EXHIBIT 6
REQUEST FOR PROPOSALS
FOR THE
NUMBER PORTABILITY
ADMINISTRATION CENTER/ SERVICE
MANAGEMENT SYSTEM
(NPAC/SMS)
in the
U.S. WEST REGION

September 16, 1996
SECTION 1: GENERAL INFORMATION

The purpose of this Request for Proposal ("RFP") is to invite you to submit a proposal to provide a Number Portability Administration Center ("NPAC") and Service Management System ("NPAC/SMS") to support the implementation of local number portability ("LNP") in the fourteen states in the U.S. WEST region.

It has been determined that:
(a) Location Routing Number (LRN) shall be the long-term network architecture employed;
(b) an NPAC shall administer an NPAC/SMS to receive, store, and broadcast this routing information; and
(c) a contracting entity shall be established to select an NPAC and NPAC/SMS vendor, contract with that vendor, and supervise that vendor's performance.

1.1 Evaluation of Proposals. The contracting entity will evaluate all proposals from a total network and operations perspective to ensure integration with existing network and operating procedures. Specifically, the contracting entity, when accepting or rejecting a proposal, will consider (a) technical merit and creativity, (b) implementation schedule, (c) price, (d) quality, (e) bidder's financial stability and performance history (including subcontractors), (f) ability to accommodate future considerations, (g) variance or deviations from specifications below, and (h) conflicts of interest. The contracting entity reserves the right to accept or reject any or all proposals made in response to this RFP based on any or all of the criteria identified in (a) through (h) above. Selection of the vendor and final contract approval may require approval by one or more state agencies.

1.2 Regulatory Oversight. This RFP, the contracting entity, the contract between the contracting entity and the vendor, and the ongoing operation of the NPAC may be subject to state Commission oversight and, as appropriate, approval. Additionally, the Federal government, through Congressional legislation, Federal Communications Commission rule making, or other mandates, may establish policies which affect this RFP, the contracting entity, the contract between the contracting entity and the vendor, and the ongoing operation of the NPAC.

---

1 Throughout this RFP the term NPAC/SMS is used to distinguish the SMS operated by the NPAC and SMSs operated by NPAC users.
1.3 Proposal.

1.3.1 Content of proposal.

TAB 1: Description of Vendor. The vendor shall identify itself and all subcontractors. The vendor shall also detail:

(a) the vendor's and all subcontractor's principal business;
(b) the vendor's and all subcontractor's related experience, in particular (1) any related telecommunications experience and (2) if the vendor has installed a similar system, identify the client, location, and date;
(c) the vendor's and any subcontractor's financial condition. Responses should include the vendor's and any subcontractor's most recent annual report or audited financial statement.

TAB 2: Conflict of Interest. The vendor shall verify that it does not have a conflict of interest as defined by Section 1.4 of this RFP.

TAB 3: Proposal Summary. The vendor shall summarize the system the vendor proposes and the system's strengths and weaknesses.

TAB 4: Technical Proposal. The vendor shall (a) describe the vendor's proposed system including (1) operating and database software and (2) hardware and (b) for each requirement detail, as specifically as possible, either (1) how the system will meet or exceed the requirement or (2) how the system will not meet that requirement as specified in this RFP and any justification for such exception or deviation. One potential justification for deviating from a requirement is if the vendor can demonstrate that an alternative approach will result in a superior product. A response that the vendor shall "comply" with the requirement without accompanying explanation as to how compliance will occur is insufficient. A statement that the vendor shall "develop a process" to meet a requirement is similarly insufficient without explanation of what that process is expected to entail.

TAB 5: Price. The vendor shall state the price. For purposes of this section, assume the contract will be for a five-year term. DO NOT INCLUDE COST OR PRICE FIGURES ANYWHERE EXCEPT IN YOUR TAB 5 RESPONSE.

1.3.2 Submission Information and Due Date. One copy of your proposal, complete in all respects, must be submitted to all of the addressees provided in the cover letter to this RFP.

Your cover letter shall include both the name(s) and phone number(s) of the individual(s) within your company who should be contacted in case any questions should arise during the evaluation of your proposal. Failure to direct your response to the address given above by the noted closing date may result in the disqualification of your proposal. The package containing your proposal shall be marked "Sealed Proposal" with this RFP title and your company's name.
Your proposal shall be in loose-leafed binders on typed double spaced on 8-1/2" x 11", 3-hole punched, white paper. Each volume shall begin on a new page and be separately tabbed. Diagrams, if applicable, shall not be in color. Additionally, an electronic copy in MS Word 6.0 format shall be provided.

1.3.3 Acceptance period. Your proposal shall indicate that it is valid for a period of at least one hundred eighty (180) days.

1.3.4 Confidentiality. Do not submit any proprietary or confidential information or mark it as such. In no event will the contracting entity consider or hold any information contained in your proposal proprietary or confidential, except for pricing information. The contracting entity reserves the right to release an average and range of the prices received.

1.3.5 Questions or Requests for Additional Information. Submit your question(s) or request(s) for additional information in writing to all of the facsimile numbers listed in the cover letter to this RFP no later than three days prior to the closing date for this RFP.

All questions and responses shall be promptly distributed to all recipients of this RFP. Please note that the identity of the requesting company shall be withheld. Telephone inquiries shall not be accommodated.

1.4 Conflict of Interest. The vendor must be a neutral third party, as may be defined by the FCC. Additionally, a neutral third party has no significant financial or market interest in providing local exchange service within the United States. To prevent a conflict of interest, the vendor shall not be: (a) a local exchange telecommunications service provider in the United States or (b) an entity (1) owned by, (2) which owns, or (3) affiliated through common ownership with any other local exchange telecommunications service provider in the United States (ownership interests of five percent (5%) or less shall not be considered ownership for purposes of this section). Once a vendor is selected, the vendor shall notify the contracting entity of any change in its neutral third party status. Such changes shall, in the sole discretion of the contracting entity, be cause for revocation of the contract.

1.5 Primary Vendor’s Acceptance of Key Business Terms and Conditions. Each Primary Vendor submitting a Pre-Qualification application to the CONTRACTING ENTITY must list the following key business terms and conditions and indicate its acceptance of these key business terms and conditions, as a pre-condition to being considered for a contract award as a Primary Vendor, by placing an “X” in the space next to each item listed. These terms and conditions are expected to form a part of the Master and Service Agreements to be executed with the Primary Vendor selected under this RFP, if any, and may not represent a full and complete listing of all contractual terms and conditions incorporated into those agreements.

KEY BUSINESS TERMS AND CONDITIONS ACCEPTED BY PRIMARY VENDORS

1. The CONTRACTING ENTITY, shall have the right to terminate the Contractual Agreement entered into through this RFP with the Primary Vendor for reasons of default (including, but not limited to, unauthorized assignment of agreement and failure to provide adequate Service), upon 30 days notice. The CONTRACTING ENTITY can avail itself of this termination option by simple majority vote of its membership. Also, the Primary Vendor is forbidden from making any unilateral changes to the Master or Service Contracts entered into under this RFP.
2. The CONTRACTING ENTITY shall be granted appropriate license rights in and to any technology or other intellectual property that is developed for and at the request of the CONTRACTING ENTITY for the purposes of providing the Services; and Primary Vendor and Sub-Contractor(s), if any, shall agree to appropriate limitations on their use of any such technology or other intellectual property for purposes other than the express provision of the Services specified in the RFP.

3. The Primary Vendor and Sub-Contractor(s), if any, shall deposit all technology and other intellectual property and related documentation under its control, that is necessary to the provision of these Services, with a mutually agreeable escrow agent for the use of the CONTRACTING ENTITY, or to allow another vendor the ability to provide Services, in the event of Supplier default (e.g., bankruptcy, failure to perform, etc.).

4. The Primary Vendor and Sub-Contractor(s), if any, agrees to indemnify and save harmless the CONTRACTING ENTITY, its Members and their parents, subsidiaries, other affiliates, their direct and indirect customers, and the officers, directors, employees, successors, agents, representatives, successors and assigns of any and all of them (all hereinafter referred to in this clause as the "CONTRACTING ENTITY") from and against any and all claims, losses, damages, expenses, liabilities, suits demands, causes of action, including costs and reasonable attorney's fees, or liens that arise out of or result from:

   (i) Injury or death to persons, or loss or damage to any and all property, including theft, in any way arising directly or indirectly out of, or occasioned by, caused or alleged to have been caused by, or on account of, the performance of the Work or Services performed by Primary Vendor, or Sub-contractor(s), if any, or its agents, or any director, officer, employee, agent or representative under this Agreement,

   (ii) Assertions under Workers' Compensation or similar acts made by persons furnished by Primary Vendor, or Sub-Contractor(s), if any, or by reason of any injuries to such persons for which the CONTRACTING ENTITY would be responsible under Workers' Compensation or similar acts if the persons were employed by the CONTRACTING ENTITY,

   (iii) Any failure on the part of Primary Vendor, or Sub-Contractor(s), if any, to satisfy all claims for labor, equipment, materials and other obligations relating to the performance of the work hereunder, and;

   (iv) any failure by Primary Vendor, or Sub-contractor(s), if any, to perform its obligations under this clause, the Insurance clause, or any clause in the Agreement.

Each party shall defend or settle, at its own expense, any action or suit against the other for which it is responsible hereunder and shall reimburse the other for reasonable attorneys' fees, interest, costs of suit and all other expenses incurred by the other in connection therewith. Each party shall notify the other promptly of any claim for which the other is responsible hereunder, and shall cooperate with the other in every reasonable way to facilitate the defense of any such claim.

5. The Primary Vendor and Sub-Contractor(s), if any, shall be willing, at the CONTRACTING ENTITY's request, to obtain a bid and/or performance bond in an amount sufficient to guarantee performance of its obligation under the RFP.
6. The Primary Vendor and Sub-Contractor(s), if any, shall treat all information obtained from the CONTRACTING ENTITY or its members confidential and proprietary unless they can demonstrate that such information was previously known by the Supplier(s) without an obligation of confidentiality.

7. No information furnished by the Primary Vendor or Sub-contractor(s), if any, in response to the RFP or under any Contractual Agreement arising out of the RFP shall be considered confidential or proprietary, except the Tab 3, cost and Price information described in Tab 5.

8. The Primary Vendor and Sub-Contractor(s), if any, shall indemnify the CONTRACTING ENTITY and its members against any infringement claims arising from the provision of Services under this RFP.

9. During the term of this Agreement, the Primary Vendor and Sub-Contractor(s), if any, shall obtain and maintain, with financially reputable insurers (i.e., carriers with an A.M. Best rating of B+: VII, or better) which are licensed to do business in all jurisdictions where any work is performed and which are reasonably acceptable to CONTRACTING ENTITY, not less than the following levels of insurance coverage:

   a.) Worker's Compensation as provided for under any worker's compensation or similar law in any jurisdiction where any work is performed, with an Employer's liability limit of not less than $500,000 per accident or disease;

   b.) Commercial General Liability, including coverage for Contractual Liability and Products/Completed Operations Liability, with a limit of not less than $1,000,000 combined single limit per occurrence for bodily injury, property damage and personal injury liability (with contractual exclusion deleted), naming CONTRACTING ENTITY, its members, their directors, officers, employees, agents and/or representatives as additional insureds;

   d.) Umbrella/Excess liability with limits of not less than $9,000,000 combined single limit in excess of the above-referenced Employer's Liability, Commercial General Liability and Business Auto liability coverage naming CONTRACTING ENTITY, its members, their directors, officers, employees, agents and/or representatives as additional insureds;

   e.) "All risk" Property insurance covering not less that the full replacement cost of Primary Vendor's and any Sub-Contractor(s), if any, personal property at risk due to this Agreement; and,

   f.) errors and Omissions Insurance in the amount of at least $1,000,000 per claim with an annual aggregate of at least $3,000,000 inclusive of legal defense costs.

Waiver of Subrogation: Primary Vendor shall look first to any insurance in its favor before making any claim against CONTRACTING ENTITY, its members, their directors, officers, employees, agents and/or representatives for recovery resulting from injury to any person (including Primary Vendor's or Sub-Contractor's employees, if any) or damage to any property arising from any cause, regardless of negligence, and does hereby release and waive to the fullest extent permitted by law, and shall cause its insurers to waive, all rights of recovery against CONTRACTING ENTITY, its members, their directors, officers, employees, agents and/or representatives.

Certificates of Insurance: Primary Vendor and Sub-Contractors, if any, must as a material condition of this Agreement, prior to the commencement of any work and prior to the renewal thereof, deliver
to CONTRACTING ENTITY a certificate of Insurance, satisfactory in form and content to CONTRACTING ENTITY, evidencing that the above insurance is in force and contains a provision that it will not be cancelled or materially altered without first giving CONTRACTING ENTITY thirty (3) days prior written notice and that all coverage is primary to any insurance carried by CONTRACTING ENTITY or its members.

Nothing contained in this section shall limit Primary Vendor of Sub-Contractor's, if any, liability to CONTRACTING ENTITY or its members to the limits of insurance coverage certified or actually carried.

10. The Primary Vendor shall submit a list of Sub-Contractor(s), if any, to the CONTRACTING ENTITY with its Pre-Qualifications submission, for review and approval. Any subsequent change in the use of any Sub-Contractor(s) shall require the review and approval of the CONTRACTING ENTITY.

11. The Primary Vendor and Sub-Contractor(s), if any, shall not have the right to assignment of the Contractual Agreement entered into through this RFP without the prior approval of the CONTRACTING ENTITY.

12. The governing law under this RFP and any Contractual Agreement entered into through this RFP shall be that of the state of Colorado, unless otherwise specified by the contracting entity.

13. In the event that the Service does not pass a mutually agreed upon Acceptance Plan, designed to determine the Primary Vendor's system compliance with the functional and technical requirements of this RFP, the CONTRACTING ENTITY shall have the option to terminate the arrangement without any penalties whatsoever to it or its member carriers.

1.6 Subcontractors. The vendor shall be solely responsible for performance and shall be the single point of contact for the contracting entity. However, the vendor, at its option, may use its own resources exclusively or engage the services of subcontractors to provide one or more elements of the NPAC/SMS platform (hardware, software, etc.). Responses to this RFP shall clearly state the roles and responsibilities of any and all subcontractors which are providing parts of the proposed solution under the direction of the vendor.

1.7 Testing. Prospective vendors may be required, at the contracting entity's sole discretion, to furnish components of their systems to the contracting entity for evaluation and testing and/or to make arrangements on their own premises for facilitating joint testing, at no charge. The contracting entity reserves the right to cancel the acceptance of a bid if the services or facilities do not pass acceptance tests.

1.8 Contract. The NPAC and NPAC/SMS shall be provided pursuant to a contract between the NPAC and the contracting entity. The contracting entity reserves the right to negotiate all terms and conditions of such a formal agreement. No contractual obligations are assumed by (a) issuing the RFP or (b) receiving, evaluating, or accepting, a vendor's response. The contracting entity reserves the right to conduct negotiations with more than one vendor simultaneously.

1.9 Modification and Revision of RFP. This RFP may include unintended errors, omissions, and/or deficiencies. Therefore, the accuracy and completeness of this document and related documents are not guaranteed. The contracting entity reserves the right to modify the RFP at any time.
further reserves the right to cancel the RFP process without penalty at any time before a written contract is entered into.

SECTION 2: OVERVIEW OF THE ROLE OF THE NPAC AND NPAC/SMS

The NPAC/SMS is a hardware and software platform which contains the database of information required to effect the porting of telephone numbers in an LRN architecture. The NPAC/SMS shall not be involved in actual call routing, but rather shall receive, store, broadcast data on ported directory numbers ("DNs"), and provide informational reports based on the information contained in the database. This information is necessary to allow each user's network to properly route calls.

The NPAC shall manage the NPAC/SMS database. The NPAC shall be responsible for the maintenance and performance of the NPAC/SMS.

The NPAC/SMS Interoperable Interface Specification (IIS) shall define the interface between the NPAC/SMS and the Service Order Administration (SOA) system and the Local NPAC/SMS.

SECTION 3: RECEIVING, STORING, AND BROADCASTING PORTED DN DATA

Section 3 defines the data which the NPAC/SMS will receive, store, and broadcast. This section also identifies the existent states in which data may be within the NPAC/SMS.

3.1 Types of data to be received, stored, and broadcast.

R3-1 The NPAC/SMS shall, at a minimum, receive, store, and broadcast the following information on each ported DN: (Descriptions of these items can be found in the glossary that is attached to this RFP as an appendix.) See Section 3.1 of the NPAC/SMS Functional Requirements Specification (FRS) for a summary of the data elements administered and utilized by the NPAC/SMS.

<table>
<thead>
<tr>
<th>Data Item</th>
<th>Size</th>
<th>Receive</th>
<th>Store</th>
<th>Regular Broadcast</th>
<th>Disconnect Notice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone Number</td>
<td>10</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>LRN</td>
<td>10</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilities-Based Provider ID</td>
<td>4</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Disconnect Date</td>
<td>8</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Date Disconnect Broadcast Rec’d</td>
<td>8</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPC for CLASS</td>
<td>9</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SSN for CLASS</td>
<td>3</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>DPC for LIDB</td>
<td>9</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSN for LIDB</td>
<td>3</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPC for ISVM</td>
<td>9</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSN for ISVM</td>
<td>3</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>DPC for CNAM</td>
<td>9</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>SSN for CNAM</td>
<td>3</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>End-user location (Future Use)</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The NPAC may require additional fields for its uses. Additionally, future considerations may require additional types of data to be received, stored, and broadcast by the NPAC/SMS (See Section 9).

### 3.2 Receiving data.

**R3-3** The NPAC/SMS shall be designed to interface electronically with three types of "users". First, large local exchange telecommunications providers will probably interface for purposes of uploading data into the NPAC/SMS and receiving broadcasts from the NPAC/SMS. Second, a small rural telecommunications provider may wish to interface with the NPAC/SMS for purposes of uploading data, but may elect to contract with another provider to maintain its routing information. Such a company, therefore, may not interface with the NPAC/SMS for receiving broadcasts. Third, an interexchange provider may only interface with the NPAC/SMS for purposes of maintaining routing information and, therefore, may not interface with the NPAC/SMS to upload information. Throughout this RFP, the term "user" is used generically. The Service Provider and Service Provider Network Data Scenarios shall be implemented as defined in Sections 6.3 and 6.4 of the IIS.

**R3-4** The NPAC shall receive and record data needed to identify, contact, and bill new NPAC/SMS users. For example, the NPAC shall receive the LRNs, portable NXXs, network addresses for interfaces, and billing information. The NPAC/SMS shall verify that the correct facilities-based service provider ID is associated with the new user. A user shall require state regulatory commission approval to use the NPAC/SMS.²

### 3.3 Storing and processing data.

**R3-5** At a high level, the data associated with each ported DN may be described as either "pending", "in effect", and "archived". The Subscription Version Data associated with each ported DN shall be defined in Section 3.1.3 of the FRS.

**R3-6** When a customer wishes to change service providers and keep the same telephone number, the new service provider shall instruct the NPAC/SMS to create a subscription associated with that customer's telephone number. The subscription shall be created in the pending state unless the subscriber already exists in pending. If the subscriber exists in pending, the NPAC shall reject any new request to create a subscription for that subscriber DN. The Subscription Version Flow Scenarios shall be implemented as defined in Section 6.5.1 of the IIS.

² An order from the state regulatory commission which certifies a provider of exchange telecommunications services shall serve as official notification of provider status. Other users of the NPAC/SMS shall provide other official documentation which demonstrates the need to have access to NPAC/SMS data, e.g., certification as an interexchange carrier, providers of SCP/STP sites, etc.
R3-7 When a subscription is in the pending state, the NPAC/SMS shall:
(a) verify the data;
(b) alert the old service provider of the creation of the subscription and allow the old service
provider the opportunity to either confirm the data in the subscription or place the
subscription into conflict;
(c) allow the new service provider the opportunity to cancel the subscription; and
(d) allow the new service provider the opportunity to activate the subscription when the new
service provider effectuates the physical act of changing the customer's service.

The Subscription Version Flow Scenarios shall be implemented as defined in Section 6.5.1 of the
IIS.

R3-8 It is possible that the old service provider has the option to send a confirmation either before or after
the new service provider sends a request to create a subscription. If this occurs, the NPAC/SMS shall:
(a) verify the data;
(b) alert the new service provider of the confirmation;
(c) if the new service provider sends a request to create a subscription within 90 days (tunable
parameter), follow the process outlined in R3-7 (except step b); and
(d) if the new service provider does not send a request to create a subscription within 90 days
(tunable parameter), delete the confirmation and issue error message.

R3-9 When a customer who has already ported at least once changes service providers again, a
subscription will be created in the pending state and, eventually, in the in effect state. At that time,
the obsolete version of the subscription existing in the in effect state shall be stored by the
NPAC/SMS in the archived state. Each archived version of a subscription shall be stored by the
NPAC/SMS for 18 months (tunable parameter). The Subscription Version Flow Scenarios shall be
implemented as defined in Section 6.5.1 of the IIS.

3.4 Conflict.

R3-10 A subscription shall be placed into conflict if the initial information provided by the new service
provider does not match the information provided by the old service provider. The Subscription
Version Conflict Scenarios shall be implemented as defined in Section 6.5.5 of the IIS.

R3-11 If a subscription has been placed into conflict the NPAC/SMS shall notify all affected users and
save the information associated with the subscription for 30 days. The Subscription Version
Conflict Scenarios shall be implemented as defined in Section 6.5.5 of the IIS.

R3-12 A subscription which has been placed into conflict shall not be broadcast by the NPAC/SMS.

3.5 Modification.

R3-13 The NPAC/SMS shall permit the new service provider to modify a subscription in the pending
state. The NPAC/SMS shall verify all modified data. The Subscription Version Modification
Scenarios shall be implemented as defined in Section 6.5.2 of the IIS.
3.5 Validations.

R3-15 When the NPAC/SMS receives and broadcasts data it shall perform the following validations: (a) all data must be in the proper format and (b) if a DN is being ported, (1) the LRN must be associated with a valid facilities-based provider, (2) the new facilities-based ID must match the new LRN, and (3) the NPA-NXX must be portable.

R3-16 If a confirmation is sent by the old facilities-based provider, the NPAC/SMS shall verify that the information sent by the old facilities-based provider matches the information sent by the new facilities-based provider.

3.7 Error/Success Messages.

R3-17 Whenever the NPAC/SMS is asked to perform a task or verify data, the NPAC/SMS shall issue an error message to the appropriate company(ies) if the task cannot be successfully completed or if the data is improper. The error message shall, when possible, identify the cause of the failure or the improper data.

R3-18 Whenever the NPAC/SMS completes a task it was asked to perform or verifies that data is proper, the NPAC/SMS shall issue a success message to the appropriate company(ies).

3.8 Broadcasting data.

R3-19 When a subscription has been activated or modified in the in effect state, the NPAC/SMS shall broadcast the subscription to all users. If the NPAC/SMS is unable to transmit the data to a particular user, the NPAC/SMS shall repeat the attempt twice (tunable parameter) and, if the data has still not been successfully transmitted, contact the user and rebroadcast the data once the problem is solved. Once a subscription has been broadcast to at least one user, the subscription shall be in the in effect state. The Subscription Version Broadcast Scenarios shall be implemented as defined in Sections 6.5.1.5 through 6.5.1.7 of the IIS.

R3-20 A customer disconnect notice to the NPAC may include two dates: (1) the “customer disconnect date,” which is always present and (2) the “broadcast date”, which is sometimes present. The “broadcast date” indicates when the broadcast is to be made. If the “broadcast date” is not provided, the broadcast is immediate. The “customer disconnect date” is never included in the broadcasted information. However, the “customer disconnect date” is sent to the SOA of the local service provider to whom the NPA-NXX of the disconnected customer is assigned. This is done at the same time the disconnect broadcast is made. The Subscription Version Disconnect Scenarios shall be implemented as defined in Section 6.5.4 of the IIS.

R3-21 The NPAC shall filter, at an NPA-NXX level, the broadcasts and other messages sent to the provider’s local SMS. That is, a provider shall be able to specify the NPA-NXXs for which it wishes to receive information.
SECTION 4: INTERFACE DESCRIPTION

Section 4 describes the interfaces between a user and the NPAC/SMS. This section also describes the interface protocols and performance requirements. There are two potential interfaces. First, the NPAC/SMS must be able to interface with a user's Service Order Administration ("SOA") platform. Second, the NPAC/SMS must be able to interface with a user's SMS.

4.1 Interfaces.

R4-1 There shall be at least one NPAC/SMS actual or virtual point of presence (POP) in each state served by the NPAC/SMS. These POPs shall be located near a Metropolitan Statistical Area (MSA) in each state.

R4-2 The vendor shall be responsible for the facilities cost between each POP and the NPAC/SMS locations.

R4-3 Each proposal shall define the location of each POP and its actual type of transmission facility.

R4-4 An NPAC/SMS to user SMS interface shall support the actual exchange of ported DN data and any error or success messages associated with those transactions. An NPAC/SMS to SOA interface shall support all other transactions and reports.

R4-5 All interfaces shall support two-way communication in real-time and batch mode.

R4-6 The NPAC/SMS to user SOA interface shall accommodate Service Provisioning OSs and/or Gateway Systems. The NPAC/SMS to user SMS interface shall accommodate SMS (or SMS-like functions by a user SCP) and/or Gateway systems.

R4-7 All interfaces shall be capable of supporting multiple independent transactions. One failed item in a request shall not cause the other items in the request to fail.

R4-8 All interfaces shall be non-proprietary.

R4-9 A user may have multiple sessions running simultaneously with the NPAC/SMS application.

4.2 Interface Protocol.

R4-10 All system to system interfaces shall be implemented as defined in Section 2.2 of the IIS with the exception that ATM shall be included in the Link Layer.

R4-11 The NPAC/SMS IIS shall define the interface between the NPAC/SMS and the Local SOA.

R4-12 The IIS shall define the interface between the NPAC/SMS and the Local SMS.

R4-13 Section 6 of the IIS shall define the message flow scenarios between the NPAC/SMS and SOA systems, and between the NPAC/SMS and the Local SMSs.
Section 7 of the IIS shall define the GDMO object definitions managed and utilized by the NPAC/SMS.

Unless otherwise stated in this RFP, the requirements in the IIS shall provide all interface specifications.

An additional, alternative NPAC/SMS to User-SOA interface shall be provided by the vendor to support communications via dial-up modem using the PPP protocol, and a vendor defined, secure, simple low-cost message protocol. A non-inclusive list of possible message protocols is shown below:

a. A fixed format record for each SOA function that can be sent to, or received from, the NPAC/SMS.

b. Sequential Query Language (SQL).

c. Any other message protocol proposed by the vendor.

The vendor defined, secure, simple low-cost message protocol, requested in R4-16, shall provide all SOA interface functionality that is required on the NPAC/SMS to User-SOA CMISE interface.

The vendor shall provide an application that can operate on Windows 95™ or Windows NT™ that will allow the user to easily enter service order data and interface with the NPAC/SMS via the secure, simple low-cost message protocol.

The Vendor’s response shall be specific in their description of any changes or losses in performance resulting from the use of the secure, simple low-cost message protocol described in R4-16.

4.3 Interface Performance Requirements.

A transaction rate of 2 transactions per second shall be supported by each NPAC/SMS to user SOA interface. A transaction rate of 25 transactions per second shall be supported by each NPAC/SMS to user SMS interface. A transaction here refers to a transfer of data about a single DN, not to a CMISE transaction.

Mass changes may be aggregated into a single file and broadcast in accordance with a file transfer mechanism, for example, FTP.

4.4 TMN Architecture.

The SMS Supplier/Vendor must be in compliance with the Telecommunications Management Network (TMN) Architecture, including, but not limited to the following documents:

(a) GR-2869-CORE, Generic Requirements for Operations Based on the Telecommunications Management Network (TMN) Architecture, Issue 1;

(b) OAM&P - Protocols for Interfaces between Operations Systems in Different Jurisdictions (ANSI T1.224-1992);

(c) TA-TSY-000899, Requirements Specifications for an Operations System (OS) to OS Interface using Generic OSI Protocols including the OSI Network Management Protocols (Consistent with ANSI T1M1.5);
OAM&P - Lower Layer Protocols for Telecommunication Management Network (TMN) Interfaces Between Operations Systems and Network Elements (ANSI T1.204-1993);

OAM&P - Upper Layer Protocols for TMN Interfaces Between Operations Systems and Network Elements (ANSI T1.208-1993);

OAM&P - Principles of Functions, Architectures, and Protocol for Telecommunications Management Network (TMN) Interfaces (ANSI T1.210-1993);

OAM&P - Extension to Generic Network Model for Interface Between Operations Systems Across Jurisdictional Boundaries (ANSI T1.227-1992);

GR-1286-CORE, AIN to Operations System (OS) - Service Control Point (SCP) Interface Generic Requirements (Information Model between SCP and SMS) using CMIP protocol; and


SECTION 5: MASS CHANGES AND OTHER MAJOR DATA TRANSMISSIONS

Section 5 describes the requirements that the NPAC/SMS be able to accommodate mass changes and major data transmissions. There are three types of mass changes and major data transmissions which are contemplated: (a) NPA splits, (b) user takeover, and (c) system failure.

5.1 NPA Splits and Other Mass Updates. The splitting of an NPA is a complex process that can take well over a year to complete. NPAC shall maintain a close working relationship with organizations responsible for NPA split/mass changes scheduling because when an NPA split takes place a large amount of ported DN data may be added or require modification.

R5-1 The NPAC/SMS shall be capable of globally modifying a large amount of ported DN data when an NPA split occurs and maintaining the dual "in effect" records required to accommodate a permissive dialing period.

R5-2 The NPAC/SMS shall be able to analyze the impact of a proposed split on NPAC/SMS administrative tables and ported DN data.

R5-3 The Mass Update Scenarios shall be implemented as defined in Sections 6.6.3 and 6.6.4 of the IIS.

5.2 User Takeover. If a user with ported DNs is taken over by another user, all ported DN data associated with the old user may need modification to reflect the change.

R5-4 The NPAC/SMS shall be capable of globally modifying the appropriate ported DN data when a user is taken over by another.

5.3 System Failure. If a user's system fails and data becomes lost or otherwise corrupted, the user may require a complete transmission (FTP) of all ported DN data.

R5-5 The NPAC/SMS shall be capable of transmitting (FTP) all or some ported DN data to a specific user.
SECTION 6: PERFORMANCE CRITERIA

Section 6 describes the specific performance criteria requirements for the NPAC and the NPAC/SMS. These requirements include the reliability of the NPAC/SMS, the availability of the NPAC and the NPAC/SMS, the capacity requirements of the NPAC/SMS, and the capabilities for disaster recovery.

6.1 Continuity of Service.

R6-1 The NPAC/SMS shall not have more than 24 hours of scheduled downtime per year. Prior to any scheduled downtime, the NPAC shall notify all potentially affected users and attempt to minimize user impact.

R6-2 Except as provided in R6-1, system performance shall not be impaired or interrupted as a result of software upgrades, hardware upgrades, capacity expansion, to perform maintenance, or during back-up and recovery.

6.2 Reliability of the NPAC/SMS.

R6-3 The NPAC/SMS shall be highly reliable. The NPAC/SMS shall include data integrity features, symmetrical multi-processing capability, and economical and efficient system expansion capability.

R6-4 The NPAC/SMS shall maintain data integrity with 99.9% reliability. The NPAC/SMS shall perform all other functions with 99.9% reliability.

6.3 System Failure.

R6-5 The NPAC/SMS shall monitor the status of all of its functions, including communications links. The NPAC/SMS shall be capable of detecting and reporting system failures, including link failures.

R6-6 The NPAC/SMS shall not have more than nine hours of unscheduled downtime per year.

R6-7 If the NPAC/SMS experiences unscheduled downtime, the mean amount of time required to repair the NPAC/SMS shall be less than one hour.

R6-8 If a failure occurs which results in downtime for any functionality, the NPAC/SMS shall queue and process any transactions received prior to the failure after the functionality returns.

R6-9 If a general failure occurs, the capability of receiving activation notices and broadcasting changes shall be given the highest repair priority.

R6-10 The NPAC/SMS shall provide alternatives for link outages, such as alternate or redundant link capabilities or diverse routing.

6.4 Availability of the NPAC/SMS and the NPAC.

R6-11 The NPAC/SMS shall be available 24 hours a day, 7 days a week. The NPAC shall have personnel on site 24 hours a day, 7 days a week.
6.5 **Capacity Requirements.**

R6-12 The NPAC/SMS and the NPAC shall have the capacity to accommodate the actual level of transactions and data storage. Since many of those levels are unknown at this time, estimates are provided.

R6-13 The system shall be capable of allowing for 40 service providers having SOA and SMS interfaces.

R6-14 If additional capacity requirements are necessary to accommodate the needs of NPAC personnel who will be users of the NPAC/SMS, please describe in detail.

R6-15 Transaction rate projections are illustrated below.

**ESTIMATE OF TRANSACTIONS**

<table>
<thead>
<tr>
<th>Year</th>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year 1</td>
<td>120 million</td>
</tr>
<tr>
<td>Year 2</td>
<td>100 million</td>
</tr>
<tr>
<td>Year 3</td>
<td>120 million</td>
</tr>
<tr>
<td>Year 4</td>
<td>90 million</td>
</tr>
<tr>
<td>Year 5</td>
<td>90 million</td>
</tr>
</tbody>
</table>

R6-16 Cumulative archived record requirements are illustrated below.

<table>
<thead>
<tr>
<th>Year</th>
<th>Archived Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year 1</td>
<td>2.7 million</td>
</tr>
<tr>
<td>Year 2</td>
<td>5.0 million</td>
</tr>
<tr>
<td>Year 3</td>
<td>7.8 million</td>
</tr>
<tr>
<td>Year 4</td>
<td>9.8 million</td>
</tr>
<tr>
<td>Year 5</td>
<td>12.0 million</td>
</tr>
</tbody>
</table>

R6-17 Broadcasts shall occur within 60 seconds of activation notice.

6.6 **Disaster Recovery.**

R6-18 The NPAC/SMS shall have disaster recovery procedures in place. Such systems shall be adequate and sufficient to meet the downtime requirements in this Section 6.

R6-19 In the event a disaster limits either the NPAC/SMS or the NPAC from functioning, the capability of receiving uploads and processing broadcasts must be restored within 24 hours and full functionality must be restored within 48 hours.

**SECTION 7: USER SUPPORT**
The NPAC shall be responsible for user support as required. Specifically, the NPAC shall (a) provide appropriate training for users; (b) provide technical support for users; and (c) perform both initial and ongoing acceptance testing for any and all functionalities.

7.1 **User Training.**

R7-1 The NPAC shall be responsible for initial and ongoing training and user support.

R7-2 The NPAC shall train users, upon request, to:

(a) upload ported DN data and user data;
(b) receive and understand broadcasts;
(c) receive and understand error/success messages;
(d) request, receive, and understand mass changes;
(e) request, receive, and understand reports (including billing); and
(f) understand security measures.

7.2 **Technical Support.**

R7-3 The NPAC shall provide technical support for users who experience problems in:

(a) uploading ported DN data and user data;
(b) receiving and understanding broadcasts;
(c) receiving and understanding error/success messages;
(d) requesting, receiving, and understanding mass changes;
(e) requesting, receiving, and understanding reports (including billing); and
(f) understanding security measures.

R7-4 The NPAC shall provide the necessary technical support to correct any data transmission problems encountered in the interfaces between the NPAC/SMS and a user.

7.3 **Acceptance Testing.**

R7-5 The NPAC shall perform acceptance testing of the initial software and hardware configurations in the NPAC/SMS.

R7-6 The NPAC shall perform acceptance testing of all modifications or upgrades to software and hardware configurations in the NPAC/SMS. This software and hardware testing shall be scheduled so as not to inhibit the ongoing functionality of the NPAC/SMS.

R7-7 The NPAC shall resolve all problems encountered during testing.

R7-8 The NPAC shall document all testing procedures and test results and shall make those results available to users.

R7-9 The NPAC shall certify all NPAC/SMS software and hardware configurations before release for operation.

R7-10 The NPAC shall support a provider’s ongoing end-to-end system testing requirements.
SECTION 8: REPORTS

The NPAC and the NPAC/SMS shall have both defined and variable reporting capability.

R8-1 The NPAC shall be capable of generating ad hoc/free format reports and predefined reports. Such reports shall be available on-line or in hard-copy at the user's option.

8.1 Informational Reports.

R8-2 The NPAC and NPAC/SMS shall be capable of producing, upon request, the following informational reports:
   (a) reports on ported DN data (keyed on one or multiple fields for a single number or a range of numbers),
   (b) reports on non-proprietary user data (keyed on one or multiple fields for a single user or a range of users),
   (c) reports on the NPAC and NPAC/SMS performance (including CPU usage, number of transactions, mean time to complete broadcasts, and user link utilization), and
   (d) reports as may be required by regulatory agencies.

R8-3 For an interim period, the NPAC/SMS shall generate a report of portable NPA-NXXs. The NPAC/SMS shall also notify all users of new portable NPA-NXXs immediately upon notification by a service provider of a new portable NPA-NXX.

R8-4 The NPAC shall notify all users when it has received the first valid create message for a DN in an NPA-NXX; this message serves as a warning to those providers who have overlooked earlier notices that an NPA-NXX has been made portable.

R8-5 The NPAC is responsible for the accuracy of all informational reports.

8.2 Billing Reports.

R8-6 The NPAC/SMS shall maintain sufficient measuring and recording capability to produce an accurate bill to users.

R8-7 Billing reports for a particular user may be based on any combination of the following:
   (a) duration, date/time, service provider ID, user login ID, of login session;
   (b) number of transactions processed;
   (c) number of updates made (by type);
   (d) number of errors encountered in transactions;
   (e) number of errors encountered during transmission;
   (f) number of pending records maintained;
   (g) number of in effect records maintained;
   (h) number of archived records maintained;
   (i) number of records downloaded as normal action;
   (j) number of records sent in response to a resend request;
   (k) number of records resent due to transmission problems;
   (l) number of records in conflict;
   (m) number of records corrected (e.g., as result of audit);
(n) number of records queried/viewed;
(o) amount of data transported to user SMS as bulk load update; CPU usage; and
(p) failures and maintenance problems in the NPAC SMS.

R8-8 The billing reports from the NPAC and the NPAC/SMS must contain sufficient information to allow for each billed user to audit such reports.

8.3 Logs.

R8-9 The NPAC/SMS shall maintain complete and accurate logs of all transactions performed by the NPAC/SMS (including transactions requested by the NPAC).

R8-10 Each log shall contain sufficient detail to record the following information for each transaction: purpose or type of transaction, date, time, requesting entity, information received or provided, direction of data flow, and disposition of request.

R8-11 The NPAC/SMS shall be capable of retrieving the information in a log within 24 hours for logs less than two years old. Logs between two years and five years old shall be archived and retrievable within 7 days. Logs greater than 5 years old need not be maintained.

8.4 Periodic Data Verification.

R8-12 Upon request, the NPAC/SMS shall provide subscription data, in electronic format (FTP), sufficient to allow a provider to validate data in its system.

R8-13 The reports generated shall contain sufficient information to provide the requesting entity with any and all information necessary.

SECTION 9. SECURITY

The NPAC, the NPAC/SMS, all interfaces, and all data must be secure.

R9-1 The SMS shall support Security Framework for Telecommunications Management Network (TMN) Interfaces per ANSI T1.233-1993. The following requirements are intended to summarize the requirements in that document.

9.1 User Identification, Authentication, and Access Control.

R9-2 The NPAC and NPAC/SMS shall maintain an environment that requires each user to have a unique, auditable identity within the system.

R9-3 Each user must be verified or authenticated to enter the system or to access any data or transactions.

R9-4 The NPAC shall develop a secure system to issue user identifications and passwords. This system shall require authorized verified statements from the entity requesting access to the NPAC/SMS, and any other requirements that will guarantee protection of the individual user identification codes and passwords.
R9-5 The NPAC/SMS must maintain no default user identifications for any user or for the NPAC itself.

R9-6 The NPAC shall control the activation and deactivation of user identification codes and passwords. Passwords shall be determined by the user within standard password requirements.

R9-7 The NPAC/SMS shall require monthly changes in user identification codes and passwords. Passwords may not be reused for a period of six months.

R9-8 The system of user identification in the NPAC/SMS shall not allow for more than a minimal number of trials (default 3) for entry into the system and all such incorrect attempts shall be recorded.

R9-9 If the default number of failures is exceeded in R9-8, the NPAC/SMS shall not allow access for that user identification code for at least 60 seconds and the NPAC shall be immediately notified of such failure. Error messages shall not reveal any information about type of failure.

R9-10 Duplicate passwords for multiple user identification codes shall not be allowed.

R9-11 Unencrypted passwords shall not be available to NPAC or NPAC/SMS personnel.

R9-12 The NPAC must have a method of resetting a password.

R9-13 A suggested password scheme would be to require at least six alphanumeric characters, including at least one alphabetic and one numeric or punctuation character. The system must distinguish between upper and lower case passwords.

R9-14 A mechanism must exist to end the session through secure logoff procedures.

R9-15 The NPAC/SMS shall display a warning message to all people accessing the NPAC/SMS which describes that unauthorized access is restricted.

9.2 Data and System Integrity.

R9-16 The NPAC/SMS shall be able to identify the originator of any data received by the NPAC or NPAC/SMS.

R9-17 The NPAC/SMS shall develop controls to verify that the data received from any user is properly received and that data cannot affect the integrity of the system.

R9-18 The NPAC shall have internal controls to identify any problems within the NPAC/SMS data systems.

R9-19 The NPAC/SMS shall have controls to verify that interfaces are transmitting accurate and uncorrupted data.

9.3 Continuity of Service.
R9-20 No user action, either deliberate or accidental, shall cause the system to be unavailable to other users.

R9-21 Procedures for software and data backups and restoration shall be completely documented.


R9-22 The NPAC and NPAC/SMS shall ensure that no unauthorized access to the system can occur.

R9-23 The NPAC/SMS software vendor shall maintain all security requirements of the NPAC and the NPAC/SMS.

R9-24 The NPAC/SMS software vendor shall not design the software to permit unauthorized access to the NPAC/SMS.

SECTION 10: FUTURE CONSIDERATIONS AND REQUIREMENTS

The future of number portability and number administration are not known at this time. The NPAC/SMS should not be designed to preclude future expansion and adaptation.

R10-1 Please describe how the NPAC and NPAC/SMS may be adapted to accommodate the following situations if the contracting entity determines that such expansion or adaptation is necessary:

(a) Geographic number portability: This will require an increase in the size of each record and the database as a whole, and an increase in both the number of updates and the number of broadcasts. Geographic portability may be done in stages, such as initially being geographic portability beyond current rate centers but within a specific region.

(b) Pooled NXXs: This will require an increase in the size of the database due to all numbers within a shared NXX being in the database, and an increase in both the number of updates and the number of broadcasts. This may also require some number administration in the NPAC/SMS.

(c) Expansion for use by wireless service providers: The use of the NPAC/SMS by Commercial Mobile Radio Services (CMRS) providers may require new data fields and an increase in the number of transactions and types of service providers. CMRS providers covered under the FCC Report and Order include Cellular, broadband PCS, and covered Specialized Mobile Radio (SMR). It has not yet been determined what additional data field elements there will be for a wireless subscriber with a ported telephone number. Potential additional requirements those already identified for a ported subscriber might be an STP, SCP or MSC address for message routing to the Home Location Register (HLR) and/or a non-dialable mobile station identification (MSID) which could be a 10-digit or 15-digit format number. This list should not be considered to all-inclusive NPAC/SMS requirements for covered CMRS providers which will be determined by the wireless industry in upcoming industry meetings and will be made available upon determination.
ABBREVIATIONS

CLASS  Custom Local Area Signaling Services
CNAM  Caller ID with Name
DN  Directory Number (telephone number)
DPC  Destination Point Code
GTT  Global Title Translation
ISVM  Interswitch Voice Message
NPAC  Number Portability Administration Center
NPAC/SMS  Number Portability Administration Center/Service Management System
LATA  Local Access Transport Area
LIDB  Line Information Database
LNP  Local Number Portability
LRN  Local Routing Number
SOA  Service Order Administration
SMS  Service Management System
SSN  Subsystem Number

GLOSSARY

GTT - performed for CLASS and LIDB access features. A 10-digit GTT is now required for LNP (instead of the current 6-digit). This requires that the NPAC/SMS maintain the DPC and DPC-type (End-office or Gateway) information for the CLASS features and LIDB.

NPAC - Number Portability Administration Center which administers the NPAC/SMS

NPAC/SMS - The SMS is the hardware/software platform to receive, store, and broadcast information on ported DNs. The NPAC/SMS is the master database for information on ported DNs.

Local Number Portability - the ability to port DNs. There are three types: (a) service provider portability, (b) location portability, and (c) service portability.

Local SMS - the SMS used by a service provider that receives LNP data from the NPAC/SMS and distributes it to the service provider's internal network.

Location Routing Number - is a 10-digit number used to uniquely identify a switch that supports porting.

Ported DN - a telephone number for a customer that has changed service providers.

Subscription - the information recorded for a DN
Definition of TMN:

According to the (logical - not physical) layered TMN architecture model, the management functional areas can be distributed across an Element Layer (EL), an Element Management Layer (EML), a Network Management Layer (NML), a Service Management Layer (SML), and a Business Management Layer (BML). EL provides the support functions needed to manage a Network Element (NE), e.g., providing management data to the EML. EML deals with managing the technology and supplier specific aspects of the NEs. NML has a network wide view and deals with the end to end connectivity issues. It also gathers filtered performance and fault management data for the complete network view from EML. SML deals with the service specific management aspects of the services being offered. BML deals with broad business management aspects of telecommunications management (e.g., policy, constraints, and boundaries of the functionality in TMN). Different telecommunications services could be managed via common systems that implement functional TMN layer(s). We believe that the SMS falls within the boundaries of the SML (SMS), but will interface and have certain dependencies on other layers of the TMN model.

Advantages of TMN Model:

It facilitates the common understanding of telecommunications network management functions and interfaces for strategists, planners, systems engineers, and developers in both the supplier and provider communities.

With a common understanding of network management functions and interfaces established, the deployment of additional management functions without changing the basic network management architecture is facilitated, e.g., it saves time and money for deploying new services.

Differences in technology and network architecture minimize the effect on higher management layers, e.g., by having intelligence in the EML, the NML or SML could be insulated from NE supplier specific differences.

Standardized interfaces between the layers (e.g., information models, protocols, etc.) helps in supporting a multi-supplier environment.

Standardized interfaces also facilitates the integration of network management functions across different technologies where appropriate.
REQUEST FOR PROPOSALS FOR THE

NUMBER PORTABILITY ADMINISTRATION CENTER/ SERVICE MANAGEMENT SYSTEM (NPAC/SMS) in the

U S WEST REGION

September 16, 1996
SECTION 1: GENERAL INFORMATION

The purpose of this Request for Proposal ("RFP") is to invite you to submit a proposal to provide a Number Portability Administration Center ("NPAC") and Service Management System ("NPAC/SMS") to support the implementation of local number portability ("LNP") in the fourteen states in the U.S. WEST region.

It has been determined that:
(a) Location Routing Number (LRN) shall be the long-term network architecture employed;
(b) an NPAC shall administer an NPAC/SMS to receive, store, and broadcast this routing information; and
(c) a contracting entity shall be established to select an NPAC and NPAC/SMS vendor, contract with that vendor, and supervise that vendor’s performance.

1.1 Evaluation of Proposals. The contracting entity will evaluate all proposals from a total network and operations perspective to ensure integration with existing network and operating procedures. Specifically, the contracting entity, when accepting or rejecting a proposal, will consider (a) technical merit and creativity, (b) implementation schedule, (c) price, (d) quality, (e) bidder’s financial stability and performance history (including subcontractors), (f) ability to accommodate future considerations, (g) variance or deviations from specifications below, and (h) conflicts of interest. The contracting entity reserves the right to accept or reject any or all proposals made in response to this RFP based on any or all of the criteria identified in (a) through (h) above. Selection of the vendor and final contract approval may require approval by one or more state agencies.

1.2 Regulatory Oversight. This RFP, the contracting entity, the contract between the contracting entity and the vendor, and the ongoing operation of the NPAC may be subject to state Commission oversight and, as appropriate, approval. Additionally, the Federal government, through Congressional legislation, Federal Communications Commission rule making, or other mandates, may establish policies which affect this RFP, the contracting entity, the contract between the contracting entity and the vendor, and the ongoing operation of the NPAC.

1 Throughout this RFP the term NPAC/SMS is used to distinguish the SMS operated by the NPAC and SMSs operated by NPAC users.
1.3 Proposal.

1.3.1 Content of proposal.

TAB 1: Description of Vendor. The vendor shall identify itself and all subcontractors. The vendor shall also detail:

(a) the vendor's and all subcontractor's principal business;
(b) the vendor's and all subcontractor's related experience, in particular (1) any related telecommunications experience and (2) if the vendor has installed a similar system, identify the client, location, and date;
(c) the vendor's and any subcontractor's financial condition. Responses should include the vendor's and any subcontractor's most recent annual report or audited financial statement.

TAB 2: Conflict of Interest. The vendor shall verify that it does not have a conflict of interest as defined by Section 1.4 of this RFP.

TAB 3: Proposal Summary. The vendor shall summarize the system the vendor proposes and the system's strengths and weaknesses.

TAB 4: Technical Proposal. The vendor shall (a) describe the vendor's proposed system including (1) operating and database software and (2) hardware and (b) for each requirement detail, as specifically as possible, either (1) how the system will meet or exceed the requirement or (2) how the system will not meet that requirement as specified in this RFP and any justification for such exception or deviation. One potential justification for deviating from a requirement is if the vendor can demonstrate that an alternative approach will result in a superior product. A response that the vendor shall "comply" with the requirement without accompanying explanation as to how compliance will occur is insufficient. A statement that the vendor shall "develop a process" to meet a requirement is similarly insufficient without explanation of what that process is expected to entail.

TAB 5: Price. The vendor shall state the price. For purposes of this section, assume the contract will be for a five-year term. DO NOT INCLUDE COST OR PRICE FIGURES ANYWHERE EXCEPT IN YOUR TAB 5 RESPONSE.

1.3.2 Submission Information and Due Date. One copy of your proposal, complete in all respects, must be submitted to all of the addressees provided in the cover letter to this RFP.

Your cover letter shall include both the name(s) and phone number(s) of the individual(s) within your company who should be contacted in case any questions should arise during the evaluation of your proposal. Failure to direct your response to the address given above by the noted closing date may result in the disqualification of your proposal. The package containing your proposal shall be marked "Sealed Proposal" with this RFP title and your company's name.
Your proposal shall be in loose-leafed binders on typed double spaced on 8-1/2" x 11", 3-hole punched, white paper. Each volume shall begin on a new page and be separately tabbed. Diagrams, if applicable, shall not be in color. Additionally, an electronic copy in MS Word 6.0 format shall be provided.

1.3.3 Acceptance period. Your proposal shall indicate that it is valid for a period of at least one hundred eighty (180) days.

1.3.4 Confidentiality. Do not submit any proprietary or confidential information or mark it as such. In no event will the contracting entity consider or hold any information contained in your proposal proprietary or confidential, except for pricing information. The contracting entity reserves the right to release an average and range of the prices received.

1.3.5 Questions or Requests for Additional Information. Submit your question(s) or request(s) for additional information in writing to all of the facsimile numbers listed in the cover letter to this RFP no later than three days prior to the closing date for this RFP.

All questions and responses shall be promptly distributed to all recipients of this RFP. Please note that the identity of the requesting company shall be withheld. Telephone inquiries shall not be accommodated.

1.4 Conflict of Interest. The vendor must be a neutral third party, as may be defined by the FCC. Additionally, a neutral third party has no significant financial or market interest in providing local exchange service within the United States. To prevent a conflict of interest, the vendor shall not be: (a) a local exchange telecommunications service provider in the United States or (b) an entity (1) owned by, (2) which owns, or (3) affiliated through common ownership with any other local exchange telecommunications service provider in the United States (ownership interests of five percent (5%) or less shall not be considered ownership for purposes of this section). Once a vendor is selected, the vendor shall notify the contracting entity of any change in its neutral third party status. Such changes shall, in the sole discretion of the contracting entity, be cause for revocation of the contract.

1.5 Primary Vendor’s Acceptance of Key Business Terms and Conditions. Each Primary Vendor submitting a Pre-Qualification application to the CONTRACTING ENTITY must list the following key business terms and conditions and indicate its acceptance of these key business terms and conditions, as a pre-condition to being considered for a contract award as a Primary Vendor, by placing an “X” in the space next to each item listed. These terms and conditions are expected to form a part of the Master and Service Agreements to be executed with the Primary Vendor selected under this RFP, if any, and may not represent a full and complete listing of all contractual terms and conditions incorporated into those agreements.

KEY BUSINESS TERMS AND CONDITIONS ACCEPTED BY PRIMARY VENDORS

1. The CONTRACTING ENTITY, shall have the right to terminate the Contractual Agreement entered into through this RFP with the Primary Vendor for reasons of default (including, but not limited to, unauthorized assignment of agreement and failure to provide adequate Service), upon 30 days notice. The CONTRACTING ENTITY can avail itself of this termination option by simple majority vote of its membership. Also, the Primary Vendor is forbidden from making any unilateral changes to the Master or Service Contracts entered into under this RFP.
2. ______ The CONTRACTING ENTITY shall be granted appropriate license rights in and to any technology or other intellectual property that is developed for and at the request of the CONTRACTING ENTITY for the purposes of providing the Services; and Primary Vendor and Sub-Contractor(s), if any, shall agree to appropriate limitations on their use of any such technology or other intellectual property for purposes other than the express provision of the Services specified in the RFP.

3. ______ The Primary Vendor and Sub-Contractor(s), if any, shall deposit all technology and other intellectual property and related documentation under its control, that is necessary to the provision of these Services, with a mutually agreeable escrow agent for the use of the CONTRACTING ENTITY, or to allow another vendor the ability to provide Services, in the event of Supplier default (e.g., bankruptcy, failure to perform, etc.).

4. ______ The Primary Vendor and Sub-Contractor(s), if any, agrees to indemnify and save harmless the CONTRACTING ENTITY, its Members and their parents, subsidiaries, other affiliates, their direct and indirect customers, and the officers, directors, employees, successors, agents, representatives, successors and assigns of any and all of them (all hereinafter referred to in this clause as the "CONTRACTING ENTITY") from and against any and all claims, losses, damages, expenses, liabilities, suits demands, causes of action, including costs and reasonable attorney's fees, or liens that arise out of or result from:

   (i) Injury or death to persons, or loss or damage to any and all property, including theft, in any way arising directly or indirectly out of, or occasioned by, caused or alleged to have been caused by, or on account of, the performance of the Work or Services performed by Primary Vendor, or Sub-contractor(s), if any, or its agents, or any director, officer, employee, agent or representative under this Agreement,

   (ii) Assertions under Workers' Compensation or similar acts made by persons furnished by Primary Vendor, or Sub-Contractor(s), if any, or by reason of any injuries to such persons for which the CONTRACTING ENTITY would be responsible under Workers' Compensation or similar acts if the persons were employed by the CONTRACTING ENTITY,

   (iii) Any failure on the part of Primary Vendor, or Sub-Contractor(s), if any, to satisfy all claims for labor, equipment, materials and other obligations relating to the performance of the work hereunder, and;

   (iv) any failure by Primary Vendor, or Sub-contractor(s), if any, to perform its obligations under this clause, the insurance clause, or any clause in the Agreement.

Each party shall defend or settle, at its own expense, any action or suit against the other for which it is responsible hereunder and shall reimburse the other for reasonable attorneys' fees, interest, costs of suit and all other expenses incurred by the other in connection therewith. Each party shall notify the other promptly of any claim for which the other is responsible hereunder, and shall cooperate with the other in every reasonable way to facilitate the defense of any such claim.

5. ______ The Primary Vendor and Sub-Contractor(s), if any, shall be willing, at the CONTRACTING ENTITY's request, to obtain a bid and/or performance bond in an amount sufficient to guarantee performance of its obligation under the RFP.
6. The Primary Vendor and Sub-Contractor(s), if any, shall treat all information obtained from the CONTRACTING ENTITY or its Members and confidential and proprietary unless they can demonstrate that such information was previously known by the Supplier(s) without an obligation of confidentiality.

7. No information furnished by the Primary Vendor or Sub-contractor(s), if any, in response to the RFP or under any Contractual Agreement arising out of the RFP shall be considered confidential or proprietary, except the Tab 3, cost and Price information described in Tab 5.

8. The Primary Vendor and Sub-Contractor(s), if any, shall indemnify the CONTRACTING ENTITY and its members against any infringement claims arising from the provision of Services under this RFP.

9. During the term of this Agreement, the Primary Vendor and Sub-Contractor(s), if any, shall obtain and maintain, with financially reputable insurers (i.e., carriers with an A.M. Best rating of B+: VII, or better) which are licensed to do business in all jurisdictions where any work is performed and which are reasonably acceptable to CONTRACTING ENTITY, not less than the following levels of insurance coverage:

   a.) Worker's Compensation as provided for under any worker's compensation or similar law in any jurisdiction where any work is performed, with an Employer's liability limit of not less than $500,000 per accident or disease;

   b.) Commercial General Liability, including coverage for Contractual Liability and Products/Completed Operations Liability, with a limit of not less than $1,000,000 combined single limit per occurrence for bodily injury, property damage and personal injury liability (with contractual exclusion deleted), naming CONTRACTING ENTITY, its members, their directors, officers, employees, agents and/or representatives as additional insureds;

   d.) Umbrella/Excess liability with limits of not less than $9,000,000 combined single limit in excess of the above-referenced Employer's Liability, Commercial General Liability and Business Auto Liability coverage naming CONTRACTING ENTITY, its members, their directors, officers, employees, agents and/or representatives as additional insureds;

   e.) "All risk" Property insurance covering not less that the full replacement cost of Primary Vendor's and any Sub-Contractor(s), if any, personal property at risk due to this Agreement; and,

   f.) Errors and Omissions Insurance in the amount of at least $1,000,000 per claim with an annual aggregate of at least $3,000,000 inclusive of legal defense costs.

Waiver of Subrogation: Primary Vendor shall look first to any insurance in its favor before making any claim against CONTRACTING ENTITY, its members, their directors, officers, employees, agents and/or representatives for recovery resulting from injury to any person (including Primary Vendor's or Sub-Contractor's employees, if any) or damage to any property arising from any cause, regardless of negligence, and does hereby release and waive to the fullest extent permitted by law, and shall cause its insurers to waive, all rights of recovery against CONTRACTING ENTITY, its members, their directors, officers, employees, agents and/or representatives.

Certificates of Insurance: Primary Vendor and Sub-Contractors, if any, must as a material condition of this Agreement, prior to the commencement of any work and prior to the renewal thereof, deliver
to CONTRACTING ENTITY a certificate of Insurance, satisfactory in form and content to CONTRACTING ENTITY, evidencing that the above insurance is in force and contains a provision that it will not be cancelled or materially altered without first giving CONTRACTING ENTITY thirty (3) days prior written notice and that all coverage is primary to any insurance carried by CONTRACTING ENTITY or its members.

Nothing contained in this section shall limit Primary Vendor of Sub-Contractor’s, if any, liability to CONTRACTING ENTITY or its members to the limits of insurance coverage certified or actually carried.

10. The Primary Vendor shall submit a list of Sub-Contractor(s), if any, to the CONTRACTING ENTITY with its Pre-Qualifications submission, for review and approval. Any subsequent change in the use of any Sub-Contractor(s) shall require the review and approval of the CONTRACTING ENTITY.

11. The Primary Vendor and Sub-Contractor(s), if any, shall not have the right to assignment of the Contractual Agreement entered into through this RFP without the prior approval of the CONTRACTING ENTITY.

12. The governing law under this RFP and any Contractual Agreement entered into through this RFP shall be that of the state of Colorado, unless otherwise specified by the contracting entity.

13. In the event that the Service does not pass a mutually agreed upon Acceptance Plan, designed to determine the Primary Vendor’s system compliance with the functional and technical requirements of this RFP, the CONTRACTING ENTITY shall have the option to terminate the arrangement without any penalties whatsoever to it or its member carriers.

1.6 Subcontractors. The vendor shall be solely responsible for performance and shall be the single point of contact for the contracting entity. However, the vendor, at its option, may use its own resources exclusively or engage the services of subcontractors to provide one or more elements of the NPAC/SMS platform (hardware, software, etc.). Responses to this RFP shall clearly state the roles and responsibilities of any and all subcontractors which are providing parts of the proposed solution under the direction of the vendor.

1.7 Testing. Prospective vendors may be required, at the contracting entity’s sole discretion, to furnish components of their systems to the contracting entity for evaluation and testing and/or to make arrangements on their own premises for facilitating joint testing, at no charge. The contracting entity reserves the right to cancel the acceptance of a bid if the services or facilities do not pass acceptance tests.

1.8 Contract. The NPAC and NPAC/SMS shall be provided pursuant to a contract between the NPAC and the contracting entity. The contracting entity reserves the right to negotiate all terms and conditions of such a formal agreement. No contractual obligations are assumed by (a) issuing the RFP or (b) receiving, evaluating, or accepting, a vendor’s response. The contracting entity reserves the right to conduct negotiations with more than one vendor simultaneously.

1.9 Modification and Revision of RFP. This RFP may include unintended errors, omissions, and/or deficiencies. Therefore, the accuracy and completeness of this document and related documents are not guaranteed. The contracting entity reserves the right to modify the RFP at any time. The contracting entity
further reserves the right to cancel the RFP process without penalty at any time before a written contract is entered into.

SECTION 2: OVERVIEW OF THE ROLE OF THE NPAC AND NPAC/SMS

The NPAC/SMS is a hardware and software platform which contains the database of information required to effect the porting of telephone numbers in an LRN architecture. The NPAC/SMS shall not be involved in actual call routing, but rather shall receive, store, broadcast data on ported directory numbers ("DNs"), and provide informational reports based on the information contained in the database. This information is necessary to allow each user's network to properly route calls.

The NPAC shall manage the NPAC/SMS database. The NPAC shall be responsible for the maintenance and performance of the NPAC/SMS.

The NPAC/SMS Interoperable Interface Specification (IIS) shall define the interface between the NPAC/SMS and the Service Order Administration (SOA) system and the Local NPAC/SMS.

SECTION 3: RECEIVING, STORING, AND BROADCASTING PORTED DN DATA

Section 3 defines the data which the NPAC/SMS will receive, store, and broadcast. This section also identifies the existent states in which data may be within the NPAC/SMS.

3.1 Types of data to be received, stored, and broadcast.

R3-1 The NPAC/SMS shall, at a minimum, receive, store, and broadcast the following information on each ported DN: (Descriptions of these items can be found in the glossary that is attached to this RFP as an appendix.) See Section 3.1 of the NPAC/SMS Functional Requirements Specification (FRS) for a summary of the data elements administered and utilized by the NPAC/SMS.

<table>
<thead>
<tr>
<th>Data Item</th>
<th>Size</th>
<th>Receive</th>
<th>Store</th>
<th>Regular Broadcast</th>
<th>Disconnect Notice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone Number</td>
<td>10</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>LRN</td>
<td>10</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Facilities-Based Provider ID</td>
<td>4</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Disconnect Date</td>
<td>8</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Date Disconnect Broadcast Rec'd</td>
<td>8</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPC for CLASS</td>
<td>9</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSN for CLASS</td>
<td>3</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPC for LIDB</td>
<td>9</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSN for LIDB</td>
<td>3</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPC for ISVM</td>
<td>9</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSN for ISVM</td>
<td>3</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPC for CNAM</td>
<td>9</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSN for CNAM</td>
<td>3</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>End-user location (Future Use)</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Item</td>
<td>Size</td>
<td>Receive</td>
<td>Store</td>
<td>Regular Broadcast</td>
<td>Disconnect Notice</td>
</tr>
<tr>
<td>------------------------</td>
<td>------</td>
<td>---------</td>
<td>-------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Billing ID (Future Use)</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: If a SSN = 0, it implies that DPC IS the gateway.

R3-2 The NPAC may require additional fields for its uses. Additionally, future considerations may require additional types of data to be received, stored, and broadcast by the NPAC/SMS (See Section 9).

3.2 Receiving data.

R3-3 The NPAC/SMS shall be designed to interface electronically with three types of "users". First, large local exchange telecommunications providers will probably interface for purposes of uploading data into the NPAC/SMS and receiving broadcasts from the NPAC/SMS. Second, a small rural telecommunications provider may wish to interface with the NPAC/SMS for purposes of uploading data, but may elect to contract with another provider to maintain its routing information. Such a company, therefore, may not interface with the NPAC/SMS for receiving broadcasts. Third, an interexchange provider may only interface with the NPAC/SMS for purposes of maintaining routing information and, therefore, may not interface with the NPAC/SMS to upload information. Throughout this RFP, the term "user" is used generically. The Service Provider and Service Provider Network Data Scenarios shall be implemented as defined in Sections 6.3 and 6.4 of the IIS.

R3-4 The NPAC shall receive and record data needed to identify, contact, and bill new NPAC/SMS users. For example, the NPAC shall receive the LRNs, portable NXXs, network addresses for interfaces, and billing information. The NPAC/SMS shall verify that the correct facilities-based service provider ID is associated with the new user. A user shall require state regulatory commission approval to use the NPAC/SMS.

3.3 Storing and processing data.

R3-5 At a high level, the data associated with each ported DN may be described as either "pending", "in effect", and "archived". The Subscription Version Data associated with each ported DN shall be defined in Section 3.1.3 of the FRS.

R3-6 When a customer wishes to change service providers and keep the same telephone number, the new service provider shall instruct the NPAC/SMS to create a subscription associated with that customer's telephone number. The subscription shall be created in the pending state unless the subscriber already exists in pending. If the subscriber exists in pending, the NPAC shall reject any new request to create a subscription for that subscriber DN. The Subscription Version Flow Scenarios shall be implemented as defined in Section 6.5.1 of the IIS.

---

2 An order from the state regulatory commission which certifies a provider of exchange telecommunications services shall serve as official notification of provider status. Other users of the NPAC/SMS shall provide other official documentation which demonstrates the need to have access to NPAC/SMS data, e.g., certification as an interexchange carrier, providers of SCP/STP sites, etc.
When a subscription is in the pending state, the NPAC/SMS shall:
(a) verify the data;
(b) alert the old service provider of the creation of the subscription and allow the old service provider the opportunity to either confirm the data in the subscription or place the subscription into conflict;
(c) allow the new service provider the opportunity to cancel the subscription; and
(d) allow the new service provider the opportunity to activate the subscription when the new service provider effectuates the physical act of changing the customer's service.

The Subscription Version Flow Scenarios shall be implemented as defined in Section 6.5.1 of the IIS.

It is possible that the old service provider has the option to send a confirmation either before or after the new service provider sends a request to create a subscription. If this occurs, the NPAC/SMS shall:
(a) verify the data;
(b) alert the new service provider of the confirmation;
(c) if the new service provider sends a request to create a subscription within 90 days (tunable parameter), follow the process outlined in R3-7 (except step b); and
(d) if the new service provider does not send a request to create a subscription within 90 days (tunable parameter), delete the confirmation and issue error message.

When a customer who has already ported at least once changes service providers again, a subscription will be created in the pending state and, eventually, in the in effect state. At that time, the obsolete version of the subscription existing in the in effect state shall be stored by the NPAC/SMS in the archived state. Each archived version of a subscription shall be stored by the NPAC/SMS for 18 months (tunable parameter). The Subscription Version Flow Scenarios shall be implemented as defined in Section 6.5.1 of the IIS.

3.4 Conflict.

A subscription shall be placed into conflict if the initial information provided by the new service provider does not match the information provided by the old service provider. The Subscription Version Conflict Scenarios shall be implemented as defined in Section 6.5.5 of the IIS.

If a subscription has been placed into conflict the NPAC/SMS shall notify all affected users and save the information associated with the subscription for 30 days. The Subscription Version Conflict Scenarios shall be implemented as defined in Section 6.5.5 of the IIS.

A subscription which has been placed into conflict shall not be broadcast by the NPAC/SMS.

3.5 Modification.

The NPAC/SMS shall permit the new service provider to modify a subscription in the pending state. The NPAC/SMS shall verify all modified data. The Subscription Version Modification Scenarios shall be implemented as defined in Section 6.5.2 of the IIS.
R3-14 The NPAC/SMS shall permit the service provider to modify a subscription in the in effect state. The NPAC/SMS shall verify all modified data and rebroadcast the subscription. The Subscription Version Modification Scenarios shall be implemented as defined in Section 6.5.2 of the IIS.

3.6 Validations.

R3-15 When the NPAC/SMS receives and broadcasts data it shall perform the following validations: (a) all data must be in the proper format and (b) if a DN is being ported, (1) the LRN must be associated with a valid facilities-based provider, (2) the new facilities-based ID must match the new LRN, and (3) the NPA-NXX must be portable.

R3-16 If a confirmation is sent by the old facilities-based provider, the NPAC/SMS shall verify that the information sent by the old facilities-based provider matches the information sent by the new facilities-based provider.

3.7 Error/Success Messages.

R3-17 Whenever the NPAC/SMS is asked to perform a task or verify data, the NPAC/SMS shall issue an error message to the appropriate company(ies) if the task can not be successfully completed or if the data is improper. The error message shall, when possible, identify the cause of the failure or the improper data.

R3-18 Whenever the NPAC/SMS completes a task it was asked to perform or verifies that data is proper, the NPAC/SMS shall issue a success message to the appropriate company(ies).

3.8 Broadcasting data.

R3-19 When a subscription has been activated or modified in the in effect state, the NPAC/SMS shall broadcast the subscription to all users. If the NPAC/SMS is unable to transmit the data to a particular user, the NPAC/SMS shall repeat the attempt twice (tunable parameter) and, if the data has still not been successfully transmitted, contact the user and rebroadcast the data once the problem is solved. Once a subscription has been broadcast to at least one user, the subscription shall be in the in effect state. The Subscription Version Broadcast Scenarios shall be implemented as defined in Sections 6.5.1.5 through 6.5.1.7 of the IIS.

R3-20 A customer disconnect notice to the NPAC may include two dates: (1) the “customer disconnect date,” which is always present and (2) the “broadcast date”, which is sometimes present. The “broadcast date” indicates when the broadcast is to be made. If the “broadcast date” is not provided, the broadcast is immediate. The “customer disconnect date” is never included in the broadcasted information. However, the “customer disconnect date” is sent to the SOA of the local service provider to whom the NPA-NXX of the disconnected customer is assigned. This is done at the same time the disconnect broadcast is made. The Subscription Version Disconnect Scenarios shall be implemented as defined in Section 6.5.4 of the IIS.

R3-21 The NPAC shall filter, at an NPA-NXX level, the broadcasts and other messages sent to the provider’s local SMS. That is, a provider shall be able to specify the NPA-NXXs for which it wishes to receive information.
SECTION 4: INTERFACE DESCRIPTION

Section 4 describes the interfaces between a user and the NPAC/SMS. This section also describes the interface protocols and performance requirements. There are two potential interfaces. First, the NPAC/SMS must be able to interface with a user's Service Order Administration ("SOA") platform. Second, the NPAC/SMS must be able to interface with a user's SMS.

4.1 Interfaces.

R4-1 There shall be at least one NPAC/SMS actual or virtual point of presence (POP) in each state served by the NPAC/SMS. These POPs shall be located near a Metropolitan Statistical Area (MSA) in each state.

R4-2 The vendor shall be responsible for the facilities cost between each POP and the NPAC/SMS locations.

R4-3 Each proposal shall define the location of each POP and its actual type of transmission facility.

R4-4 An NPAC/SMS to user SMS interface shall support the actual exchange of ported DN data and any error or success messages associated with those transactions. An NPAC/SMS to SOA interface shall support all other transactions and reports.

R4-5 All interfaces shall support two-way communication in real-time and batch mode.

R4-6 The NPAC/SMS to user SOA interface shall accommodate Service Provisioning OSs and/or Gateway Systems. The NPAC/SMS to user SMS interface shall accommodate SMS (or SMS-like functions by a user SCP) and/or Gateway systems.

R4-7 All interfaces shall be capable of supporting multiple independent transactions. One failed item in a request shall not cause the other items in the request to fail.

R4-8 All interfaces shall be non-proprietary.

R4-9 A user may have multiple sessions running simultaneously with the NPAC/SMS application.

4.2 Interface Protocol.

R4-10 All system to system interfaces shall be implemented as defined in Section 2.2 of the IIS with the exception that ATM shall be included in the Link Layer.

R4-11 The NPAC/SMS IIS shall define the interface between the NPAC/SMS and the Local SOA.

R4-12 The IIS shall define the interface between the NPAC/SMS and the Local SMS.

R4-13 Section 6 of the IIS shall define the message flow scenarios between the NPAC/SMS and SOA systems, and between the NPAC/SMS and the Local SMSs.
R4-14 Section 7 of the IIS shall define the GDMO object definitions managed and utilized by the NPAC/SMS.

R4-15 Unless otherwise stated in this RFP, the requirements in the IIS shall provide all interface specifications.

R4-16 An additional, alternative NPAC/SMS to User-SOA interface shall be provided by the vendor to support communications via dial-up modem using the PPP protocol, and a vendor defined, secure, simple low-cost message protocol. A non-inclusive list of possible message protocols is shown below:
   a. A fixed format record for each SOA function that can be sent to, or received from, the NPAC/SMS.
   b. Sequential Query Language (SQL).
   c. Any other message protocol proposed by the vendor.

R4-17 The vendor defined, secure, simple low-cost message protocol, requested in R4-16, shall provide all SOA interface functionality that is required on the NPAC/SMS to User-SOA CMISE interface.

R4-18 The vendor shall provide an application that can operate on Windows 95™ or Windows NT™ that will allow the user to easily enter service order data and interface with the NPAC/SMS via the secure, simple low-cost message protocol.

R4-19 The Vendor’s response shall be specific in their description of any changes or losses in performance resulting from the use of the secure, simple low-cost message protocol described in R4-16.

4.3 Interface Performance Requirements.

R4-20 A transaction rate of 2 transactions per second shall be supported by each NPAC/SMS to user SOA interface. A transaction rate of 25 transactions per second shall be supported by each NPAC/SMS to user SMS interface. A transaction here refers to a transfer of data about a single DN, not to a CMISE transaction.

R4-21 Mass changes may be aggregated into a single file and broadcast in accordance with a file transfer mechanism, for example, FTP.

4.4 TMN Architecture.

R4-22 The SMS Supplier/Vendor must be in compliance with the Telecommunications Management Network (TMN) Architecture, including, but not limited to the following documents:
   (a) GR-2869-CORE, Generic Requirements for Operations Based on the Telecommunications Management Network (TMN) Architecture, Issue 1;
   (b) OAM&P - Protocols for Interfaces between Operations Systems in Different Jurisdictions (ANSI T1.224-1992);
   (c) TA-TSY-000899, Requirements Specifications for an Operations System (OS) to OS Interface using Generic OSI Protocols including the OSI Network Management Protocols (Consistent with ANSI T1M1.5);
SECTION 5: MASS CHANGES AND OTHER MAJOR DATA TRANSMISSIONS

Section 5 describes the requirements that the NPAC/SMS be able to accommodate mass changes and major data transmissions. There are three types of mass changes and major data transmissions which are contemplated: (a) NPA splits, (b) user takeover, and (c) System failure.

5.1 NPA Splits and Other Mass Updates. The splitting of an NPA is a complex process that can take well over a year to complete. NPAC shall maintain a close working relationship with organizations responsible for NPA split/mass changes scheduling because when an NPA split takes place a large amount of ported DN data may be added or require modification.

R5-1 The NPAC/SMS shall be capable of globally modifying a large amount of ported DN data when an NPA split occurs and maintaining the dual "in effect" records required to accommodate a permissive dialing period.

R5-2 The NPAC/SMS shall be able to analyze the impact of a proposed split on NPAC/SMS administrative tables and ported DN data.

R5-3 The Mass Update Scenarios shall be implemented as defined in Sections 6.6.3 and 6.6.4 of the IIS.

5.2 User Takeover. If a user with ported DNs is taken over by another user, all ported DN data associated with the old user may need modification to reflect the change.

R5-4 The NPAC/SMS shall be capable of globally modifying the appropriate ported DN data when a user is taken over by another.

5.3 System Failure. If a user's system fails and data becomes lost or otherwise corrupted, the user may require a complete transmission (FTP) of all ported DN data.

R5-5 The NPAC/SMS shall be capable of transmitting (FTP) all or some ported DN data to a specific user.
SECTION 6: PERFORMANCE CRITERIA

Section 6 describes the specific performance criteria requirements for the NPAC and the NPAC/SMS. These requirements include the reliability of the NPAC/SMS, the availability of the NPAC and the NPAC/SMS, the capacity requirements of the NPAC/SMS, and the capabilities for disaster recovery.

6.1 Continuity of Service.

R6-1 The NPAC/SMS shall not have more than 24 hours of scheduled downtime per year. Prior to any scheduled downtime, the NPAC shall notify all potentially affected users and attempt to minimize user impact.

R6-2 Except as provided in R6-1, system performance shall not be impaired or interrupted as a result of software upgrades, hardware upgrades, capacity expansion, to perform maintenance, or during back-up and recovery.

6.2 Reliability of the NPAC/SMS.

R6-3 The NPAC/SMS shall be highly reliable. The NPAC/SMS shall include data integrity features, symmetrical multi-processing capability, and economical and efficient system expansion capability.

R6-4 The NPAC/SMS shall maintain data integrity with 99.9% reliability. The NPAC/SMS shall perform all other functions with 99.9% reliability.

6.3 System Failure.

R6-5 The NPAC/SMS shall monitor the status of all of its functions, including communications links. The NPAC/SMS shall be capable of detecting and reporting system failures, including link failures.

R6-6 The NPAC/SMS shall not have more than nine hours of unscheduled downtime per year.

R6-7 If the NPAC/SMS experiences unscheduled downtime, the mean amount of time required to repair the NPAC/SMS shall be less than one hour.

R6-8 If a failure occurs which results in downtime for any functionality, the NPAC/SMS shall queue and process any transactions received prior to the failure after the functionality returns.

R6-9 If a general failure occurs, the capability of receiving activation notices and broadcasting changes shall be given the highest repair priority.

R6-10 The NPAC/SMS shall provide alternatives for link outages, such as alternate or redundant link capabilities or diverse routing.

6.4 Availability of the NPAC/SMS and the NPAC.

R6-11 The NPAC/SMS shall be available 24 hours a day, 7 days a week. The NPAC shall have personnel on site 24 hours a day, 7 days a week.
6.5 **Capacity Requirements.**

R6-12 The NPAC/SMS and the NPAC shall have the capacity to accommodate the actual level of transactions and data storage. Since many of those levels are unknown at this time, estimates are provided.

R6-13 The system shall be capable of allowing for 40 service providers having SOA and SMS interfaces.

R6-14 If additional capacity requirements are necessary to accommodate the needs of NPAC personnel who will be users of the NPAC/SMS, please describe in detail.

R6-15 Transaction rate projections are illustrated below.

**ESTIMATE OF TRANSACTIONS**

<table>
<thead>
<tr>
<th>Transactions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Year 1</td>
<td>120 million</td>
</tr>
<tr>
<td>Year 2</td>
<td>100 million</td>
</tr>
<tr>
<td>Year 3</td>
<td>120 million</td>
</tr>
<tr>
<td>Year 4</td>
<td>90 million</td>
</tr>
<tr>
<td>Year 5</td>
<td>90 million</td>
</tr>
</tbody>
</table>

R6-16 Cumulative archived record requirements are illustrated below.

<table>
<thead>
<tr>
<th>Archived Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year 1</td>
</tr>
<tr>
<td>Year 2</td>
</tr>
<tr>
<td>Year 3</td>
</tr>
<tr>
<td>Year 4</td>
</tr>
<tr>
<td>Year 5</td>
</tr>
</tbody>
</table>

R6-17 Broadcasts shall occur within 60 seconds of activation notice.

6.6 **Disaster Recovery.**

R6-18 The NPAC/SMS shall have disaster recovery procedures in place. Such systems shall be adequate and sufficient to meet the downtime requirements in this Section 6.

R6-19 In the event a disaster limits either the NPAC/SMS or the NPAC from functioning, the capability of receiving uploads and processing broadcasts must be restored within 24 hours and full functionality must be restored within 48 hours.

**SECTION 7: USER SUPPORT**
The NPAC shall be responsible for user support as required. Specifically, the NPAC shall (a) provide appropriate training for users; (b) provide technical support for users; and (c) perform both initial and ongoing acceptance testing for any and all functionalities.

7.1 User Training.

R7-1 The NPAC shall be responsible for initial and ongoing training and user support.

R7-2 The NPAC shall train users, upon request, to:
(a) upload ported DN data and user data;
(b) receive and understand broadcasts;
(c) receive and understand error/success messages;
(d) request, receive, and understand mass changes;
(e) request, receive, and understand reports (including billing); and
(f) understand security measures.

7.2 Technical Support.

R7-3 The NPAC shall provide technical support for users who experience problems in:
(a) uploading ported DN data and user data;
(b) receiving and understanding broadcasts;
(c) receiving and understanding error/success messages;
(d) requesting, receiving, and understanding mass changes;
(e) requesting, receiving, and understanding reports (including billing); and
(f) understanding security measures.

R7-4 The NPAC shall provide the necessary technical support to correct any data transmission problems encountered in the interfaces between the NPAC/SMS and a user.

7.3 Acceptance Testing.

R7-5 The NPAC shall perform acceptance testing of the initial software and hardware configurations in the NPAC/SMS.

R7-6 The NPAC shall perform acceptance testing of all modifications or upgrades to software and hardware configurations in the NPAC/SMS. This software and hardware testing shall be scheduled so as not to inhibit the ongoing functionality of the NPAC/SMS.

R7-7 The NPAC shall resolve all problems encountered during testing.

R7-8 The NPAC shall document all testing procedures and test results and shall make those results available to users.

R7-9 The NPAC shall certify all NPAC/SMS software and hardware configurations before release for operation.

R7-10 The NPAC shall support a provider's ongoing end-to-end system testing requirements.
SECTION 8: REPORTS

The NPAC and the NPAC/SMS shall have both defined and variable reporting capability.

R8-1 The NPAC shall be capable of generating ad hoc/free format reports and predefined reports. Such reports shall be available on-line or in hard-copy at the user's option.

8.1 Informational Reports.

R8-2 The NPAC and NPAC/SMS shall be capable of producing, upon request, the following informational reports:
   (a) reports on ported DN data (keyed on one or multiple fields for a single number or a range of numbers),
   (b) reports on non-proprietary user data (keyed on one or multiple fields for a single user or a range of users),
   (c) reports on the NPAC and NPAC/SMS performance (including CPU usage, number of transactions, mean time to complete broadcasts, and user link utilization), and
   (d) reports as may be required by regulatory agencies.

R8-3 For an interim period, the NPAC/SMS shall generate a report of portable NPA-NXXs. The NPAC/SMS shall also notify all users of new portable NPA-NXXs immediately upon notification by a service provider of a new portable NPA-NXX.

R8-4 The NPAC shall notify all users when it has received the first valid create message for a DN in an NPA-NXX; this message serves as a warning to those providers who have overlooked earlier notices that an NPA-NXX has been made portable.

R8-5 The NPAC is responsible for the accuracy of all informational reports.

8.2 Billing Reports.

R8-6 The NPAC/SMS shall maintain sufficient measuring and recording capability to produce an accurate bill to users.

R8-7 Billing reports for a particular user may be based on any combination of the following:
   (a) duration, date/time, service provider ID, user login ID, of login session;
   (b) number of transactions processed;
   (c) number of updates made (by type);
   (d) number of errors encountered in transactions;
   (e) number of errors encountered during transmission;
   (f) number of pending records maintained;
   (g) number of in effect records maintained;
   (h) number of archived records maintained;
   (i) number of records downloaded as normal action;
   (j) number of records sent in response to a resend request;
   (k) number of records resent due to transmission problems;
   (l) number of records in conflict;
   (m) number of records corrected (e.g., as result of audit);
(n) number of records queried/viewed;
(o) amount of data transported to user SMS as bulk load update; CPU usage; and
(p) failures and maintenance problems in the NPAC SMS.

R8-8 The billing reports from the NPAC and the NPAC/SMS must contain sufficient information to allow for each billed user to audit such reports.

8.3 Logs.

R8-9 The NPAC/SMS shall maintain complete and accurate logs of all transactions performed by the NPAC/SMS (including transactions requested by the NPAC).

R8-10 Each log shall contain sufficient detail to record the following information for each transaction: purpose or type of transaction, date, time, requesting entity, information received or provided, direction of data flow, and disposition of request.

R8-11 The NPAC/SMS shall be capable of retrieving the information in a log within 24 hours for logs less than two years old. Logs between two years and five years old shall be archived and retrievable within 7 days. Logs greater than 5 years old need not be maintained.

8.4 Periodic Data Verification.

R8-12 Upon request, the NPAC/SMS shall provide subscription data, in electronic format (FTP), sufficient to allow a provider to validate data in its system.

R8-13 The reports generated shall contain sufficient information to provide the requesting entity with any and all information necessary.

SECTION 9. SECURITY

The NPAC, the NPAC/SMS, all interfaces, and all data must be secure.

R9-1 The SMS shall support Security Framework for Telecommunications Management Network (TMN) Interfaces per ANSI T1.233-1993. The following requirements are intended to summarize the requirements in that document.

9.1 User Identification, Authentication, and Access Control.

R9-2 The NPAC and NPAC/SMS shall maintain an environment that requires each user to have a unique, auditable identity within the system.

R9-3 Each user must be verified or authenticated to enter the system or to access any data or transactions.

R9-4 The NPAC shall develop a secure system to issue user identifications and passwords. This system shall require authorized verified statements from the entity requesting access to the NPAC/SMS, and any other requirements that will guarantee protection of the individual user identification codes and passwords.