currently require the registration of PORs, PODs, sources, and sinks and the association of Control Areas to Reliability Coordinators. This functionality must be retained and updated to reflect the NERC Functional Model. Registry administrator or designee (e.g., MO, TSP, or BA) approval of registered topology information must be supported.

The most significant immediate extension needed by the industry is a means to validate tag path information through the Registry. The requirements of this particular requirement are discussed in the following subsections along with some of the simpler topological relationships that may be represented in the Registry.

1.1.6.1 Interconnection

The Registry must provide for a hierarchical model of inter-relationships to represent the different topologies, physical, commercial, and/or political that is needed by the industry. Definition of the three major synchronous Interconnections, Western, Eastern, and ERCOT, must be included in the Registry as a foundational element. Creation and maintenance of Interconnection registration may be the responsibility of the registry administrator.

1.1.6.2 Regional Reliability Organization

Regional Reliability Organizations (RROs) may be included in the Registry to identify the overseeing RRO that has responsibility for a reliability area and/or balancing area.

RROs must be registered and associated with a single entity/entity code acting as that RRO. Registration of reliability areas and/or balancing areas as being associated with a given RRO must be supported. The possibility of a given reliability area being associated with more than one RRO must be supported.

1.1.6.3 Reliability Area

Reliability authorities/coordinators must have the ability to define their specific areas of influence. It is assumed that a reliability area would not cross an Interconnection. It may be related to one or more Regional Reliability Organizations and, it would include one or more balancing areas.

Reliability areas must be registered and associated with a single entity/entity code acting as reliability authority. The registry administrator may take on the responsibility for creating and maintaining registration of reliability areas.

1.1.6.4 Market Area

The boundaries of centrally administered markets may be registered. This information may be used by applications such as e-tagging to limit market operator re-dispatch of tagged transactions to only those balancing areas over which they have such authority. It is assumed that a market area can span one or more reliability areas, one or more Regional Reliability Organizations, but will contain, in its entirety, one or more balancing areas. The Registry must support market area registration. Market Operator adjustments would depend on this information.

Market areas must be registered and associated with a single entity/entity code acting as market operator. The registry administrator may take on the responsibility for creating and maintaining registration of market areas.

1.1.6.5 Balancing Area

The balancing area represents a named metered area overseen by a single certified balancing authority. It is assumed that a BA will be within one and only one Interconnection and one and only one market area (if any) and one and only one reliability area. The BA may span one or more Regional Reliability Organizations.

Balancing areas must be registered and associated with a single entity/entity code certified to act as a BA. The registry administrator may take on the responsibility for creating and maintaining registration of balancing areas.

1.1.6.6 Control Zone

The Registry must support the concept of control zones that represent subsets of a balancing area. This supports the potential for increased granularity for system reliability tools when identifying the impact of certain transactions on network elements. At least one control zone must be registered for each balancing area. Where increased model granularity must be recognized, the ability to associate multiple control zones within a single balancing area must be supported (e.g., PJM as balancing area has control zones of CE, AEP, DPL, etc.).

Control zones may be registered by the single entity/entity code certified to act as the BA that contains that control zone. Definition of control zones must be coordinated by those responsible for wide-area network modeling and maintenance of reliability tools that rely on those models. The registry administrator may take on the responsibility for creating and maintaining registration of control zones.

1.1.6.7 Service Points

The current Registry provides for transmission service provider definition of the commercial PORs and PODs used in OASIS. The Registry also provides for PSEs to define e-tag sources (for GPEs) and sinks (for LSEs). This functionality must be retained. However, a more rigorous process for Registry administrator or designee validation of these service point registrations should be instituted.

When registered, the relationship of each commercial service point to the entity making the registration (e.g., TSP for PORs/PODs), and the various “areas” in which the point is located (e.g., Interconnection, reliability area, market area, balancing areas, etc.) such that all the operational entities that may be involved with commercial or reliability issues associated with that point may be identified.

The Registry must provide for the association of a given source or sink with one and only one control zone. The Registry must also provide for the association of which registered entity/entity code of type

GPE may reference a given source and the association of which registered entity/entity code of type LSE may reference a given sink.

Currently, GPEs/LSEs are allowed to submit registrations of sources and/or sinks with approval granted to the referenced BA and/or MO. Since this information is so integrally tied into market and reliability processes and systems, the industry may elect to change the registration procedure to be controlled by operational entities rather than merchant entities. The Registry implementation must be flexible to allow control over source/sink registration by PSEs with approval of a balancing authority or market operator or limit registration to only be submitted and maintained by the BA/MO.

1.1.6.8 Paths

The Registry must support the definition of commercial transmission paths by each entity/entity code registered as a TSP. A path is defined as a valid POR and POD pair that may be scheduled with a designated scheduling entity (SE). There must be no restriction that a given named path may be associated with multiple POR/POD pairs, or that a given POR/POD pair may be associated with multiple paths. The combination of TSP, POR, POD, Scheduling Entity, and path name must be unique. Registration of paths and their associated POR/POD pair and Scheduling Entity must support the OASIS S&CP path naming convention.

For TSPs that have many Interconnections, physical and/or contractual, with other TSPs, the number of unique POR/POD pairs that represent valid commercial paths within their systems can be voluminous. The Registry implementation must provide for the ability to define paths using wildcard designations or other user interface or application programming interface structures to provide for an efficient mechanism to manage this large volume of information. The internal representation of path information in the Registry, however, may be very explicit to simplify programmatic use of the information.

That is, a TSP that has ten POR/PODs, and all possible pair-wise combinations of POR and POD are legitimate scheduling paths with a given Scheduling Entity, must be able to register and manage this information in an efficient manner even though the actual Registry may contain the explicit definition of the paths that result from those ten POR/PODs.

1.1.6.9 Path Adjacency

The Registry must support the ability to identify adjacencies between TSPs and Scheduling Entities'. This information is intended to be used specifically for e-tag scheduling path validations. Many constructs could be used to register and identify these adjacencies. The most direct method would be to identify which specific TSP registered paths (POR. POD, Scheduling Entity, Path combination) are adjacent to both any upstream TSP (i.e., TSP POR adjacent to upstream POD) and downstream TSP (i.e., TSP POD adjacent to downstream POR).

The Registry must recognize the many permutations of physical and contractual adjacencies that must be supported in order to accurately represent valid scheduling paths between TSPs and controlled by Scheduling Entities'. As with path definitions, this data can be voluminous and shorthand, efficient methods to enter and maintain the necessary associations must be implemented.

1.1.6.10 Source-POR Adjacency

The current source and POR registration must be extended to provide a mechanism to register the commercial relationship between a source resource and the TSP PORs over-which transmission service must be secured to schedule energy. Alternatively, source to path adjacency could be used to define this relationship more explicitly.

1.1.6.11 POD-Sink Adjacency

The current sink and POD registration must be extended to provide a mechanism to register the commercial relationship between a sink resource and the TSP PODs over-which transmission service

must be secured to schedule energy. Alternatively, source to path adjacency could be used to define this relationship more explicitly.

1.1.7 Reference Documents

The following reference documents provide additional information on the various functional requirements that must be met by the TSIN Registry 1.7.

- Standards and Communication Protocols for Open Access Same Time Information System (OASIS), Version 1.4, FERC Docket No. RM95-9-014.
- Open Access Same-Time Information System and Standards of Conduct, Order No. 638, FERC Docket No. RM95-9-0014.
- Master Registry Definition Document, Version 1.7, NERC.
- Electronic Tagging — Functional Specifications, Version 1.7.095, NERC.
- Electronic Tagging — Registry Definition, Version 1.7.04, NERC.
- NAESB WEC PKI Standard and Certificate Policy; pending approval of fNEASB.
- Registry Technical Specification, Version 2.0.3, NERC.

1.2 Glossary

Any definitions not contained herein may be found in the NERC Glossary of Terms Used in Reliability Standards (April 1, 2005), the NAESB WEQ Glossary, or FERC Glossary.

Application Programming Interface (API) – A language and message format used by an application program to communicate with the operating system or some other control program such as a database management system (DBMS) or communications protocol.

Application Service Provider (ASP) – An **ASP** is a business that provides computer-based services to customers over a network. The most limited sense of this business is that of providing access to a particular application program (such as medical billing) using a standard protocol such as HTTP.

Balancing Authority (BA) – The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.

Certification Authority (CA) – The organization that issues and manages certificates.

Certificate issuer – The Certification Authority

Certificate OID – Each certificate policy is uniquely represented by an "object identifier" (OID) which is a numeric string that is contained in a field of each certificate that is issued according to a given certificate policy. In order to ensure interoperability and uniqueness of each OID, these are registered with recognized international bodies according to a structure defined in X.208 from the International Telecommunications Union (ITU) (the structure can be examined at http://www.alvestrand.no/objectid/top.html).

Client certificate – X.509 Digital Certificate received (by a “client”) from a Certification Authority.

Digital certificate – The digital equivalent of an ID card used in conjunction with a public key encryption system. Also called "digital IDs," digital certificates are issued by a trusted third party known as a "certification authority" (CA) such as VeriSign (www.verisign.com) and Thawte (www.thawte.com). The CA verifies that a public key belongs to a specific company or individual (the "subject"), and the validation process it goes through to determine if the subject is who it claims to be depends on the level of certification and the CA itself.

Data Universal Numbering System®(DUNS) – The **Data Universal Numbering System®**, abbreviated as **D-U-N-S®** , is a system developed and regulated by Dun & Bradstreet (D&B) which

assigns a unique numeric identifier to a single business entity. This numeric identifier is commonly referred to as a D-U-N-S number.

Electric Reliability Organization – Responsible organization authorized under the Federal Power Act to develop and enforce Reliability Standards that provide for an adequate level of reliability of the Bulk-Power System.

Entity affiliate – An organization that is associated with another organization as a subordinate, subsidiary, or member.

Entity predecessor – The organization that preceded the current organization. This typically follows a reorganization, merger, acquisition, or divestiture.

Extensible Markup Language (XML) – A metalanguage written in SGML that allows one to design a markup language, used to allow for the easy interchange of documents on the World Wide Web.

Generation Providing Entity (GPE) – Merchant selling energy from owned, affiliated, or contractually bound generation.

Global attribute – Industry defined attributes such as TS_CLASS FIRM.

Independent market monitor – An organization that is not affiliated with any electric industry Market Participant, Market Operator, or Transmission Service Provider that is responsible for monitoring market activities.

Load-Serving Entity (LSE) – Secures energy and transmission service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.

Local attribute – An attribute defined by the TSP such as SERVICE_INCREMENT SEASONAL.

Market Operator(MO) – Entities registered as market operators and serving as either source or sink for a TRANSACTION may exercise such functions in order to indicate correct flow based on market clearing.

PKI certification authority (PKICA) – In cryptography, a certificate authority or certification authority (CA) is an entity which issues digital certificates for use by other parties. It is an example of a trusted third party. CA's are characteristic of many public key infrastructure (PKI) schemes.

Point Of Delivery (POD) – A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction leaves or a Load-Serving Entity receives its energy.

Point Of A Receipt (POR) – A location that the Transmission Service Provider specifies on its transmission system where an Interchange Transaction enters or a Generator delivers its output.

Policy Authority – The entity that has ultimate responsibility for approving the Certificate Policy used to govern the issuance, management and usage of a specified set of digital certificates

Reliability Authority/Coordinator (RA/RC) – The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator’s vision.

Root CA identifier – Unique OID of the Root CA.

Root CA Public key – The pubic key of the Root Certificate Authority X.509 digital certificate that is provided to the Root CA’s subordinate Certificate Authorities.

Root Certificate – In cryptography and computer security, a **Root Certificate** is an unsigned public key certificate, or a self-signed certificate, and is part of a public key infrastructure scheme. The most common commercial variety is based on the ISO X.509 standard. Normally an X.509 certificate includes a digital signature from a certification authority (CA) which vouches for correctness of the data contained in a certificate.

Scheduling Entity (SE) – An entity responsible for approving and implementing Interchange Schedules.

Transmission Operator (TO) – The entity responsible for the reliability of its "local" transmission system, and that operates or directs the operations of the transmission facilities.

Transmission Service Provider (TSP) – The entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.

Unaffiliated entity – Any of two or more organizations that are not associated with each other as a subordinate, subsidiary, or member.

Uniform Resource Locator (URL) – The address that defines the route to a file on an Internet server (Web server, FTP server, mail server, etc.). URLs are typed into a Web browser to access Web pages and files, and URLs are embedded within the pages themselves as hypertext links.

2 Registry Processes and Procedures

2.1 General Concepts

Due to the industry's heavy reliance on the existing TSIN Registry 1.7 in the e-tag application, implementation of a new Registry should consider it essential to maintain full backward compatibility to re-create the existing Registry schema and publication mechanisms (Access MDB and CSV files).

Every Registry entry must also support tracking of the following key information:

- Creation Date – date/time the entry was first inserted into the Registry
- Activation Date – date/time the entry becomes active or in use
- Deactivation Date – date/time the entry is no longer to be used
- Last Update – date/time the registry was last updated
- Modified By – identifying information for the person or software application that created/modified the Registry entry

The registry design must also consider providing a general mechanism to audit Registry changes and reconstruct the Registry at a given point in time. Consideration should be given to a uniform database table update process whereby the record to be updated is marked as 'deactivated' and the updated data inserted as a new record with a corresponding 'activation' date/time.

2.2 Registry Administrator Procedures

2.2.1 Administrator Base Data

Certain base data information will need to be established and maintained by the registry administrator. Such information might include:

- Entity Identifier Types — DUNS, etc.
- Entity Role Types — BA, LSE, ASP, etc.
- Client Role Types — Entity Admin, Registry Admin, etc.
- Contact Types — Administrative, 24-Hour, Technical Support, etc.
- Applications — OASIS, e-tag, etc.
- Application Service (Server) Types — OASIS, Tag Agent, etc.
- Application Attributes — TS_CLASS, SECURITY_TYPE, etc.
- Interconnections — Eastern, Western, ERCOT
- Regions — MAAC, WECC, etc.
- Service Point Role Types — Source, POD, etc.

Additions, updates, and deletions (deactivation) of records within these tables will be restricted to the registry administrator only. The user interface will allow the registry administrator to view, add, and modify records in these tables as necessary. General access to these tables by all other users will be restricted to read only access. Addition of new information in these tables may be initiated by industry participants through an off-line administrative procedure with appropriate "checks and balances" as established by the registry administrator.

Until a PKI policy authority is identified, the registry administrator, under the direction of the NAESB Certificate Policy, will assume sole responsibility for maintaining the content of the following Cyber-Security related base data:

- Certificate Root – Authorized Certification Authority (CA) Root Certificate
- Certificate Policy – Authorized CA OID(s) for certificates issued
- Certificate Issuer – Distinguished name of Authorized CA Issuing Authority(ies)

2.2.2 Full Registry Publication

The registry administrator is responsible for the periodic publication of the full Registry and potentially selected subsets of that registry. The publication of the registry requires taking a snapshot of the Registry at the time indicated in the Registry Version and Publication Date field. The Registry will then be made available for download in the following formats:

- XML via defined web services using SOAP encapsulation and XML schema(s)

The current publication frequency is:

- Registry published daily at midnight.
- Published Registry's activation date set for midnight twenty-four hours after publication.

The new Registry may need to be published more frequently than the current TSIN Registry. This publication schedule may change in the future dependent on how frequently Registry data is modified.

The Registry may be cleaned of all spurious data corrections made between publications due to mistakes, typos, etc., made during the registration process. The registry administrator may archive all records whose creation date AND deactivation date is greater than the last publication date but less than the publication date (i.e., records that never became active in the Registry).

Rather than periodic publication of the Registry on a fixed schedule, the registry administrator may elect to only publish a new Registry when information has changed since it was last published. The ability for any registered entity/entity code to subscribe for notification of the availability of a new Registry must be provided.

2.2.3 V1.7 Registry Publication — Backward Compatibility

The implementation of the new Registry requires 100% backward compatibility with the existing NERC V1.7 Registry publication methods to minimize the immediate impact on existing production applications that rely on the Registry. The Registry Detailed Design Specification must describe the mechanism for reconstituting the contents of the various V1.7 Registry table records from the new Registry's schema.

Coincident with the publication of the full Registry, automated procedures will be executed to convert that Registry information into the V1.7 Registry Microsoft Access database ".mdb" file and to generate all associated Comma Separated Values CSV files. The V1.7 Registry database and "CSV" files will be published on the same frequency as the full Registry. The registry administrator will also execute and/or review the results of a record-by-record comparison of the new V1.7 Registry with that published previously to determine if there are any obvious errors in the conversion process.

Note that in retaining backward compatibility, features added specifically for the new Registry (e.g., PKI certificate information) will not be accessible through the V1.7 * ".mdb" or * ".csv" files. Applications will need to be updated to read the new V2.0 Registry information published in XML format available via web services, since the backwards compatibility will only be maintained for 18 months from the go live date of the new Registry.

2.2.4 Tag Registry Publication

The NERC e-tagging specification requires only a subset of pertinent information from the full Registry. Coincident with the publication of the full Registry, a subset of Registry information may be made available for use by tagging application service providers. This data will be provided in CSV file format consistent with the currently provided e-Tag CSV Registry data for backwards compatibility for 18 months. During this time the users of this data will need to convert over to the new V2.0 Registry information published in XML format available via web services.

2.2.5 OASIS Registry Publication

The OASIS application requires only a subset of pertinent information from the full Registry. Coincident with the publication of the full Registry, a subset of Registry information may be made available for use by OASIS application service providers. This data will be provided in CSV file format consistent with the currently provided OASIS version 1.4 CSV Registry data for backwards compatibility for 18 months. During this time the users of this data will need to convert over to the new V2.0 Registry information published in XML format available via web services.

2.3 Entity — Initial Registration

The following information must be collected as part of the initial registration process for a new entity:

- User — information regarding the individual submitting the initial entity registration; this information will populate an initial client associated with the entity and assigned the role of "Entity Administrator" (See Client – Initial Registration);
- Entity — information including official/legal entity name, business address, etc.;
- Entity Code — one or more short acronyms to be associated with the entity with one or more entity role(s) can be assigned to each entity code;
- Entity Identifier — one or more industry recognized legal entity identifiers (e.g., DUNS) if any entity code assigned the role of TSP (transmission service provider), or TC (transmission customer). Additional validations/requirements may depend on other roles assigned to the entity ;(Determined at a later date.)
- Entity Affiliates — zero or more identifications of any active, registered entities to which the new entity is affiliated;
- Entity Predecessor — zero or more associations to existing registered entities, which gave rise to formation of the new entity (e.g., merger, acquisition, divestiture, etc.).

The following subsections describe specific requirements relative to the validation and processing of the entity's initial registration.

2.3.1 Entity

The entity's official/legal name must be verified for uniqueness. Desired "activation date" will default to the Registry Version Activation Date unless an alternative date in the future is supplied by the user (activation date in the past must be flagged as an error).

The activation date will apply to all entity related information records inserted into the Registry during initial registration.

Prior to insertion into the database, a unique master registry identifier must be assigned to the entity being registered. This identifier should be used as the reference identifier in all data registered by that entity. Changes in information such as entity address, etc., should not constitute registration of a new entity. Mechanisms must be supported that allow the transfer of all existing registered information associated with one entity to another through a user request.

2.3.2 Entity Identifier

Entity identifier information submitted must supply both the value for the identifier (e.g., DUNS number) along with the "type" of identifier represented by that value (e.g., "DUNS"). Entity identifier information submitted must be verified for uniqueness. If the entity has attempted to register an entity code with entity role of TSP or TC, the registration information must contain a DUNS number as at least one of their entity identifiers to comply with OASIS registration requirements.

2.3.3 Entity Affiliate

Entity affiliate information, if any, must verify that the affiliated entity is still a valid/active entity. Entities and affiliates must mutually approve the establishment of the relationship.

2.3.4 Entity Predecessor

Entity predecessor information, if any, must verify the validity of the preceding entity registration(s). This information would most likely be presented and submitted from the UI when the user seeks to change an existing registered entity to reflect merger, divestiture, etc. If an existing entity is being replaced, both the predecessor and the successor must agree to this relationship. Predecessor entities do not necessarily have to be active to be associated with a new entity registration.

Along with identifying any predecessor entity, the reason for the change in entity registration must be identified from a set of enumerated reasons including:

- Merger
- Acquisition
- Divestiture
- Reorganization
- Other

2.3.5 Entity Code and Entity Role

At least one entity code must be provided and associated with at least one entity role. The entity role of "unaffiliated entity" (or any of its specific associated roles) must be the only entity role selected and be associated with only a single entity code, i.e., unaffiliated entities are limited to one registered entity code and only the role of "unaffiliated entity".

For backward compatibility, only one entity code may be identified as "O/SE" (operations or security entity) and only one entity code may be identified as "TC/PSE". This entity code represents the V1.7 Registry records in the Entity Registration table, and corresponds to the transmission service provider and transmission customer codes used in the OASIS application (e.g., SELLER and CUSTOMER data elements).

There is no restriction on a given entity registering separate entity codes as both an "O/SE" and "TC/PSE". If not explicitly supplied, the O/SE and/or TC/PSE role will be assumed by default for the first entity code registered that has one or more of the specific O/SE or TC/PSE roles defined as shown below. In addition, the role of PSE will be assumed if either GPE or LSE is selected.

- Current O/SE (Operations) associated entity roles
  - RA — Reliability Authority (formerly Security Coordinator)
  - BA — Balancing Authority (formerly Control Area)
  - MO — Market Operator
  - TOP — Transmission Operator
  - TSP — Transmission Service Provider
  - IA – Interchange Authority
  - GO – Generator Operator
- Current TC/PSE (Merchant) associated entity roles
  - TC — Transmission Customer (i.e., OASIS customer code)
  - PSE — Purchasing Selling Entity (i.e., Tagging desk code)
  - LSE — Load Serving Entity (implies PSE)
  - GPE — Generation Providing Entity (implies PSE)

- Other Functional Model Roles
  - GOP – Generator Operator
  - GO – Generator Owner
  - TO – Transmission Owner
  - PA – Planning Authority
  - TP – Transmission Planner
  - RP – Resource Planner
  - DP – Distribution Provider
- Additional entity roles
  - Registry Administrator
  - ASP — Application Service Provider
  - PKICA — PKI Certification Authority
  - PKIPA — PKI Policy Authority
  - ERO — Electric Reliability Organization
  - RRO — Regional Reliability Organization
  - IMM — Independent Market Monitor
  - Other

Certain restrictions may be required that would make some combinations of entity roles mutually exclusive, i.e., registration of an entity code as both a TSP and PSE may be invalid. All submitted entity codes must be verified for uniqueness. Prior to insertion into the Registry, a unique master registry identifier may be assigned to each of the Entity Codes being registered.

The capability to designate an entity with registration approval rights over the registered entity code/entity role must be provided unless the entity code is registered with any of the entity role of "other". These entities may represent regulatory agencies, universities, consulting groups, etc., that do not have an active merchant or operations role in the electric industry. These entity registrations may be required to designate a Sponsoring Entity (i.e., one with merchant or operations role) that will serve as the registrant's approval entity. Alternatively, the registry administrator may take on this approval role.

Following submission of the registration of an entity code table, as a triggered event or controlled by a batch script procedure, e-mail notifications must be generated to the administrative contact for the entity identified as having approval rights over the entity code registration. Similarly, once an entity code registration has been approved, an e-mail notification must be sent to that entity's administrative contact.

2.3.6 Entity Contact and Entity Code Contact

Registration of contact information must be provided at both the entity level and at the entity code/role level. User information identifying the registrant will be used to create an initial client record associated with the new entity registration. By default, entity contact and entity code contact information create a mapping of this client to the "Administrative" contact for the entity as a whole and for each supplied entity code. The administrative contact will then be responsible for adding additional client records in association with the various contacts, which may be associated with the entity and/or entity code(s) after the initial registration (e.g., 24 hour, Technical Support, etc.).

The following enumerated contact types must be supported:

- Administrative
- Technical
- 24 hour
- Operations — Real-time
- Operations — Day-ahead/pre-schedule
- Customer relations

Not all contact types are required or applicable to each of the various entity roles. Certain contact types may be required by industry standards and practices in association with specific entity roles, and such requirements must be modeled in the Registry.

2.4 Entity — Updates

2.4.1 Entity

Authorized "Entity Administrators" may update information associated with their entity registration. These updates would be to legal business entity name and/or location. Update operation is effected by deactivating the current record and inserting a new record with the updated information activated coincident with the deactivation of the original record. Entity relationships within the various registered objects must key to unique identifiers assigned to the entity and maintained across updates to that entity's registered information and not to specific table record identifiers. This ensures that the Registry contains both current and all historic records associated with the entity. Similar constructs must be applied to all registered objects.

2.4.2 Entity Identifier

New entity identifiers may be registered by authorized entity administrators. Entity identifiers may be updated to reflect corrections or changes in the value of any registered identifier by first deactivating the current registered information and then inserting the updated information into the entity identifier table.

2.4.3 Entity Affiliate

New entity affiliate associations may be inserted by authorized entity administrators. New information will be verified in the same manner as performed for the initial entity registration. Termination of entity affiliate relationship records is accomplished by updating the deactivation date field to reflect when the affiliation was terminated, and may occur at any time without restriction. There is no information that may be updated with respect to entity affiliation.

2.4.4 Entity Predecessor

New entity predecessor associations may be inserted by authorized entity administrators. New information will be verified in the same manner as performed for the initial entity registration. Entity predecessor information is restricted to being registered by the succeeding entity only. Modification of existing information will be accomplished by deactivating the current information and inserting the updated/corrected information.

Deletion of entity predecessor records is accomplished by updating the deactivation date field to reflect when the association between the entities was terminated; this is assumed to mainly be the result of correcting an error on registration.

2.4.5 Entity Code and Entity Role

Updates to entity code information are restricted to the addition or deactivation of entity role information. The entity code itself may only be altered if it has not been approved, and is subject to all uniqueness checks as described for initial entity registration.

New entity code and entity role associations may be submitted for an existing entity. Entity code and entity role information will be validated to insure it passes all validations as described for a new entity registration.

Entity code and entity role associations must support the ability to track approval of that code/role by an authorized third party, i.e., NERC would have approval of entities registering with the balancing authority role as part of their certification program.

See discussion below for restriction on deactivation of entity code or entity role information.

2.4.6 Entity Contact and Entity Code Contact

Contact information associating entity or entity code/role with a client may be added, updated or deactivated. Updating an entity contact or entity code/role contact record to reference a new client must result in deactivation of the existing record and insertion of a new record. Deactivation of an entity contact or entity code contact record may occur at any time without restriction. Insertion of new entity contact or entity code contact records requires only that the associate client record is currently active.

2.4.7 Entity Code Service

Certain entity codes must be mapped to appropriate application services (servers), e.g., PSEs mapped to TagAgent Server, TSP mapped to OASIS Server, etc. The entity administrator may insert, update or deactivate entity code service registrations at anytime without restriction. Update of entity code service associations is accomplished by deactivating the current record and inserting a new entity code service association. Note that the actual service registrations are performed by the entity providing that service.

2.5 Entity – Deactivation

The following subsections describe specific constraints or requirements for deactivation of Entity and related Registry information.

2.5.1 Entity

Deactivation of an entity requires the simultaneous deactivation of all associated records containing the following information/associations:

- Entity affiliate associations
- Entity codes
- Entity contacts
- Entity identifiers
- Clients

Each of these may have further constraints or requirements for deactivation of associated records.

Presence of active records associated with the entity to be deactivated for the following information will block deactivation of the entity. The user/administrator must deactivate these records prior to attempting to deactivate the entity.

- Services (for ASP entities)
- Certificate root (for PKICA entities)
- Certificate issuer (for PKICA entities)

2.5.2 Deactivation of an Entity Code

Entity code requires the simultaneous deactivation of all the following associated registry information:

- Entity roles
- Entity code contacts
- Entity code services
- Entity code service points (for TSP, GPE and LSE entities)
- Entity code paths (for TSP entities)
- All topology related mappings to entity code

Each of these may have further constraints or requirements for deactivation of associated records.

2.5.3 Entity Role

Deactivation of an entity role associated with a given entity code is subject to the following constraints:

- If the entity role to be deactivated is an entity role type of RA or SC, there must be no active reliability area registrations associated with the entity code
- If the entity role to be deactivated is an entity role type of BA or CA, there must be no active balancing area registrations associated with the entity code
- If the entity role to be deactivated is an entity role type of MO, there must be no active market area registrations associated with the entity code
- If the entity role to be deactivated is an entity role type of TSP, there must be no active POR/POD, path or path adjacency registrations associated with the entity code
- If the entity role to be deactivated is an entity role type of PSE, there should be no active source/ sink associated with the entity code
- If the entity role to be deactivated is entity role type of ASP, there must be no active application service registrations associated with the entity code

Any such active registrations referencing an entity role to be deactivated must first be deactivated or assigned to another entity code prior to deactivation of the entity role record.

2.6 Client — Initial Registration

Submission of client information is subject to uniqueness and validation checks. Initial registration of an entity always must result in insertion of an active client record associated with the role of entity administrator. At a minimum, client registration information will be used for Registry Access Control.

Submission of client information may be performed by clients associated with active, approved, registered entities where the client has been assigned the role of user administrator. All information is subject to uniqueness and validation checks. Information required for registration of a client includes designation of name and contact information. Additional information may be submitted to define associated:

- Client certificates (or more generic client credentials)
- Client roles

Contact information associated with entities, entity codes, or services may be modeled as registered clients and mapped to entity, entity code, or service and contact type information, or maintained separately from the client registration.

Prior to insertion into the database, a unique master registry identifier must be assigned to the client being registered.

2.7 Client — Updates

2.7.1 Client Role

Association/disassociation of roles to an active client may occur at anytime without restriction. Now, the only roles envisioned are those required to implement Registry Access Control, including but not limited to:

- Entity administrator
- User administrator

2.8 Client — Deactivation

Deactivation of a client record is subject to the following constraints and/or requirements:

- All active client role records associated with the client to be deactivated must be deactivated simultaneously

If client registrations are used to identify contacts, the following additional constraints are required:

- All active entity contact registrations associated with the client to be deactivated must be deactivated simultaneously
- All active entity code contact records associated with the client to be deactivated must be deactivated simultaneously
- All active service contact records associated with the client to be deactivated must be deactivated simultaneously

2.9 Application — Initial Registration

The only application related registration information accepted from external entities is registered Application Services and Application Attribute Values. All other application related registry information is maintained by the registry administrator. This includes the identification of the registered applications and associated application service types (e.g., e-tag Tag Agent Service).

2.9.1 Application Services

Submission of service registration information may be performed by clients of an active, approved registered entity with at least one entity code assigned the role of ASP. All information is subject to uniqueness and validation checks.

Information required for registration of a service includes designation of the service type, URI, and a description. Additional information may be submitted to identify one or more service contact information (e.g., technical support, etc.).

Prior to insertion into the database, a unique master registry identifier must be assigned to the service being registered.

2.9.2 Application Attribute Value

Submission of application attribute value information includes the name of the application as defined in the application base data and the particular data element whose value is being registered as defined in the application attribute name base data.

Currently, submissions of application attribute values are only allowed for the OASIS application and may only be submitted by clients whose parent entity contains an active, approved entity code designated with the entity role of TSP.

The application attribute base data defines whether the application attribute value is subject to approval by another entity and which entity is granted approval rights. If approval is not required, the registry administrator will be the approval entity and the registered value will be automatically approved on insertion into the database.

If approval is required, an e-mail notification must be sent to the administrative contact(s) associated with the approval entity. Once that entity updates the record to indicate approval (or disapproval), an e-mail notification will be sent to the registering entity's administrative contact.

Attributes that require approval must be considered ‘global’ attributes that any TSP may reference or use (e.g. TS_CLASS). Attributes not requiring approval must be considered ‘local’ and apply only to the entity that registered that attribute value.

2.10 Application — Updates

2.10.1 Application Service

Authorized ASP entity administrators may update information associated with their service registrations. These updates would be to service URL or description. Update operation is effected by deactivating the current registration and inserting a new record with the updated information.

2.10.2 Entity Code Service

Addition, update or deactivation of registered entity code service associations are controlled by the entity owning that entity code. Activation of new records or deactivation of existing records may occur at any time without restriction. Update of existing records, i.e., changing service association, must be accomplished by deactivating the current record and inserting a new record with the updated information.

2.10.3 Application Service Contact

Contact information associated with a service may be added, updated or deactivated. Updating a service contact registration will result in deactivation of the existing record and insertion of a new record. Deactivation of a registered service contact may occur at any time without restriction.

2.10.4 Application Attribute Values

Once registered, OASIS application attribute value registrations may only be deactivated by the entity that approved the registration. The registering entity may update the value and associated description fields prior to approval of the registration only, i.e., for correction of errors or on the advice of the approval entity. Once approved, no updates will be allowed except for deactivation by the approval entity. Transmission and ancillary service attributes are examples of OASIS attributes, which require oversight and approval. Once these attributes are registered by one TSP, they must be re-useable by any other TSP. This would prevent unnecessary duplication of effort and eliminate a possible source of inconsistencies.

Certain OASIS application attributes are private to the TSP (local), such as REDUCTION_TYPE, SYSTEM_ATTRIBUTE, etc. No Registry administrator or designee approval is required for these attributes, and they may be updated by the entity that registered the attribute.

2.11 Application — Deactivation

2.11.1 Application Service

Deactivation of a registered application service is subject to the following constraints and requirements:

- All application service contact records associated with the service to be deactivated must be deactivated simultaneously
- Any active entity code service associations to the service to be deactivated must block deactivation of the service

The Registry may support the registration of application services, which are ‘voluntary’ in nature. These services may be registered, updated and deactivated at will by the registering entity without affecting operations of any other services.

2.11.2 Application Attribute Value

Registered application attribute value records may be deactivated as described in the update process at any time. Global attributes must be deactivated by the entity that approved the registration; local attribute values may be deactivated by the registering entity.

2.12 Topology — Initial Registration

The following subsections outline the basic processes required for initial registration of topology information.

2.12.1 Interconnection

The registry administrator will assume responsibility for establishing the base definitions for the electrical system synchronous interconnections.

2.12.2 Regional Reliability Organization

The registry administrator will assume responsibility for establishing the base definitions for the Regional Reliability Organizations at the direction of NERC.

2.12.3 Reliability Area

A registered and approved (by NERC) reliability authority must have the ability to register a reliability area. Key attributes are:

- Area name
- Association to the Reliability Authority
- Association to one or more Balancing Areas

The entity that approved the registration of the reliability authority must also have the rights to define the reliability area on the RAs behalf.

The registry administrator at the direction of NERC will most likely establish the initial set of Reliability authorities/coordinators and areas.

2.12.4 Market Area

A registered and approved market operator must have the ability to register a market area. Key attributes are:

- Area name
- Association to the market operator
- Association to one or more balancing areas

The entity that approved the registration of the market operator must also have the rights to define the market area on the MOs behalf.

A validation rule must be enforced that a given balancing area may not appear in multiple market areas.

2.12.5 Balancing Area

A registered and approved (by NERC) balancing authority must have the ability to register a balancing area. Key attributes are:

- Area name
- Association to the balancing authority
- Association to one or more control zones
- Association to the market area (if any)
- Association to one reliability areas
- Association to one or more Regional Reliability Organization (optional)

The entity that approved the registration of the balancing authority must also have the rights to define the balancing area on the BAs behalf.

The registry administrator at the direction of NERC will most likely establish the initial set of balancing authorities and areas.

2.12.6 Control Zone

Control zones are subsets of balancing areas that allow reliability tools, such as IDC, have increased granularity over transaction impacts than for the balancing area as a whole. Control zone definitions require coordination between NERC, network modeling groups, reliability tool developers, etc.

A registered and approved (by NERC) balancing authority must have the ability to register a control zone. By default, each balancing area must have one control zone registered whose name is identical to the parent balancing area. Key attributes are:

- Zone name
- Association to the balancing area
- Association to one or more service points (sources/sinks)

The entity that approved the registration of the balancing authority must also have the rights to define the control zone on the BAs behalf.

The registry administrator, at the direction of NERC, will most likely establish the initial set of balancing areas and control zones.

2.12.7 Service Points

NAESB Business Practice Standards require registration of PORs and PODs by TSPs. Key attributes include:

- Point name
- Role (POR and/or POD)
- Association to the transmission service provider

No approval should be required for an entity code with role of TSP to register PORs and PODs.

Registration of sources and sinks is currently handled by purchasing selling entities with approval granted by the balancing authority. Provisions must be made to allow sources and sinks to be registered directly by the balancing authority or market operator (for BAs within their market) in coordination with the PSE(s). Key attributes include:

- Point name
- Role (source and/or sink)
- Association to one or more purchasing selling entity
- Association to the control zone

PSEs associated with a source point must have the additional entity role of GPE; PSEs associated with a sink point must have the additional entity role of LSE.

No approval should be required for an entity code with role of TSP to register PORs and PODs.

2.12.8 Paths

To support tag path validation, TSPs will be required to register all valid commercial transmission service paths and their associated upstream and downstream adjacencies. Key elements of a registered path are:

- Path name
- POR
- POD
- Association to the transmission service provider

- Association to the scheduling entity

Paths are uniquely identified by the combination of all five attributes. Due to the large volume of data this represents for each TSP, the UI forms for registering paths must make efficient use of wildcards.

The OASIS S&CP identifies the following sub-attributes of a standardized path name:

- Region code
- Provider code
- Path code
- Optional code
- Spare code

2.12.9 Adjacencies

Path and source/sink adjacency information must be registered by the TSP. Path adjacency information would indicate:

- Association to upstream path
- Association to downstream path

Source adjacency information would indicate:

- Association to source service point
- Association to downstream path

Sink adjacency information would indicate:

- Association to upstream path
- Association to sink service point

2.13 Topology — Updates

2.13.1 Interconnection

The registry administrator will assume responsibility for performing any updates on the definitions for the electrical system synchronous Interconnections.

2.13.2 Regional Reliability Organization

The registry administrator will assume responsibility for performing any updates on the definitions for the Regional Reliability Organizations at the direction of NERC.

2.13.3 Reliability Area

The reliability authorities or the entity that approved the RAs registration must be able to update the registration of the reliability area. This would be limited to changing the area name, the associations of balancing areas to the reliability area, and assignment of responsibility from the current owning reliability authority to another approved RA.

2.13.4 Market Area

The market operator must be able to update the registration of the market area. This would be limited to changing the area name, the associations of balancing areas to the market area, and assignment of responsibility from the current owning market operator to another approved MO.

2.13.5 Balancing Area

The balancing authorities or the entity that approved the BAs registration must be able to update the registration of the balancing area. This would be limited to changing the area name, the associations of

control zone(s) to the balancing area, and assignment of responsibility from the current owning balancing authority to another approved BA.

2.13.6 Control Zone

The balancing authorities or the entity that approved the BAs registration must be able to update the registration of the control zone. This would be limited to updating the control zone's name, or adding/removing source sink points.

2.13.7 Service Points

TSPs must have the ability to update their POR/POD service point registrations.

BAs and or MOs whose balancing areas are under the control of the MO must have the ability to approve and/or update their source/sink service point registrations.

2.13.8 Paths

TSPs must have the ability to update their path registrations.

2.13.9 Adjacencies

TSPs must have the ability to update the path adjacencies associated with any of the TSPs defined paths. Adjacency registration should be coordinated by the adjacent entities and responsibility delegated to one or the other parties to avoid conflicts.

TSPs must also have the ability to update the path to source/sink adjacencies in coordination with the source/sink balancing authority.

2.14 Topology — Deactivation

2.14.1 Interconnection

The registry administrator will assume responsibility for performing any deactivations of the definitions for the electrical system synchronous Interconnections.

2.14.2 Regional Reliability Organization

The registry administrator will assume responsibility for performing any deactivations of the definitions for the Regional Reliability Organizations at the direction of NERC.

Deactivation of a Regional Reliability Organization will simultaneously deactivate all associations of the RRO to balancing authorities (if any).

2.14.3 Reliability Area

The reliability authority or the entity approving the RA must have the ability to deactivate a reliability area.

Deactivation of a reliability area will simultaneously deactivate all associations of the RA to balancing authorities (if any).

2.14.4 Market Area

The market operator must have the ability to deactivate a market area.

Deactivation of a market area will simultaneously deactivate all associations of the MO to balancing authorities (if any).

2.14.5 Balancing Area

The balancing authorities or the entity that approved the BAs registration must be able to deactivate the registration of the balancing area. Deactivation of the balancing area must simultaneously deactivate the area's associations to registered RROs, reliability areas, and/or market areas. Deactivation must be blocked if there are any active control zones associated with the balancing area.

2.14.6 Control Zone

The balancing authorities or the entity that approved the BAs registration must be able to deactivate the registration of the control zone. Deactivation of the control zone must simultaneously deactivate the zone's associations to register the balancing area. Deactivation must be blocked if there are any active service points associated with the control zone.

2.14.7 Service Points

TSPs must be allowed to deactivate service points. Deactivation of a POR/POD must be blocked if the service point is associated with an active path. . Deactivation of a source/sink must simultaneously deactivate that point's association with the control zone, and any of the point's path adjacencies.

2.14.8 Paths

TSPs must be allowed to deactivate paths. Deactivation of a path must simultaneously deactivate any path adjacencies referencing that path.

2.14.9 Adjacencies

TSPs must be allowed to deactivate path adjacencies at will.

3 User and Registry Interaction

3.1 Browser Interface

The registry shall implement a web browser user interface, allowing users to access and manually register and enter data into the Registry without requiring any special software installations.

3.2 Encryption

The vendor shall allow (or require) the user to use 128 bit SSL.

3.3 Data Access Rights

Users (including programmatic users via API) shall be allowed access to data based on their registered and approved data access rights. Registered users will be allowed only read access rights to data "belonging" to other entities (as described in section 2). Users may only modify, delete, or create data what "belongs" to them. NERC may initiate deletion of invalid data according to the procedures described in section 2.

3.4 Data Validation at Entry

The system shall validate data content and format on data entry wherever possible providing meaningful error messages to the user that will allow the user to determine how to correct the data entry error.

3.5 Data Validation after Entry

The accuracy and validity of registry entries MUST be verified by automated and/or manual processes prior to use by industry participants. Prior to populating the "production" or "active" Registry, updates to the Registry must be confirmed with the appropriate stakeholders. The vendor will work with NERC to determine the appropriate data validation procedures and practices and then optimize the efficiency of this validation.

3.6 Display Consistency

Display formats and function must be consistent across all displays. NERC staff will have final authority on determining if the vendor has met these requirements. If NERC believes that the display is deficient in some manner, then they will provide the vendor with a specific description of what the vendor must change in order to achieve compliance with this requirement.

3.7 Color to Meaning Assignment

If the registry imparts information by color, then this color should be used to mean the same thing on all displays. For example, if the color RED is used to show a data format problem, it must not also be used to highlight data in an "accepted" state.

3.8 Application Programming Interface

The registry will provide the ability to upload data to and download data from the Registry using XML files defined by a published XML schema. Standards consistent with e-tag and WECC's EIDE system shall be used including, SOAP, SMXP, and GMT for time representation. Any XML schemas used in the API must be provided to NERC for public distribution. The XML API shall use 128 bit SSL.

The registry shall also provide registry data in a CSV file format that can be downloaded using https. The SSL required for this download is 128 bit.

For backward compatibility, all methods available today to download the registry data files (Access and CSV formats) shall continue to be supported until this backward compatibility requirement is removed eighteen months from the publication of version 2.0.

3.9 Filtering and Sorting

All user data displays must include filter and sort capability as appropriate.

Columns in displays shall all be able to be sorted in both ascending and descending order by any column (i.e. Source, Sink, POR, POD, etc.).

Displays shall all be able to be filtered based on the values in any meaningful column. Numeric columns shall be filterable based on both absolute and range values. Text columns must be filterable based on partial string matches and exact matches with negation. String filtering shall not be case sensitive. It shall be possible to enter up to 20 text strings for a single field that shall be logically "OR"d together.

Examples:

- PointID=6007,
- NERCID between 511 and 801,
- POR contains NYPD,
- PSE does not contain ENRN,
- POD = MALN OR CAPJ.

4 Hardware and Software Standards

4.1 No Single Point of Failure

The Registry shall be designed so that there are no single points of failure that would result in the Registry being unavailable for greater than one hour. For example, the system could be fully redundant with hot standby/failover functions. This availability requirement extends to the Internet connections, which could also be redundant and through two, independent Internet service providers. All failover, including network failover, must be automatic.

The Registry shall be designed so that there is no single point of failure that would result in the loss of Registry data for greater than one hour. For example, disks could be mirrored and configured in an array with hot spares.

Internet and Registry system redundancy could be satisfied by replication between diverse sites.

4.2 Data Backup and Storage

The Registry data must be backed up at least daily, with data being moved offsite at least weekly. The data must be under the protection of access controls such that no single employee has access to the offsite data storage. Management approval must be required to access the offsite data. There are no historical data storage requirements other than what is needed for disaster recovery.

4.3 Disaster Recovery

The Registry system must be capable of being restored entirely assuming the destruction of the entire registry system. Documentation and procedures must be available that provide for the complete re-installation/re-construction of the Registry hardware, software, and data. The registry must demonstrate that the documentation and procedures are accurate by having NERC staff perform or witness the building of the system from scratch.

4.4 Structured and Coordinated Upgrades

Upgrades/modifications to any component of the Registry that would affect the users must be coordinated with NERC staff and the Registry user community. Upgrades that would change an API must be implemented following a structured implementation plan. This plan must include reasonable periods of at least three weeks for the Registry users to have access to the revised XML schema or whatever else is necessary for the Registry users to implement and test changes in their automated systems. The three-week period must be followed by two weeks of testing with a near-continuous test Registry available for the users to test against. This system must be populated with either test, or actual data.

4.5 Sizing and Performance

The system must be sized and designed so that it provides robust performance for both current and expected usage.

- CPU utilization, averaged over one minute, must be below 20% 95% of the time.
- Disk space utilization at full expected size of the Registry must be 50% or less.
- RAM must be sized sufficiently on all systems (including database servers) so that disk swapping does not exceed 20 pages per minute.

4.5.1 Moderate Activity State

Display call up times and API retrieval times shall be measured when the system is in a *moderate activity state*, carrying out normal functions, while 50 users simultaneously use the interface for normal activities and the API is being used by 50 systems to retrieve data.

Under this loading state:

- User displays call up and display change must not exceed five seconds (excluding internet latency and browser start up times).
- Response to SOAP method calls shall be within five seconds.

4.5.2 Heavy Activity State

Display call up times and API retrieval times shall be measured when the system is in a *heavy activity state*, carrying out *peak* normal functions, while 50 users simultaneously use the interface for normal activities and the API is being used by 150 systems to retrieve data.

Under this loading state:

- User displays call up and display change must not exceed ten seconds (excluding internet latency and browser start up times).
- Response to SOAP method calls shall be within ten seconds.

4.6 Availability

The Registry must be available 99.5% of the time measured over any rolling 30-day period.

4.7 Auditability

The database and registry systems must be auditable. While maintaining records with start/stop dates partially accomplishes this goal, other values need to be tracked for audit purposes. These at a minimum include the user requesting data modifications (inserts, updates, deletes), timestamp, and similar information for the approval/authorization process (NERC staff member/timestamp) for example. XML input documents must also be retained for a configurable number of days.

4.8 Data Integrity

Database and data integrity must be guaranteed. The registry can choose from a number of different tools and procedures to ensure this.

4.9 NERC Cyber Security

The Registry and related components are critical to both operational and commercial sectors of the power industry. As such, NERC classifies the entire system as a Critical Cyber Asset and requires that the registry and any subsequent entities maintaining the Registry comply with applicable NERC CIP standards.

5 Testing

5.1 Structured Test Document

The vendor shall provide a structured test document that tests all functional and performance requirements of the Registry. NERC staff and, at NERC's option, NERC members, may review the document and provide input and corrections which must be incorporated prior to the start of structured testing. The test document must contain numbered sections consistent with the system requirements document so that testers may easily reference required functionality and compare it to rest results.

5.2 Problem Reporting

The vendor shall provide a structured method of reporting, classifying, and tracking problems.

5.2.1 Structured Problem Reporting

Each identified possible problem shall be assigned a unique number and assigned a classification.

5.2.2 Problem Classifications

Problems will be classified as:

- R — Required Functionality (In the System Requirements Document)
- E — Enhancement (Identified as necessary but not in the System Requirements Document)
- B — Bug (Software or Hardware Problem)
- D — Disputed (Agreement cannot be reached)

Problems will further be classified as:

- C — Critical (Required for system to be considered operational)
- H — High priority (Not required but very important)
- M — Medium priority
- L — Low priority

5.3 Factory Acceptance Testing

Factory Acceptance Testing (FAT) shall be conducted on-site. Certain client functions may be tested remotely at the client facilities.

The FAT will consist of both structured testing and unstructured testing. Structured testing will be conducted first.

Unstructured testing will include testing of any required functions in any order at any loading level.

FAT may be conducted several times. Passing FAT is defined as completion of structured and unstructured testing without finding any problems above those classified as low priority.

FAT testing will continue until the NERC staffs or vendor staffs determine that system problems are so severe that no further testing should be done until the problems are corrected.

At completion of FAT testing, if FAT is not passed, the vendor shall correct all problems classified above low priority and another FAT shall be started. This will include re-testing of functions already tested since corrections of problems may cause problems elsewhere in the system.

The vendor will perform a minimal set of FAT and provide results of that testing to NERC before scheduling on site FAT. (Hopefully minimizes travel to on-site location)

5.4 Factory Performance Testing

Factory Performance Testing (FPT) shall be conducted on-site. Certain client functions may be tested remotely at the client facilities.

The FPT will consist of confirmation that the system meets sizing and performance requirements. The vendor will be responsible for loading the system to both the medium and heavy activity state. NERC staff will have ultimate approval and confirmation rights that these activity states are met for the duration of the appropriate performance tests.

Either the vendor or the NERC staff may devise mutually agreeable timing tests (including the use of a stopwatch, performance monitors, or software timers).

5.5 Site Acceptance Testing

Site Acceptance Testing (SAT) shall be conducted at the Registry host facility (ies). Client functions will be tested remotely at the participating client facilities.

SAT is a repeat of FAT with the exception that passing SAT is defined as completion of structured and unstructured testing without finding *any* problems. SAT testing will be open to any NERC member.

5.6 Site Performance Testing

Site Performance Testing (SPT) shall be conducted at the Registry host facility (ies). Certain client functions may be tested remotely at the client facilities.

SPT is a repeat of FPT.

SPT *may be* waived by NERC at their discretion.

6 Documentation

The vendor will be responsible for providing hardware and software documentation. NERC staff shall have approval rights over all documentation provided. The documentation requirements are not waived if the successful vendor provides the Registry service via an application service provider. For example, technical documentation, meeting the requirements described herein, will still be required to be provided to the vendor's own technical staff in this case.

NERC must have the capability to modify and maintain the documentation described in this section or the vendor must maintain it. The intent is that the documentation be kept up to date as changes are made to the Registry system.

Frequently Asked Question (FAQ) documents must also be created and made available online. Provisions must be provided so that these may be maintained on an ongoing basis.

6.1 Technical Documentation

The vendor shall provide NERC with technical documentation describing the hardware architecture and software architecture of the system. The intent of the technical documentation is to allow NERC or their appointees to maintain the system. Since a number of methods are possible for describing the system, including UML, DFD's, etc, there will be no specific requirement in this document as to the form of this documentation. The only requirement is that the intent be met.

6.2 User Documentation

The vendor shall provide the Registry users with user documentation that describes how the client interface is used and all of its possible functions. NERC staff will have approval rights over this documentation.

The documentation must be provided online at the Registry site. Documentation on user registration must be provided online at the NERC Web site.

Documentation must include examples where appropriate.

6.3 Automated Interface Documentation

The vendor shall provide NERC with API documentation that describes, in detail, how users may install and/or utilize the API to the Registry. Any related XML schemas shall be provided to the users so that they may implement their own XML processor independent of any specific vendor solution.

The documentation must be provided online at the Registry site.

Documentation must include examples where appropriate.

7 Training

The vendor will be responsible for providing training courses. NERC staff has approval rights over course content and quality. The vendor must provide courses that meet NERC approval. Training must be presented both in person and online via webex.

These classes may need to be presented in a variety of locations over a number of different days in order to provide access to all Registry users. NERC staff will coordinate training class locations and dates with NERC members and ensure that all NERC members are provided with access to training.

7.1 Technical Training

The vendor shall provide technical training to NERC staff or their appointees in order to assure that they have sufficient knowledge to maintain the system (depending on the final roles) and interact with it (for data confirmation, deletion procedures, etc.).

7.2 User Training

The vendor shall provide training to the Registry users so that at the end of the course, the users are proficient at using the client interface and understand all of its functions.

7.3 API Training

The vendor shall provide technical training to Registry users on the use of the API so that the users, at the end of the course, have a thorough understanding of the interface and how to use it.

7.4 Refresher and ongoing Training

The vendor will provide updated training for system upgrades and changes so that ongoing training may be conducted and available.

8 Post Implementation Requirements

The vendor will be responsible for providing a number of services after implementation of the Registry. All upgrades or modifications to software described in this section must be implemented following requirements outlined in previous sections 4.0, 5.0, 6.0 and 7.0 of this document.

8.1 Problem Reporting and Enhancement Requests

The vendor shall provide a mechanism for both NERC staff and NERC members to report and classify problems and enhancement requests. These will be assigned priority levels by NERC members and staff as follows:

- C — Critical (Required for system to be considered operational)
- H — High priority (Not required but very important)
- M — Medium priority
- L — Low priority

They will also be assigned a classification as follows:

- E — Enhancement
- B — Bug (software or hardware problem)
- D — Disputed (Agreement cannot be reached)

The vendor will allocate resources to correct the identified problems consistent with the priority level assigned as follows:

- C = Immediate mitigation effort required and will be continuous until problem is resolved. Daily status updates from the vendor will be required.
- H = Mitigation efforts must start no later than the next working day and continue during normal working hours until complete. Daily status updates from the vendor will be required.
- M = Mitigation efforts must start within the next ten working days. Vendor will provide an estimate for completion acceptable to NERC Staff. Staff and vendor will work together to prioritize “M” issues. Weekly status updates from the vendor will be required.
- L = Vendor will provide an estimate for completion acceptable to NERC staff. Staff and vendor will work together to prioritize “L” issues. Weekly status updates from the vendor will be required.

8.2 System Upgrades

NERC staff or the vendor, with agreement from NERC staff, may initiate system hardware and/or software upgrades in order to remain current with external vendor support levels (such as the operating system, programming language, or database vendor) or improve performance or reliability.

Responsibilities for staff performing the upgrades need to be established with the vendor in the Registry contract or according to sections 4.0, 5.0, 6.0 and 7.0 of this document as a minimum.

8.3 System Patches

NERC staff and the vendor must establish a method by which critical operating system patches, database system patches, and any other applicable patches required for ensuring system security, implementing bug fixes, and implementing enhancements will be applied. Patches that correct security issues must be applied as soon as possible. Patch application must conform to NERC Cyber Security standards.

8.4 Virus Detection Updates

Virus detection software must be installed and continuously running on the Registry computer systems. NERC staff and the vendor must establish a method by which virus detection software is updated. Updates must be downloaded and applied daily.