J.2 ATTACHMENT A - STATEMENT OF WORK

STATEMENT OF WORK
Specification for North American SynchroPhasor Initiative (NASPI)
May 2008

A. SCOPE OF WORK

The scope of work is limited to the contractor developing, and delivering a specification for a NASPI network (NASPInet) to the Department of Energy's (DOE), National Energy Technology Laboratory (NETL). NAPSInet will be composed of Phasor Gateways, a Data Bus, and a set of common Services, all per the Technical Requirements below. NETL anticipates using the specification delivered by the contractor to implement NASPInet.

B. PROJECT BACKGROUND

NETL is issuing this solicitation for work in support of DOE's Office of Electricity Delivery and Energy Reliability in its mission to lead national efforts to modernize the electric grid, enhance the security and reliability of the energy infrastructure, and facilitate recovery from disruptions to the energy supply.

NASPI's mission is to create a robust, widely available and secure synchronized data (Synchrophasor) measurement infrastructure for the interconnected North American electric power system with associated analysis, monitoring tools for better planning and operation, and with improved reliability. NASPI's ultimate objective is to de-centralize, expand, and standardize the current Synchrophasor infrastructure through the introduction of a NASPI network (NASPInet) that will be composed of Phasor Gateways, a Data Bus, and a set of common Services. A mature NASPInet could involve hundreds of Phasor Gateways and tens of thousands of Phasor Measurement Units, each typically sampling data at 30 times per second.

The NASPI data measurement infrastructure currently involves a number of devices, including, among others, Phasor Measurement Units (PMUs) and Phasor Data Concentrators (PDCs).

PMUs are the source of synchronized phasor data. They are located in the field at a utility substation, receiving station, or generating station. They may be a stand-alone piece of equipment or a function embedded within another type of equipment, such as a microprocessor-based relay or a Disturbance Fault Recorder. All PMUs require a highly accurate clock signal for referencing, a sampling/measurement front end, and some sort of communication link to output synchrophasor data.

Phasor measurement data is typically transmitted continually from a PMU to a PDC. PDCs are generally located in the utility office environment, although they could physically be located in the field. PDCs function as an aggregation point for data from one or more PMUs that is streamed in via communication links to the field. Some local storage may be present along with an administrator interface and possibly some visualization tools. Today's PDCs were not designed to support the scalability and flexibility required to meet NASPI's mission.

Data retrieval and handling devices are installed by North American utilities within their own company guidelines and infrastructure. Data from these devices is currently sent to centralized data gathering locations, e.g. Tennessee Valley Authority, Bonneville Power Administration, where data is then made available for authorized distribution as required.

A utility's portal through which Synchophasor data will be published and subscribed is called a "Phasor Gateway." A Phasor Gateway may handle data directly from a PMU, but most likely will send and receive data from one or more PDCs. A logical entity, called the "Data Bus" will transport data from one Phasor Gateway to another. The Data Bus is one logical entity, but it will be comprised of a large number of components throughout the NASPInet, much like the Internet has network-level routers deployed everywhere the Internet is accessible.

A basic conceptual architectural diagram of the NASPInet that includes PMUs, Phasor Gateways and the Data Bus are shown in Figure 1.

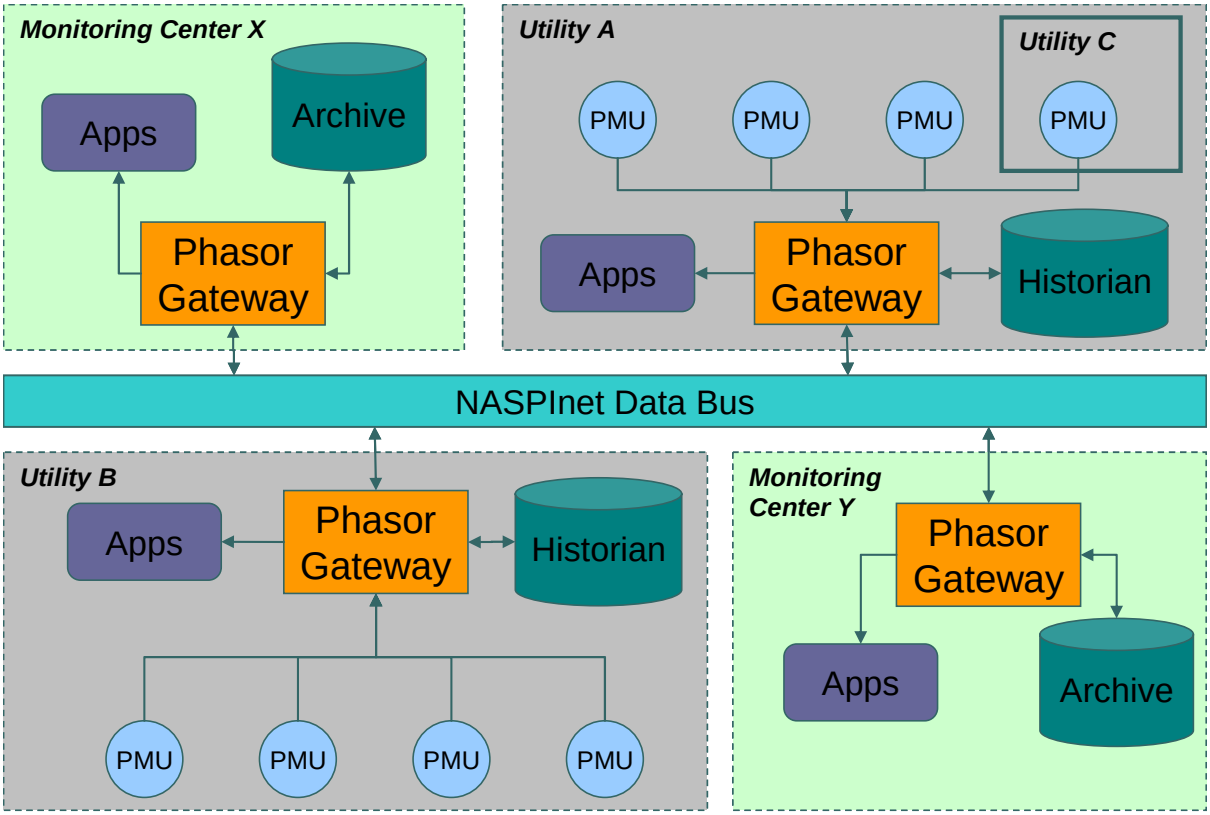

Figure 1. Basic Conceptual NASPInet Architecture

Rest of Page Intentionally Left Blank

The NASPInet will support a hierarchical flow of data and information from utilities, to regional reliability centers, and on to NERC (North American Electric Reliability Corporation), as shown in Figure 2. NERC has been designated by the Federal Energy Regulatory Commission to be the Electricity Reliability to implement mandatory reliability standards for North American utilities. NERC will use a subset of the NASPInet data to perform this function.

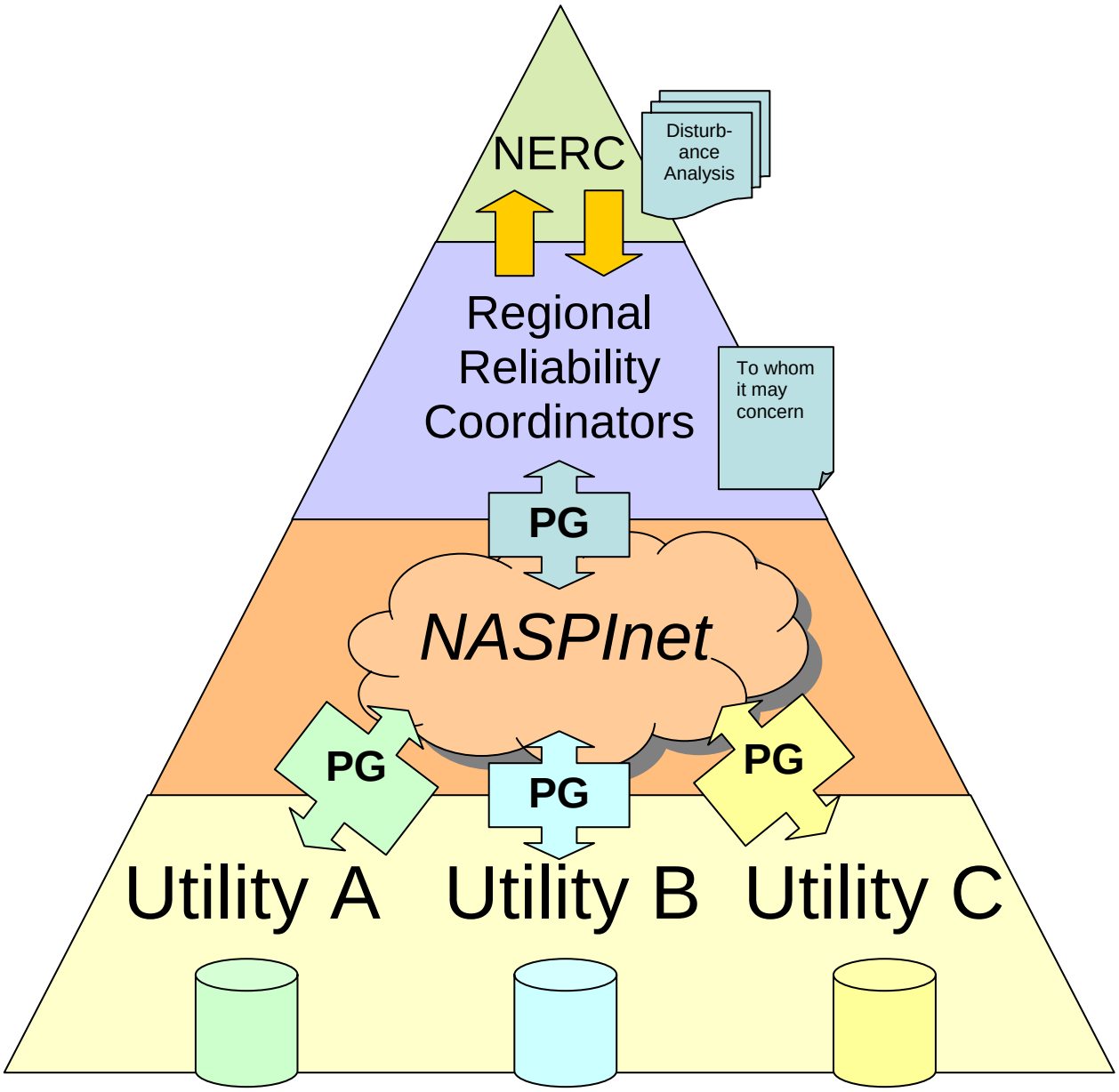

Figure 2. Top-down view of information flow from Utilities to the Regional Reliability Coordinators, and ultimately, on to NERC - all via the NASPInet and associated Phasor Gateways.

Rest of Page Intentionally Left Blank

The main purpose of the Phasor Gateway is as follows:

- Serve as the sole access point to the Data Bus for inter-organizational Synchrophasor traffic
- Administer and disseminate cyber security and access rights
- Monitor and maintain data integrity
- Manage traffic format and timing compatibility issues
- Manage traffic priority according to Service Classes

The main purpose of the Data Bus is as follows:

- Provide connectivity between Phasor Gateways and other elements of the NASPInet
- Provide Quality of Service (QoS) guarantees for reliable and redundant delivery of real-time operational data
- Provide QoS conformance monitoring over NASPInet for Service Classes
- Enforce conformance with cyber security and access control policies

The NASPInet Services support the operation of the NASPInet's Phasor Gateways, Data Bus, Data Bus elements, and NASPInet applications. NASPInet services can be grouped in to the following three general categories:

- Name Services
- Cyber Security Services
- Data and Control Services

C. WORK TO BE PERFORMED

Develop a specification for NASPInet consistent with the following technical requirements. Technical requirements are described in each of four areas:

General Technical Requirements
Phasor Gateway Technical Requirements
Data Bus Technical Requirements
NASPInet Services

General Technical Requirements

The Specification of the NASPInet system-level behavior shall do the following as shown for each topic area:

G1. Equipment and Device Naming conventions

- Provide for guaranteed unique assignments
- Be tolerant of errors and failures
- Describe the necessary attributes of the NASPInet component naming convention(s)

G2. Protocols

- Enumerate which core interoperability protocol(s) will be mandated
- Outline an interoperability framework for extending the core protocols so that a vendor can provide support for additional or new functionality
- Identify all relevant existing protocols with which the NASPInet system must be compatible or interoperable
- Identify whether any new protocols are needed and if so, specify their attributes

G3. Service Classes

- Address the Service Classes identified in Appendix A (located in Section G)
- Address the need for a variety of NASPInet applications that span multiple Service Classes (see Appendix A located in Section G)
- Address the co-existence of multiple Service Classes within the NASPInet
- Enumerate all additional Service Classes included in the Specification

G4. Quality of Service (QoS)

- Address end-to-end QoS issues for both data and control traffic per each Service class
- Address latency, throughput, cyber security strength and any other Quality of Service issues relevant to the specifications for the Phasor Gateways, the Data Bus and its components, the overall NASPInet system and its applications

G5. Cyber Security

- Address cyber security, both globally for the NASPInet and locally for individual NASPInet components (e.g., Phasor Gateway (PG) and Data Bus (DB) elements)
- Address cyber security for both data and control traffic as it flows through the NASPInet
- Address the following cyber security properties: confidentiality, integrity, availability, non-repudiation, and privacy
- Include the cyber security architecture and mechanism(s) by which a positive cyber security model (i.e., a list of allowed behaviors is used instead of a list of disallowed behaviors) will be implemented, managed, and verified
- Address the need to defend against, tolerate (or fail gracefully), and recover from cyber security attacks
- Require that any vendor extension meet or exceed the Specification's cyber security standards
- Provide an architecture for ensuring verifiable end-to-end "chain of custody" for both data and control traffic
- Address cyber security for Phasor Gateways, the Data Bus and its components, the overall NASPInet system and its applications
- Address relevant "chain of custody" issues

G6. Emergency Modes

- Support for emergency mode management and operations
- Identify which emergency modes are required and identify what component operational requirements are in effect when in those modes

G7. Trust Management

- Describe an architecture to both provide and validate trust within a given organization and across organizational boundaries
- Present an architecture for providing multiple layers of trust, flexible deployment, retention, and upgrading trust mechanisms for the lifespan of the data
- Describe a trust management architecture for inter- and intra-organizational trust
- Describe a architecture that provides multiple layers of trust and that supports operational reliability

G8. Open Standards and Vendor Diversity

- Be an open standard that can be implemented by a variety of vendors
- Not adopt proprietary technologies or protocols in order to promote vendor diversity and avoid vendor 'lock-in'
- Provide an extensibility framework within which vendors may exceed the Specification's standards
- Describe the extensibility framework to be used for vendor extensions

G9. Instrumentation

- Address the need for instrumentation of all components within the NASPInet for the purposes of network management, cyber security, diagnostics, performance, and post-event analysis
- Describe the instrumentation requirements

G10. Data Standards and Formats

- Enumerate which core data standards and formats will be mandated
- Describe a data framework that allows for the extension of the core data standards and formats so that a vendor can provide support for additional or new data
- Identify all relevant existing data standards with which the NASPInet system must be compatible or interoperable
- Identify whether any new data standards are needed and if so, specify their attributes

G11. Policy-based Control

- Enumerate the key facets of the NASPInet that required policy-based control of admission control for subscribers, configuration of Data Busses, adaptations to failures, emergency modes, and other things the Offeror believes should not be "hard-coded" within the NASPInet.
- Provide a policy architecture(s) that shall enable policy-based control of these identified policy-controlled facets of NASPInet. The architecture should address whether a given facet that needs policy control can be controlled by simple database tables or would requite something more flexible such as a small policy language for that facet.

G12. Phased Implementation Approach

- Address the need, or lack thereof, for a phased approach to the implementation of the Specification
- Provide a strategy for implementation of this Specification in logical and coherent phases

Phasor Gateway Technical Requirements

The Specification of the Phasor Gateway (PG) must do the following as shown for each topic area:

P1. Scalability

- Address scalability
- Describe the mechanism(s) by which scaling is achieved and define the range over which traffic load will be supported
- Consider the long-term (20 year+) time horizon
- Describe the important dimensions of scalability

P2. Fault Tolerance

- Address tolerance to traffic flow degradation, equipment failure, configuration management errors, and other errors that could affect overall system availability
- Include requirements related to any needed data buffering, retransmission, recovery, and the extent to which they are necessary for each Service Class

P3. Availability

- Describe how to achieve a very high level of system availability
- Quantify the level of system availability that the will be specified, and describe how this level of availability is achieved and quantified for each Service Class
- Specify the required availability of individual components and of each Service Class
- Describe a high-level architecture that is anticipated to achieve system availability in the face of individual component failures

P4. Industry-standard protocol support

- Identify the required industry-standards that must be supported at each level of the protocol stack(s).
- Include support for IEEE C37.118 devices

- Include support for International Electrotechnical Commission (IEC) 61850
- Include a requirement for Institute of Electrical and Electronic Engineers (IEEE) C37.118
- Include support for IEC 61850 and enumerate all other standards and protocols deemed necessary
- Describe how interoperability with Specification standards is to be achieved so that proprietary vendor components can seamlessly interact with standards-based solutions

P5. Vendor interoperability

- Address an interoperability framework for vendor software and hardware interoperability
- Address both legacy and forward compatibility

P6. Traffic flow management

- Address traffic flow management in the context of the Service Classes
- Address the mechanism(s) used to implement traffic flow management, including but not limited handling of time stamps, control messages prioritization and disposition of stale data for each Service Class
- Address the requirements for traffic flow management mechanisms across the classes of traffic
- Address the priorities of multiple classes of control traffic
- Address how these priorities are used to ensure that critical traffic is delivered in the presence of anomalies such as Information Technology (IT) failures and cyber-attacks

P7. Failure mode & event notification

- Address the conditions under which operator/administration attention is required, and the mechanisms by which the operator(s) and administrator(s) are notified and the information that is provided
- Address the dissemination of failure and adverse event notices for each class of service, including the mechanism(s) by which users of the data are notified of service degradation
- Enumerate what failures will be monitored and what type and level of notification is required in the event of failure

P8. Data & task logging

- Describe the capabilities needed for data and control logging and determine the quality and completeness of the logging. The logs must be sufficient to enable post-event analysis, forensic analysis, and other post-anomaly analyses
- Include mechanism(s) that enable triggered high-resolution logging. The events can include either conditions arising out of part NASPInet components as well as conditions arising out of the PMU data itself
- Describe the required data that is recorded in the logs, and provide requirements for what is deemed necessary

P9. Naming Conventions

- Address the implementation of the global logical and physical naming conventions, name resolution, name assignment, and physical-logical name translation
- Allow the vendors to use proprietary naming protocols on the private side of the PG
- Describe the necessary attributes of the NASPInet component naming convention(s) as it applies to the Phasor Gateways

P10. Access control

- Address the requirements and implementation of access control and the mechanism(s) that vendors will be required to use
- Address the NASPInet's long-term identification, authentication, and access control requirements

- Describe the granularity (e.g., device, data block, data item, variable) at which access control is specified
- Distinguish between human-device and device-device access control
- Propose an architecture for access control implementation
- Anticipate a 20+ year life expectancy

P11. Cyber security

- Address how the Phasor Gateways will comply with the Specification's overall cyber security requirements (see requirement G5: Cyber Security), especially with regard to data and control traffic
- Describe a framework that allows Phasor Gateways to describe the cyber security requirements for end-to-end traffic that they deliver to the Data Bus
- Conform to the NERC Critical Infrastructure Protection (CIP) Standards and all other applicable cyber security standards.
- Address how CIP standards compliance is achieved. Specifically, NERC CIP reports must be generated for Phasor Gateways according to the NERC CIP Standards, and any additional reporting requirements arising from the Specification must be reported
- Propose a cyber security architecture for implementing and auditing compliance with cyber security standards

P12. Gateway utilization

- Address the need for the Phasor Gateways to make efficient use of its capabilities, i.e. one-to-many connections that optimize network utilization, such as a publish-subscribe architecture
- Identify appropriate mechanisms, such as User Datagram Protocol (UDP) multicast or Internet Protocol, version 6 (IPv6) multicast, that support this feature
- Describe a high-level architecture that supports multicasting capabilities

P13. Open Application Programming Interface (API) feature

- Address what standards are to be adhered to in the area of PG API development and specify the degree of compliance to be achieved
- Enumerate, at a high level, the required core API interfaces that will be implemented by the Phasor Gateways

P14. Support and training

- Address any necessary hardware, software and training support requirements, such as:
  - Adequate hardware and software support, including spare component availability
  - On-site start-up support to the end-user
  - Training for end-users during start-up & commissioning and upon major feature revisions
  - All hardware, software, and PG system features documentation and instruction manuals
- Outline the expected support and training needs for the Phasor Gateways

Data Bus Technical Requirements

The Specification of NASPInet Data Bus (DB) the must do the following as shown for each topic area:

D1. Data Bus Access

- Mandate that access to the Data Bus shall only be through Phasor Gateways. All SynchroPhasor data must first flow through a Phasor Gateway before it reaches the Data Bus

D2. Forwarding Latency

- Address the forwarding latency requirements for each Service Class
- Specify performance requirements in milliseconds/hop and maximum hops for each Service Class over NASPInet (i.e., source PG to destination PG)
- Describe the maximum allowable latency(ies) in milliseconds per hop and maximum hops for each class of service

D3. Throughput

- Address the forwarding throughput requirements for each Service Class
- Address how the Data Bus manages load balancing
- Describe the minimum throughput and shall provide specific metrics in data-points/second for each Service Class over NASPInet (both per Data Bus component and for Data Bus aggregate)

D4. Cyber Security

- Address how the Data Bus enables and implements end-to-end cyber security for the cyber security services described in the Services specification
- Describe a framework that allows Phasor Gateways to describe the cyber security requirements for end-to-end traffic that they deliver to the Data Bus
- Describe the high-level cyber security architecture for end-to-end security of the data and control traffic flow

D5. Traffic Prioritization

- Address admission control management and admission decisions for traffic of various classes over the NASPInet to manage dynamic, variable traffic loads
- Address traffic prioritization at both the component and the aggregate Data Bus level if traffic load shedding is required

D6. Network Utilization

- Address the issue of efficient data delivery and network utilization when a single payload must be delivered to multiple end-users (e.g., multicasting)
- Describe a high-level architecture that supports efficient network utilization in data and control traffic delivery

D7. Flexibility and Heterogeneity

- Support vendor diversity
- Address how multiple hardware platforms, network topologies, communications infrastructures, network transports, vendors, and software technologies will be supported
- Anticipate a 20+ year life expectancy

D8. Quality of Service (QoS)

- Address the Data Bus QoS for each data stream
- Provide measurements of QoS that will permit data end-users to determine whether a data stream conforms to a given quality of service at any component of the network
- Address how data streams are constructed end-to-end such that the quality of service is provided (e.g., guaranteed delivery vs. best effort, frequency of delivery)
- Enumerate the QoS metrics collected and maintained by the Data Bus and its components

D9. Temporal Synchronicity

- Address mechanism(s) that support temporal synchronism across multiple data streams

- Describe the appropriate rate filtering, data decimation, and data sequencing requirements for each class of service

D10. Instrumentation

- Address instrumentation of the Data Bus and its components for the purposes of network management, cyber security, diagnostics, and performance
- Include at least link latency, throughput, availability, and QoS violations in instrumentation metrics
- Describe the required data that is collected

D11. Anomaly Resilience

- Address how anomalous traffic or behavior from either Phasor Gateway or Data Bus components can be managed so as to ensure resilient Data Bus performance
- Propose an architecture for implementing anomaly resilience within the Data Bus

NASPInet Services

Core services are those which are necessary to the operation of the NASPInet system, some of which are enumerated below. Value-added services are those which vendors may find provide benefits to NASPInet users and/or product differentiation. The Specification of NASPInet Services must do the following as shown for each topic area:

- Address the services below to ensure that a standardized approach for communicating between the various applications, PG and DB are included in the Specification
- Describe a services architecture as well as a services implementation framework
- Address core services and should address value-added services. However, the Responses should address in detail those services that are critical in the immediate future.

Name Services

1. Component registration services address the registration of physical devices.
2. Name registration services address the registration and resolution of logical names to physical devices.

Cyber Security Services

1. Authentication services provide identity verification for both equipment (e.g., devices and software with Personal Computer (PC) cards) and people (e.g., users with passwords) entities.
2. Key management services provide key assignment and resolution.
3. Non-repudiation services verifies that the entity reporting to have performed an action actually performed the action.
4. Data integrity services provide protection of data for the purpose of guaranteeing that the data has not been modified since it was generated, and information about whether a data or control transaction requires integrity protection.
5. Data confidentiality services provide protection of data for the purpose of guaranteeing that only authorized entities can obtain the data, and information about whether a data or control transaction requires confidentiality protection.
6. Access authorization and control services provide access rights information for devices and users with respect to data or control traffic.
7. Trust management services address the question of who is permitted to administer what parts of the NASPInet system (e.g., user/device credentials, inter- and intra-organization access control updates).

Data and Control Services

1. Chain of custody services provide data and control pedigree/provenance tracking during network routing from source to destination.
2. Connection management services provide bandwidth, resource allocation, and cyber security conformance management to accommodate varying demand and traffic loads.
3. Configuration management services provide support for all administration activities such as rollbacks and backup.

D. DELIVERABLES/SCHEDULE

D.1 The following deliverables shall be submitted:

1. Presentation materials for project overview briefing (due one week before briefing)
2. Presentation materials for project status briefing (due one week before briefing)
3. Presentation materials for briefing on the Conceptual Framework of the Specification Development (due one week before briefing)
4. Presentation materials for briefing on the Conceptual Framework of the Specification Development, revised to incorporate agreed upon changes (due two weeks after briefing)
5. Presentation materials for briefing on Draft Specification (due one week before briefing)
6. Presentation materials for briefing on Draft Specification, revised to incorporate agreed upon changes (due two weeks after briefing)
7. Draft complete specification (due five months after award)
8. Presentation materials for briefing on the Final Specification (one week before briefing)
9. Presentation materials for briefing on the Final Specification, revised to incorporate agreed upon changes (due two weeks after briefing)
10. Complete specification (due seven months after award)

D.2 Format

D.2.1.a. Specifications shall be delivered in Microsoft Word or Adobe Acrobat format

D.2.1.b. Presentation materials shall be delivered in Microsoft Word, Microsoft PowerPoint or Adobe Acrobat format

D.2.2. For all deliverables, one hard copy and one electronic copy should be submitted to the Contract Specialist (CS) for the contract file and one electronic copy to the Contracting Officer's Representative (COR).

E. BRIEFINGS

E.1. The contractor shall present a project overview on the "Specification for North American SynchroPhasor Initiative (NASPI)" – October 2008, at the DOE Visualization and Controls Peer Review. It is anticipated that this will be a 20-minute presentation with 10 minutes of questions.*

E.2. The contractor shall present the status of project at the NASPI Working Group Meeting in February 2009 in Phoenix AZ.*

E.3. The contractor shall present the Conceptual Framework of the Specification Development to the Data Network Management Task Team (DNMTT) (approximately two months after award.)*

E.4. The contractor shall present the Draft Specification to the DNMTT (approximately four months after award.)*

E.5. The contractor shall present the Final Specification to the DNMTT (approximately six months after award.)*

*The exact date, duration and location of the briefings E.1. through E.5. will be mutually agreed upon by the contractor and NETL.

F. DECISION POINTS

After the E.3, E.4, and E.5 presentations, the NASPI DNMTT will review progress and will make recommendations to NETL. Based on these recommendations, NETL will make a decision on how to proceed and the Contracting Officer will notify the Contractor accordingly. Possible decision outcomes include:

1. Go Decision – SOW revisions are **not** necessary. The contractor shall continue progress of the specification for the next deliverable/presentation.

2. No-Go Decision - SOW revisions **are** necessary. The contractor shall not progress toward the next deliverable/ presentation until SOW revisions are incorporated by modification to the contract.

G. Appendix A - Service Classes

To support varying end-user application requirements with different data needs, currently five classes of synchrophasor data service have been identified and defined within NASPInet. These Service Classes are based upon qualitative end-to-end application requirements and therefore may have varying Phasor Gateway, Data Bus, and NASPInet Service requirements. NASPI Service classes are both a generalization and expansion of the per-link scalability and performance requirements from [1], which mainly involves a substation-level scope. The original analysis and justification of many of the flexibility and robustness requirements and emergency modes for the NASPInet Data Bus are found in [2]. Many future-looking case studies of what NASPInet may be used for, as well as data availability requirements, can be found in [3]. The implementation of the Specification may require the quantification of end-to-end resource usage requirements, in which case it may be useful to define quantifiably-defined sub-classes within each qualitatively-defined Service Class.

The five currently defined Service Classes are as follows:

CLASS A: Feedback Control Typical use: Small Signal Stability
This class is characterized by very low latency and a fast data rate (e.g., 60 messages per second). Data must be transmitted and received as quickly as possible. A high level of data availability is required (no gaps). End user applications of this data class are generally operating on data from a small number of PMUs that are likely geographically close.

CLASS B: Feed-forward Control Typical use: State Estimator Enhancement
Latency requirement is less strict than class A due to the relatively slower processing rate of state estimator applications. However, the time alignment of the received data from the entire set of PMUs is critical.

CLASS C: Post Event Typical use: Post-mortem Event Analysis
This class requires a high degree of data completeness and accuracy. Higher latency is acceptable since analysis is generally conducted off-line (hours or days later) with archived data, as opposed to an on-line data stream. A high message rate is desirable to be able to reconstruct as many power system event characteristics as possible. However, in practice this may not be achievable for large-scale post event data sets due to NASPInet bandwidth limitations that may be imposed on Class C traffic.

CLASS D: Visualization Typical use: Operator visibility
Latency is not a critical issue. Data must be time-aligned, but not to the extent of class B data. There is a wider tolerance for accuracy. This data class is analogous to a Doppler radar view of the system. End-user applications may retrieve data from many PMUs across a wide geographical area.

CLASS E: Research Typical use: Testing or Research and Development (R&D)
There are no guarantees on any attributes of this data class. Class E shall be given the lowest priority of all NASPInet data traffic.
The table below summarizes key NASPInet traffic attributes, as of January 2008, among the five classes:

NASPInet Traffic Attribute	CLASS A Feedback Control	CLASS B Feed-forward Control	CLASS C Post Event	CLASS D Visualization	CLASS E Research
Low Latency	4	3	1	2	1
Availability	4	2	3	1	1
Accuracy	4	2	4	1	1
Time Alignment	4	4	1	2	1
High message rate	4	2	4	2	1
Path Redundancy	4	4	1	2	1
Table key: 4 – Critically important, 3 – Important, 2 – Somewhat important, 1 – Not very important					

H. ACRONYMS AND DEFINITIONS

API	Application Programming Interface
CIP	Critical Infrastructure Protection
CS	Contract Specialist
COR	Contracting Officer's Representative
DB	Data Bus
DNMTT	Data Network Management Task Team
DOE	Department of Energy
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IPv6	Internet Protocol, version 6
IT	Information Technology
MTBF	Mean Time Between Failures
MTTR	Mean Time To Recovery
NASPI	North American SynchroPhasor Initiative
NASPInet	NASPI network, composed of Phasor Gateways, a Data Bus and a set of common services
NERC	North American Electric Reliability Corporation
NETL	National Energy Technology Laboratory
PC	Personal Computer
PDC	Phasor Data Concentrator
PG	Phasor Gateway
PMU	Phasor Measurement Unit
QoS	Quality of Service
R&D	Research & Development
UDP	User Datagram Protocol

Availability - A probabilistic measure of whether a service or component is correctly functioning when needed [4]. There are many sub-definitions. Steady-state availability is this measure over all time, and is quantified by Mean Time Between Failures (MTBF)/[MTBF+Mean Time To Recovery (MTTR)]. Interval availability is a measure over a given time interval, for example time to delivery a single data update or alert.

Confidentiality – The concealment of information or resources from unauthorized entities.

Fault Tolerance - The ability of a component, service, or system to operate satisfactorily under anomalous conditions such as traffic flow degradation, equipment failure, configuration management errors, and other errors that could affect overall system availability. [4]

Integrity – The accuracy and completeness of data and resources. Data integrity ensures that only authorized entities may modify data content. Origin integrity ensures that entities trust the origin of data or resources.

Traffic Load Shedding - The act of reducing data or control traffic, based on service class, during times of high demand to insure service class requirements are met.

NASPInet – NASPI data delivery service and network on which it is built.

Privacy – The prevention of unauthorized dissemination of information about an entity and its actions.

Reliability - A measure of the probability that a system or component or service does not fail during a given time period; i.e., time to first failure [4].

Service Classes - Synchrophasor data service groupings based upon qualitative end-to-end application requirements.

Synchrophasor - Synchronized phasors.

The Specification - The work product the contractor will deliver to DOE per the Statement of Work

Traffic - Refers to the transmission of both control and data elements.

- Control Traffic - Refers to the transmission of non-data elements.
- Data Traffic - Refers to the transmission of data elements.

I. REFERENCES

[1] IEEE 1646 Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation, IEEE, 2004.

[2] David E. Bakken, Carl H. Hauser, Harald Gjermundrød, and Anjan Bose. "Towards More Flexible and Robust Data Delivery for Monitoring and Control of the Electric Power Grid", Technical Report EECS-GS-009, School of Electrical Engineering and Computer Science, Washington State University, May 30, 2007. Available via http://www.gridstat.net/TR-GS-009.pdf.

[3] IntelliGrid Project, "The Integrated Energy and Communication Systems Architecture, Vol. IV: Technical Analysis".2004, Available via http://www.epri.com/IntelliGrid/.

[4] A. Avizienis, J. Laprie, B. Randell, and C. Landwehr. "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE Transactions on Dependable and Secure Computing, 1:1, January 2004, 11-33.

IEEE C37.118-2005 IEEE Standard for Synchrophasors for Power Systems, IEEE, 2006.

IEC 61850 Communication Networks and Systems in Substations
http://www.61850.com/index.html.
NERC Critical Infrastructure Protection Standards
http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection.