SECTION 1: GENERAL INFORMATION

1.1 Introduction

1.1.1 Purpose of Request for Proposal

The purpose of this Request for Proposal (RFP) is to invite you to participate in submitting a total solution and associated firm pricing proposal to provide a Number Portability Administration Center and Service Management System (NPAC/SMS) to support the implementation of Local Number Portability in the Chicago LATA 358 in the state of Illinois. Your response should be based upon the specifications provided in this RFP and should contain detailed information on degree of compliance to requirements, pricing and availability.

The Selection Committee consisting of Ameritech, AT&T Corp., TCG, MCI Metro, Sprint/Centel and MFS will evaluate all proposals from a total network and operations perspective to ensure integration with existing network and operating procedures. Proposals will also be assessed on their ability to evolve, as necessary, from serving a limited geographic area to a nationwide service and with minimal obsolescence of existing investment.

Prospective vendors may be required to furnish components of their systems to the Selection Committee for evaluation and testing and/or to make arrangements on their own premises for facilitating joint testing, at no charge.

1.1.2 Use of RFP Information

You shall use this RFP and any other information furnished to you under this RFP solely for the purposes of responding to this RFP. All such documents and information you receive shall remain the property of the Selection Committee, shall be kept confidential and shall be returned to the Selection Committee upon request. Reproduction of any part of this RFP is authorized only for the preparation of your response. You shall not disclose this RFP to any of your employees who do not have a "need to know" or to any third party working with or for you without the prior written consent of the Selection Committee. You shall ensure that all such copies (both paper and computer form) are destroyed when no longer required in connection with this RFP.

1.1.3 Vendor's Information

Do not submit any proprietary or confidential information or mark it as such. Information furnished by you to the Selection Committee pursuant to this RFP shall not be considered by you to be confidential or proprietary. In no event will the Selection Committee consider or hold any information contained in your proposal proprietary or confidential, except for pricing information.

1.1.4 Background

1.1.4.1 History of LNP Activities in Illinois to Date

An industry task force was formed in Illinois in April 1995, pursuant to the Illinois Commerce Commission (ICC) Order on Customers First Plan (Docket 94-0096 dated April 7, 1995), to develop a permanent number portability solution for Illinois. During the year, this task force has made significant progress in defining and resolving the issues related to implementing number portability. Among other things, the task force has determined that:

-Initially, only wireline service provider portability within existing LEC rate centers will be implemented.

- The long-term architecture for routing calls will be Location Routing Number (LRN).

- The target date for LRN implementation is second quarter 1997.

Consistent with the timetable, it is the intention of the task force to select an NPAC/SMS vendor on or about the end of the first quarter 1996, start system testing in the fourth quarter 1996, with projected full functional operability in the second quarter 1997.

1.1.4.2 Impact of Federal Regulation and Legislation on this Procurement

This RFP is being issued by a group of service providers who currently provide or intend to provide facilities-based local exchange services in the state of Illinois. LNP implementation is subject to oversight by the Illinois Commerce Commission (ICC). However, bidders should be aware that the Federal government, through Congressional legislation, Federal Communications Commission rule making, or other mandates, may establish policies for local competition which may affect the operation of the NPAC.

1.2 Description of LNP Environment

1.2.1 LNPArchitecture
The Illinois Local Number Portability task force has selected the Location Routing Number (LRN) architecture to enable the correct routing of calls in this number portability environment. A high-level description of the LRN architecture is presented in Section 16, Figure 5 (Part 1 and 2).

1.2.2 Functions of the SMS
The Service Management System is a hardware and software platform which contains the database of information required to effect the porting of telephone numbers. In general, the SMS receives customer information from both the old and new service providers (including the new Location Routing Number), validates the information received, and downloads the new routing information when a "activate" message is received indicating that the customer has been physically connected to the new service provider's network The SMS also

contains a record of all ported numbers and a history file of all transactions relating to the porting of a number. The SMS shall also provide audit functionality and the ability to retransmit LNP information to service providers under certain conditions. The SMS is not involved in real time call processing.

1.2.3 Management and Integration Role of NPAC

The NPAC shall provide management oversight for and integration of the data center operations and software development and maintenance functions. It shall have responsibility for achieving performance standards established by the industry and for providing user and technical support services and training for industry participants.

1.3 Eligibility to Submit Proposals

1.3.1 Prime Vendor

NPAC/SMS business shall be awarded to a single Prime Vendor who shall be responsible for providing a total solution encompassing the NPAC functionality and the SMS platform (both hardware and software). The Prime Vendor shall be responsible for all NPAC administration duties and system performance adherence in accordance with the requirements of this RFP. The Prime Vendor shall be the single point of contact for the Contracting Entity. The Prime Vendor shall be required to submit a comprehensive proposal to provide all elements of the solution. At its option, the Prime Vendor may use its own resources exclusively or engage the services of subcontractors to provide one or more elements of the SMS platform (hardware, software, etc.) or other elements of the total solution.

1.3.2 Neutral Third Party

NPAC/SMS business shall be awarded to a Prime Vendor and/or NPAC administrator who is a "neutral third party." A neutral third party is an entity which:

l) is not a telecommunications service provider. A telecommunications service provider is an entity which provides, for generally-available public use, the transmission of information by electromagnetic or optical means;

2) is not owned by, or does not own, any telecommunications service provider. Ownership interests of five percent (5%) or less shall not be considered ownership for purposes of this section;

3) is not affiliated, by common ownership or otherwise, with a telecommunications service provider.

1 .3.3 Subcontractors

Responses to this RFP shall clearly state the roles and responsibilities of any and all subcontractors which are providing parts of the total solution under the direction of the Prime Vendor.

1.3.4 Additional Qualifications

1.3.4.1 General Background of Bidder(s)
RFP responses shall contain a concise description of the principal business of the Prime Vendor and any subcontractors, including such items as company background, characteristics of business strength, performance support for a multiyear business award, accomplishments and capabilities which demonstrate a strong foundation for managing and operating the NPAC, policies and procedures that will ensure evenhanded treatment of all carriers, and certification that the Prime Vendor and any subcontractor shall comply with the provisions of this Section.

1.3 .4.2 Industry Experience
RFP proposals shall include a concise description of the telecommunications experience of the Prime Vendor and any subcontractors, including such items as products and services offered, customers served, successful performance of the functional skills required by this RFP on activities performed for other customers, and customer benefits that resulted from such successful performance.

1.3.4.3 Financial Stability
RFP proposals shall include a concise description of the financial condition of the Prime Vendor and any subcontractors. Responses should include the most recent annual report or audited financial statement of the Prime Vendor and any subcontractors. Proposals shall include all characteristics of bidder(s) financial strength to support a multi-year business award.

1.4 Preparation of Responses

1.4.1 Proposal Submission
Your proposal, complete in all respects, must be submitted to the following address:
M. Gary Berg
2000 West Ameritech Center Drive
4C87A
Hoffman Estates, IL 60196-1025
Your cover letter should 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.

Please give written notice of your interest to respond as soon as possible to the above address, **but no later than February 12, 1996.** If you would like to validate your neutrality status as a Prime Vendor please submit this request at the same time and you will be notified within ten working days. This validation will not impact the timeframe for response to this RFP. In addition, upon receipt of your interest to bid, a sample contract will be provided.

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.

1.4.2 Closing Date

All proposals in response to this RFP shall be received NO LATER THAN 12:00 Noon (Central Standard Time), **March 18, 1996.**

1.4.3 Response Composition

You shall submit seven (7) sets (hard copy and diskette copy in IBM DOS format, Word 5.0/ Excel 4.0) of copies of your proposal. Please mark all pages of one (1) paper copy "Master Copy". If discrepancies between copies and/or the diskette are found, the "Master Copy" will govern.

Your proposal shall be typed double spaced on 8-1/2" x 11" 3-hole punched paper with each volume beginning on a new page and separately tabbed.

You are requested not to make your proposal elaborate with respect to binding or presentation. A simple, straightforward. economically reproduced proposal is strongly recommended. Our proposal evaluation procedure places a higher premium on thoroughness of presentation, i.e., responsiveness, rather than on quantity of material included.

1.4.4 Questions or Requests for Additional Information

Submit your question(s) or request(s) for additional information in writing to the following facsimile number listed below no later than **February 22, 1996** prior to the closing date for this RFP.

847 248-3284
ATTN: M. Gary Berg

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 will not be accommodated.

1.4.5 Acceptance Period

Your proposal shall indicate that it is valid for a period of at least one hundred eighty (180) days from the closing date.

1.4.6 Contract Award
The contracting entity or entities of the Selection Committee reserve the right:
a) to reject any and all responses:
b) to conduct negotiations with more than one vendor simultaneously
c) to add, delete and/or change the terms of this RFP and to issue corrections and amendments to the RFP
d) to accept or reject, in whole or in part, any response without giving any reason for the decision

e) to enter into a contractual arrangement with any vendor and is not limited by any event associated with this RFP

f) to have any documents submitted by a vendor reviewed and evaluated by any individuals, including, independent consultants;

and
g) to cancel the RFP process without penalty at any time before a written contract is entered into.

1.4.7 No contractual obligations are assumed by issuing the RFP, receiving, accepting, and evaluating the vendor's response, and/or making a preliminary vendor seleciion.

1.4.8 The Selection Committee reserves the right to cancel any agreement if the services or facilities do not pass mutually agreeable acceptance tests. This will be done at no cost or obligation to the Selection Committee contracting entity or entities.

1.4.9 The Selection Cornmittee contracting entity or entities reserve the right to negotiate all terms and conditions in order to enter into a formal agreement with the successful vendor. This document, the vendor's response, and full system documentation will form part of the agreement.

1.4.10 No publicity or news releases pertaining to this RFP, responses to this RFP, discussions of any kind regarding the RFP, or the award of any agreement related to the bid document may be released without the prior written approval of the Selection Committee.

1.4.11 All work and materials must comply with all federal and state law, municipal ordinances, regulations, and directions of inspectors appointed by proper authorities having jurisdiction.

1.4.12 The vendor shall not assign, transfer, or sublet the RFP service agreement or any interest therein or any part thereof without prior written consent. All subcontractors must be identified and approved prior to disclosure of any information. If subcontracting is involved, the primary vendor shall be responsible for the workmanship, costs, etc. Incurred by the sub-contractor in the performance of their duties.

1.4.13 The vendor, by stating compliance to a requirement in this RFP, agrees that the vendor has read and understood the requirement and that compliance is complete and deliverable at no additional cost unless otherwise noted.

1.4.14 This RFP may include unintended errors, omissions, and/or deficiencies. Therefore, the accuracy and completeness of this document and related documents are not guaranteed. In the event that such errors, omissions, and/or deficiencies are discovered by the vendor, the vendor shall notify the Selection Committee in writing within 48 hours.

The vendor is expected to examine the specifications and instructions carefully. Calculation errors shall be the vendor's risk. In the event of a vendor's error in price, time or calculations, quoted items shall prevail.

1.5 Additional Contractual Terms and Conditions This section identifies contractual terms and conditions that the contracting entity intends to incorporate into the Agreement. The following list is in addition to the terms and conditions specified in the RFP.

1. Conformity with Law Vendor shall comply with all applicable FCC rules and federal, state, and local statutes, regulations and case law.
2. Indemnification Vendor shall provide indemnification with regard to damage, death, or personal injury due to vendor's acts or omissions.

3. Trademarks and Publicity

Vendors shall have no rights to use names or trademarks.

4. Confidentiality Vendor shall not disclose confidential information.

5. Termination The Agreement shall establish the right of termination without liability if vendor substantially defaults in performing obligations.

6. Limitation of Liability Except specifically provided in the Agreement, there shall be no liability for vendor's damages.

7. Taxes Vendors shall file all tax returns required by law to be filed by vendor: vendor shall provide access to relevant documents for tax audits.
8. Insurance Vendor shall maintain worker's compensation insurance, employer's liability insurance, comprehensive general liability insurance, and motor vehicle insurance.
9 Authonty Vendor shall represent and warrant that vendor has approval and authority to execute the Agreement.
10. Mechanic's Lien Vendor shall perform services free of mechanic's lien or other liens.

1.6 Preparation of Proposal Response

1.6.1 Content Structure You are responsible for any and all costs incurred in the preparation of your response to this RFP. Your proposal shall consist of the following separate Tabs: Tab 1 Proposal Summary Tab 2 Functional and Technical Requirements Tab 3 Cost and Price

DO NOT INCLUDE COST OR PRICE FIGURES ANYWHERE EXCEPT IN YOUR TAB 3 RESPONSE, THE COST AND PRICE SECTION.

All proposals meeting the stated requirements and specifications except for minor exceptions and deviations, shall be considered. Failure to meet requirements may disqualify a proposal from the selection process. However, proposals having minor exceptions and deviations shall be considered only if the following conditions are satisfied: (a) all exceptions and deviations from the specifications are explicitly stated in the Proposal Summary; and (b) all exceptions and deviations are appropriately justified on the basis of performance, schedule and/or relative price.

1.6.2 Tab Content

The required content of each tab of your proposal follows:

Proposal Summary (TAB 1)

This tab should summarize all key features of your proposal response. All deviations and exceptions from the RFP should be stated, and a brief justification given. A more detailed justification can be included in the tab that covers the subject.

Functional and Technical Requirements (TAB 2)

This section should discuss the major aspects of the functional design. You should address

(1) all areas which result in a potentially high degree of risk
(2) all areas which impose an unusually high degree of responsiveness, and

(3) areas that are deficient and that could be improved.

Cost and Price (TAB 3)

This tab shall include a description of the proposed costs and prices. All pricing information shall be limited solely to this tab of your proposal. For purposes of your response you should provide both a three year and five year view. (See Section 10, R10-17 and 18) This tab should address all requirements set forth in this RFP as well as any other items pertinent to your proposal pricing such as additional discounts for increased volume, prompt payment, transportation charges (FOB destination)etc. Pricing shall also be firm for all orders place through December 31, 2001, and shall be based on the EF&I of all applicable goods, software, and services of the most recent vintage and/or technology available in the telecommunications industry.

1.7 Evaluation of Proposals

The criteria to be used for the proposal evaluation include:
(a) technical merit
(b) schedule
(c) price and cost
(d) quality considerations
(e) responsiveness to contract provisions

(f) Prime's financial stability, history, including program management

No weighting or relative importance of criteria is intended or implied by this list.

You shall furnish all information as requested per the applicable instructions providing sufficient data to enable us to evaluate the proposal. Any deviations or exceptions to the RFP should be noted. Any supplier who does not completely reply to the proposal as requested may be eliminated at the discretion of Selection Committee.

The same article, section or paragraph number and title used in the RFP shall be used for your comments.

In the cases where your reply is "will not be complied with" or "not agreed to", you shall indicate your reasons for such disagreement and provide an alternative with which you will comply or agree.

SECTION 2: BUSINESS PROCESS FLOWS

The following process flows indicate how the NPAC and NPAC/SMS are used in the various business processes associated with number portability. This information is intended to provide an overview of the role of the SMS in number portability. Details of steps in the processes that do not involve the NPAC or NPAC SMS, such as interactions between service providers, will be determined by the service providers and are beyond the scope of this document. Specific requirements generated by the process flows are included in the appropriate sections later in the document.

2.1 **Provision Service Process**

This process flow defines the provisioning flow in which a customer ports a telephone number to a new service provider.

The new service provider will obtain authorization to port the customer and notify the old service provider according to processes internal to the service providers. Both the old and new service providers will send a notification to the NPAC SMS from their Service Order Administration Systems. When the NPAC SMS receives the notification(s), it will perform certain validation checks, including that both the old and new service provider has sent a notification. If errors are found or both service providers did not send notifications, the SMS will enter into a coordination process described in the next paragraph. Assuming the notifications are valid, the two service providers will complete any physical changes required. At the time new service provider is ready to provide service, it will send an activation notice to the NPAC SMS. The NPAC SMS will place an activation time stamp on the update and broadcast the update out in real time to all local service providers' networks. Upon receiving the update from the NPAC SMS, all service providers will update their networks. The NPAC SMSwiU record any transmission failures and take the appropriate action.

In the case where either the old or new service providers did not send a notification to the NPAC SMS, the NPAC SMSwiU notify the service provider from which it did not receive a notification that it is expecting a notification. If it then receives the missing notification and the notifications indicate agreement among the service providers, the process proceeds as normal. If it still does not receive a notification and if it is the old service provider that failed to respond, the NPAC SMSwiU log the failure to respond and then the process proceeds as normal. If it was the new service provider that failed to respond, the NPAC will log the failure to respond, cancel the notification, and notify the old service provider of the cancellation. If there is disagreement among the service providers as to who will be providing service for the telephone number, the conflict resolution procedures will be implemented. Processes for obtaining authorization from the customer to port a number are defined by the service providers. The NPAC is not involved in obtaining or verifying authorization.

From the time the new service provider sends a notification to the time it sends the activation notice, the new service provider may send a message to the NPAC SMS to cancel the notification. If this occurs, the NPAC SMS will remove the notification from its database and notify the old service provider that the notification has been canceled.

(refer to Figure 1 in Attachments)

2.2 **Disconnect Process**

When a ported number is being disconnected, the customer and service provider will agree on a date. After an aging period, if any, the service provider will send an update indicating the disconnect to the NPAC SMS. The NPAC SMS will broadcast the update to all service providers and remove the telephone number from its database of ported numbers. Upon receiving the update, all service providers will remove the telephone number from their LNP databases. The NPAC SMS will log the update in history. Calls to the telephone number will be routed as a nonported number.

In both the service provisioning process and disconnect process, when the NPAC SMS is performing validity checks (such as confirming that required data fields are filled in), if an error is found, the NPAC SMS will notify the service provider's with an appropriate error message. The service provider will have to resend the notification to have it processed.
(refer to Figure 2 in Attachments)

2.3 Repair Service
A problem will be detected either by a service provider or by a customer contacting a service provida.

There will be audit capabilities in the NPAC SMS to aid in isolating problems. If an inaccuracy is found, the NPAC SMS will broadcast the correct data to any involved local service provider to correct inaccuracies.

(refer to Figure 3 in Attachments)

2.4 Conflict Resolution Process
If service providers disagree on who will serve a particular line number, the NPAC will place the request in "conflict" and notify both service providers. The service providers will determine who will serve the customer via internal processes. When a resolution is reached, the NPAC will be notified and will remove the request from "conflict" or cancd it.

2.5 **Disaster Recovery and Backup Process**
If there is planned downtime for the NPAC SMS, the NPAC SMS will send an electronic notification to the service provider's SOAs that includes information on when the downtime will start, how long it will be and if they will be required to switch to the backup or disaster recovery machine. Downtime is considered planned when the NPAC can provide notification to the service providers at least 24 hours in advance. If the downtime will be less than 60 minutes, the service providers will remain connected to the primary machine and not send any updates during the downtime. If the downtime will be longer than 60 minutes, the NPAC service providers will switch to the backup or disaster recovery machine as indicated in the notification. There will be a quiet period (minutes) when no updates can be sent in order to allow the NPAC to coMect the service providers to the proper machine. At the end of the quiet period, processes will proceed as normal. When the primary machine is brought back up, the backup or disaster recovery machine will send an electronic notification to the service providers' SOAs indicating the time the NPAC will switch them back to the primary machine. At the end of the quiet period, processes will

continue as normal and the NPAC will synch up the database in its primary SMS with any updates sent to the backup or disaster recovery machine during the downtime.

If there is unplanned downtime, the NPAC will assess how long the primary machine will be down. The NPAC will notify all of the service providers by telephone calls to the service providers' contact numbers of the situation and planned action. If the downtime is expected to be less than 60 minutes, the service providers will remain connected to the primary machine and not send any updates during the downtime. If the downtime will be longer than 60 minutes, the service providers will switch to the backup or disaster recovery machine and later back to the primary using the same process as described for planned downtime. In addition, once the service providers have been switched off of the primary machine, each service provider will check to see if any updates of newly ported numbers sent to the primary machine during the time it went down were not broadcast out. If a service provider finds such updates, the service provider may use internal inter-carrier processes to update its own SCPs and have other carriers update their SCPs with the information in order to ensure service to the affected customers. This will not be needed for disconnect orders. Even if it finds such updates, a service provider may choose to wait until it can begin sending updates to the backup or disaster recovery machine and then just resend the updates that had died in the primary machine. If a service provider does use internal processes to request updates to SCPs while waiting to be able to send them to the backup or disaster recovery machine, the service provider will still resend the updates when backup or disaster recovery machine can begin processing them in order to ensure every service provider and the NPAC SMS receive the update.
(refer to Figure 4 in Attachments)

3.1 Overview The NPAC SMS manages the ported TN information associated with the service provider portability for the LNP service.

3.1.1 Service Data The Service Data contains global parameters specific to the LNP service. Examples of some of these parameters are described below. The description presents a logical representation of the data, not an implementation view. Time interval for concurrence from both service providers (Section 5, R5-21) Number of retries for download to Local SMS (Section 5, R5-59) Time interval a subscription version stays in conflict (Section 5, R5-44)

3.1.2 Service Provider Data Service Provider Data contains information about service providers participating in the LNP service. The data items that need to be administered by Service Provider Data Administration include (but are not limited to): A. Service Provider Name B. Facility-based Service Provider Identification C. Service Provider Address D. Service Provider Phone E. Service Provider Contact F. Service Provider Repair Center Information G. Service Provider System Data Link Information

3.1.3 Subscription Data Subscription Data consists of information about the ported TNs. The data items that need to be administered by Subscription Data Administration functions are described below. The description presents a logical representation of the data, not an implementation view. Table 3-1 describes the data items associated with each ported TN that are maintained by the NPAC SMS. Size of the data items is in bytes.

TABLE DID NOT SCAN

3.1.4 Network Data

The data items that need to be administered by Network Data Administration functions are described below. The description presents a logical representation of the data, not an implementation view.
A. Participating facilities-based service providers and their IDs
B. NPA-NXXs that are portable
C. LRNs associated with each facilities-based service provider
D. Service Provider valid Location Values
E. Valid Billing Ids

Certain types of updates made to network data, such as NPA splits, may cause mass changes to data managed by the NPAC. The NPAC will need to support such mass changes, which typically involve an investigation of all service, service provider, and subscription data in order to determine if such data will be affected by the change, as well as the potential modifications and activation of the data records affected by the change.

An NPA split is supported by maintaining two sets of records or an equivalent mapping to reduce memory costs and administrative care (old NPA and new NPA) in the NPAC SMS, Local SMSs, and SCPs for the duration of the permissible dialing period, during which dialing of both NPAs are allowed. After the expiration of the transition period, all records for the old NPA are removed from the systems.

3.2 NPAC Personnel Functionality
R3- l Authorized NPAC personnel shall be able to initialize the network data when the NPAC SMS is initially deployed.
R3-2 Authorized NPAC personnel shall be able to administer NPAC network data.
R3-3 Authorized NPAC personnel shall be able to open up a new NPA-NXX for LNP.
R3-4 Authorized NPAC personnel shall be able to add/delete a service provider.
R3-5 Authorized NPAC personnel shall be able to administer information related to a service provider.

R3-6 Authorized NPAC personnel shall be able to perform mass changes that affect several records. NPA splits, LRN changes, LIDB changes and other similar network data changes affect multiple subscription records in the NPAC SMS.
R3-7 Authorized NPAC personnel shall be able to select a subset of data which matches a user defined selection criteria, and specify a mass update action to be applied against all key data elements found in the selected records.

3.3 System Functionality
R3-8 The NPAC SMS shall support an off-line batch download (e.g., via tape) mechanism to mass update Local SMSs (e.g., for new service providers, or in case of disaster recovery for a Local SMS).

R3-9 The NPAC SMS shall be able to download network data (e.g. portable NPA-NXX data), to the Local SMSs.

R3- 10 The NPAC SMS shall notify (electronic bulletin) all service providers about the availability of the NPA-NXXs for porting. NOTE: This is a temporary solution.

R3- 1 1 The NPAC shall notify (broadcast / electronic bulletin) all service providers about a new service provider and the associated LRNs. NOTE: This is a temporary solution.

R3- 12 The NPAC shall validate the service, service provider, and subscription data against the current network data.

R3-13 The NPAC SMS shall have the capability to identify all records affected by mass changes, (such as NPA splits), and automatically carry out the required updates and download the modified data to the Local SMSs.

SECTION 4: SERVICE PROVIDER DATA ADMINISTRATION

4.1 Service Provider Data Administration and Management

Service Provider Data Administration functions allow NPAC personnel to receive and record data needed to identify authorized LNP service providers. The service provider data indicates who the LNP service providers are and includes location, contact name, security, routing, and network interface information. These functions will be accessible to authorized NPAC personnel.

Service Provider Administration supports functionality to manage service provider data. There can be only one instance of service provider data for a specific LNP service provider.

Service Provider Administration Requirements

4.1.1 User Functionality
Authorized NPAC personnel can invoke the following functionality in the SMS to administer service provider data:

R4- 1 Create a new service provider - creates, validates, and updates new service provider data.
R4-2 Modify service provider data - modifies, validates, and updates existing service provider data.
R4-3 Delete service provider data - deletes the service provider data and stores it in a history file.
R4-4 View service provider data.
R4-5 View a list of subscriptions associated with the service provider (i.e., see all ported INs associated with a specific service provider).
Additionally, authorized service provider personnel can view their own service provider data.

4.1.2 System Functionality
This section describes SMS functionality required to support the NPAC user requests described in the above section. The following specifies user requests and lists the SMS functionality needed to support those requests:

4.1.2.1 Service Provider Data Creation
An NPAC user requests that service provider data be Heated in SMS by associating an action of "aeate" with the data. This functionality enables a new instance of service provider data for a service provider be Heated, provided that no other service provider data exists for the service provider.

R4-6 When the NPAC user is creating a new service provider, SMS shall receive the following to identify the service provider:

R4-7Service Provider ID - identifier of the service provider (e.g., the OCN).
SMS shall check to see if there is an existing service provider with the same service provider ID. If there is, the SMS shall notify the user that the service provider data already exists for the service provider and that the new service provider data cannot be created.

R4-8 If there is no existing service provider data, the SMS shall receive the following data:

Service Provider name, address, phone number, and contact organization <-- required data:

Service Provider billing name, address, phone number, and billing contact for NPAC billing <-- optional data. If left blank this shall default to service provider name, address, phone number, and contact.

Service Provider to service provider Repair contact name and phone number <-- optional data. If left blank this shall default to service provider contact and phone number.

Location Routing Numbers (LRN) - the identifier of the switches having portable NXXs and used by the service providers <- at least one LRN is required.

Assigned NPA-NXXs open for LNP <-- at least one required.
Network Address of NPAC to Local SMS interface
Network Address of NPAC to SOA interface
Security data
R4-9 After the service provider data has been collected, SMS shall validate that all required data has been received as defined in R4-8.
R4- 10 If all validations are passed, SMS shall notify the user that the request to create the service provider data was successful.
R4- 11 If the service provider data fails validation, SMS shall issue an appropriate error message to the request originator. The service provider data shall not be created.

4.1.2.2 Service Provider Data Modification

An NPAC user requests that service provider data be modified in SMS by associating an action of "modify" with the service provider data. This functionality enables a user to add or change data for the service provider.

R4- 12 SMS shall receive a request to modify service provider data.
R4-13 SMS shall receive the following data from the user to identify the service provider data to be modified: the Service Provider ID.

R4-14 If the service provider data does not exist, SMS shall issue an appropriate error message to the request originator. SMS shall not proceed further with the modification request.

R4- 15 SMS shall allow all data to be modified or added to the service provider data with the exception of the SeNice Provider ID which is the key to the service provider data.

R4- 16 When a user attempts to submit modified service provider data, SMS shall revalidate the service provider data. This revalidation process shall include the validations defined in R4-9.

R4- 17 If the service provider data fails validation, SMS shall issue an appropriate error message to the request originator.
R4- 18 If the validations defined in R4-9 are passed, SMS shall determine if there are any subscriptions associated with the Service Provider ID.
(A) If there are no subscriptions, SMS shall notify the user that the request to modify the seNice provider data was successful, or
(B) If there are subscriptions that contain data that is dependent on the service provider data proposed for change, SMS shall notify the user that the request to modify the senice provider data cannot be completed until the individual subscriptions are modified via subscription administration functions.

4.1.2.3 Delete Senice Provider Data
When an NPAC user requests that senice provider data be deleted in SMS a network action of "delete" will be associated with the subscription data and it will be written to a history file.
R4- 19 SMS shall receive a request to delete service provider data.
R4-20 SMS shall receive the following data from the user to identify the seNice provider data to be deleted: the Senice Provider ID.
R4-21 If the service provider data does not exist, or if is has already been deleted and exists only in a history file, SMS shall generate an error message and send it to the request originator. SMS shall not proceed further with the deletion request.
R4-22 If the seNice provider data does exist, SMS shall do the following:

SMS determine if there are any subscriptions (i.e., ported TNs) associated with the service provider:
(A) If there are no subscriptions, SMS shall notify the user that the request to delete the seNice provider data was successful and shall write the service provider data to a history file which includes the date and time of deletion and the login of the NPAC personnel.

(B) If there are subscriptions, SMS shall notify the user that the request to delete the service provider data cannot be completed until the subscriptions are deleted or are associated with a different service provider.

4.1.3 Service Provider Queries

The query functionality discussed in this section will give users the ability to view service provider data without being able to update that data. A user may not be able to modify a particular data item because that user does not have the proper security permissions and the data is made available via SMS for read-only purposes.

Assumptions

Users will need to be able to retrieve service provider data that they cannot modify.

User Functionality

R4-23 An authorized SMS user shall be able to invoke the following functionality in the SMS to query service provider data: a service provider may view only its own service provider data. R4-24 Authorized NPAC personnel shall be able to view: all subscriptions associated with a service provider, or all subscriptions associated with a LRN.

System Functionality

The following specifies SMS functionality needed to support the user requests described above.

Service Provider Query

R4-25 For queries regarding service provider data, SMS shall receive the Service Provider ID.

R4-26 If SMS does not have service provider data as specified by the request originator, SMS shall provide the request originator with a message indicating that there was no data in SMS that matched the search keys. Otherwise SMS shall return all service provider data associated with the Service Provider ID.
R4-27 For queries regarding subscription data for a specific service provider, SMS shall receive the Service Provider ID, a request to view subscription data, and optionally the subscription data status types to be returned (e.g., active only, active or pending).

R4-28 If SMS does not have subscription data as specified by the request originator, SMS shall provide the request originator with a message indicating that there was no data in SMS that matched the search keys. Otherwise SMS shall return all subscription data associated with the Service Provider ID and any optional status requests.

Subscription List Query

R4-29 For queries regarding subscriptions, SMS shall receive the attributes to be searched on. Allowable attributes are all data elements in Table 3-1 or subsets thereof.

R4-30 If SMS does not have subscriptions as specified by the request originator, SMS shall provide the request originator with a message indicating that there was no data in SMS that matched the search keys. Otherwise, SMS shall return all subscriptions (active versions only) which satisfy the selection criteria. If more than a pre-specified number of subscriptions are found. (This shall be a parameter which is tuneable by the SMS System Administrator the default value shall be 50.) The subscription data shall be returned to a previously designated (off-line) output device/medium.

SECTION 5: SUBSCRIPTION ADMINISTRATION

5.1 Subscription Administration and Management

Subscription Administration functions allow users to specify data needed for ported numbers. The gubgenptian data indicates how local number portability should operate to meet subscribers' needs. These functions will be accessible to authorized service provides via an interface (e.g., the SOA interface) from their operations systems to the NPAC SMS and will also be accessible to (and performed by) NPAC personnel.

Subscription Administration supports functionality to manage multiple versions of subscription data. A subscription version can be associated with the following statuses: invalid, pending, sending, active, conflict, failed, canceled, or old (history). See Version Management for more details on different states of a version. There can be only one invalid, pending, sending, conflict, or failed version per subscription. There can also be one active subscription version at any time and multiple old and/or canceled subscription versions.

5.1.1 Version Management

Version management provides functionality to manage multiple time-sensitive views of subscription data. This sections addresses version management for LNP and the user and system functionality needed for subscription administration. In this context a version may be defined as time-sensitive subscription data.

At any given time, a subscription version in the SMS can have one of several statuses (e.g., active, invalid) and may change status depending on results of different SMS processes (e.g., modification, activation). This section describes different statuses that a version can have and the SMS processes that can change the status.

This section on Version Management discusses functionality and data that is needed for Subscription Administration.

Requirements

Version Status

R5- 1 At any given time, a version in the SMS will have one of the following statuses:

Pending - passed initial validations and edits and will be submitted to the network (i.e., Local LNP SMSs) when activation is requested.

Invalid - failed validations.

[Note: SMS will not create subscriptions or accept updates to subscriptions which result in an invalid condition. However, pending subscriptions will be revalidated prior to sending updates to the local SMSs. Subscriptions that fail this revalidation will have a status of invalid. It will be necessary to notify the porting service provider of this change in status.]

Conflict - non-concurrence from old facilities-based service provider, lack of concurrence from new facilities-based service provider, or dispute between two new facilities-based service providers. Sending - being sent to the network. Active - currently active in the network. Failed - failed activation in the network (at one or more Local SMSs). Old - previously active in the network. Canceled - previously pending, invalid, or in conflict.

The length of time that old subscription versions will be retained (before deletion) and will be accessible through a query request will be a tuneable pararneta that is tuneable by the SMS Administrator (with the appropriate security permission). The default value for this parameter will be eighteen (18) months.
R5-3 The length of time that canceled subscription versions will be retained (before deletion) and will be accessible through a query request will be a tuneable parameter that is tuneable by the SMS Administrator (with the appropriate security permission). For canceled versions, this parameter shall be tuneable based on the last status of the version. The default values for these parameters shall be as follows:

Last status before cancellation	Parameter value
pending	90 Days
invalid	90 Days
conflict	30 Days

Figure 5-1 illustrates the possible status transitions a subscription version may undergo.

Figure 5-1 Version Statuses

R5-4 The LNP SMS will maintain only a single pending version of a subscription.
R5-5 Subscriptions for individual ported TNs that are created through a "TN rangelevel" request shall be treated as individual subscription versions after activation has occurred.

R5-6 SMS shall log all subscription administration transactions. The log entries shall include: Activity Type: create, modify, active, activate, conflict "on," conflict "off," disconnect, cancel, or query Initial Version Status

New Version Status User ID and/or Login Local Number Portability Type (SP, Loc., Serv) Date and Time Starnp

Ported Telephone Nurnber

Status Flag - successful or failed

5.1.2 Subscription Administration Requirements

5.1.2.1 User Functionality

Authorized users2 can invoke the following functionality in the SMS to administer subscription data:
R5-7 Create a subscription version - creates, validates, and pends (if valid) a new subscription version for activation in the network.
R5-8 Modify a subscription version - modifies, validates, and pends (if valid) a pending, invalid, or active subscription version for activation in the network. Old, canceled, conflict, and failed versions cannot be modified.

R5-9 Activate a subscription version - activates a pending subscription version in the network.
R5- 10 Conflict "On"/Conflict "Off" - places a subscription version in conflict or removes it from conflict. A subscription version in conflict cannot be activated.
R5- 11 Disconnect a subscription version (from the network) - deletes the active subscription version in the network and stores it as an old subscription version.
R5- 12 Cancel a subscription version - removes an invalid, conflict or pending subscription version and stores it as a canceled subscription version.
R5-13 Query: displays a subscription version and its associated parameters.

5.1.2.2 System Functionality

This section describes SMS functionality required to support user requests defined in the above section. Subscription versions can be created or viewed by the old facilities-based service provider. Subscription versions can be created, modified, activated, disconnected, canceled, or viewed by the new facilities-based service provider. In addition to being able to create, modify, activate, disconnect, cancel, and view subscriptions, only authorized NPAC personnel can place subscriptions in conflict and remove them from conflict. Additionally, any authorized service provider can view any subscription version for any ported TN. (Note: Tuneable security permission matrix may be required.)
Additionally, SMS functionality is required to perform operations which are not invoked by a direct user request. This functionality shall monitor a subscription version to determine whether the old and the new facilities-based service providers have authorized the transfer of service for a ported number, shall issue appropriate notifiers to service providers, and shall change the status of a subscription version based on tuneable parameters, e.g. pending version will be automatically canceled after an "X" number of days ("X" = tuneable parameter)

2 An "authorized user" shall be able to access the data that is part of or controlled by the SMS. A user, either an individual or machine, shall be identified by a unique user identification code (user id).

The following specifies user requests and lists the SMS functionality needed to support those requests:

5.1.2.2.1 Subscription Version Creation

A user requests a subscription to be created in SMS by associating an action of "create" with a version. This functionality, which can be invoked by the old or the new facilities-based service provider, enables a new instance of a subscription version for the ported telephone number to be created, provided that there exists at most one active subscription version. Multiple old and/or canceled subscription versions may exist. If a create is initiated by the old facilities-based service provider, they shall identify the ported telephone number, the new facilities service provider, the due date and indicate that they are authorizing the transfer of service. If the create is initiated by the new facilities-based service provider, all information pertaining to the ported TN may be provided, with the exception of the old facilities-based service provider's authorization.

R5-14 When the user is the old (ported-from) service provider SMS shall receive the following to identify the subscription version to be created:

Local Number Portability Type IO - identifier of the Local Service Provider Portability (LSPP) type. (NOTE: While Local Service Provider Portability will be the first type supported by the NPAC SMS, the system needs to be extensible so as to support multiple types at a future date.)

Ported Telephone Number(s) - this entry can be a single TN or a continuous range of TNs that identifies a subscription or a group of subscriptions that share the same attributes.
Due Date - date on which transfer of service from old facilities-based service provider to new service provider is planned to occur.

New facilities-based service provider ID - the identifier of the new facilities-based service provider.

Old facilities-based service provider ID - the identifier of the old facilities-based service provider.

Authorization from old facilities-based service provida - indication that the transfer of service is authorized by the ported-from service provider.

R5-15 When the user is the new facilities-based service provida SMS shall receive the following to identify the subscription vasion to be created:

Local Number Portability Type ID - identifier of the Local Service Provider Portability type.

Ported Telephone Number (TN) - the identifier of a subscription (i.e., the telephone number assigned to the customer).

Due Date - date on which transfer of service from old facilities-based service provider to new facilities-based service provider is planned to occur.

New Facilities-based Service Provider ID - the identifier of the new facilities-based service provider.

Old Facilities-based Service Provider ID - the identifier of the old facilities-based service provider.

Authorization from New Facilities-Based service provider - indication of whether the transfer of service is authorized by the new Facilities-based service provider.

Location Routing Number (LRN) - the identifier of the ported-to switch.

LIDB Global Title Translation (GTT) data - network addressing information for routing to the serving LIDB.

Destination Point Code (DPC) type for LIDB features GTT indicates whether destination point code identifies the subsystem or a gateway STP.

CLASS Global Title Translation (GTT) data for LIDB DPC network addressing information (i.e., mapping of new LRN to destination point code) for routing TCAP messages to the ported-to switch.

Destination Point Code (DPC) type for CLASS features GTT indicates whether destination point code identifies the end of fice or a gateway STP.

R5-16 The following fields are for future use. The new facilities-based service provider may not be required to treat these fields as mandatory.

Billing Service Provider ID
End-User Location - Value
End-User Location - Type
Future 1
Future 2
Future 3

SMS shall invoke the following Version Creation functionality:
R5-17 When a user attempts to submit a new version, SMS shall determine whether a pending version already exist for the entity in question.

If a pending version exists and if the authorized user is associated with the old or new facilities-based service provider (who has not yet authorized the transfer of service), SMS shall:

Allow the old facilities-based service provider to perform the functions defined in R5-14
or
Allow the new facilities-based service provider to perform the functions defined in R5-15 and R5-16.

Otherwise, the SMS will send an error message to the request originator.

R5-18 If there is no pending version of the subscription (or if the conditions in R5-17 have been met) and no active version, SMS shall proceed as follows:

SMS shall perform the following validations for the version: All data has been received as defined in R5-14 or R5-15 and R5-16. The old and the new facilities-based service provider must agree as to the Due Date. The Due Date is the current date or a future date.

The NPA-N~ of the ported Telephone Number must be in the Portable NPA-NXX table. The old and new facilities-based service provider IDs must match existing service provider data.

The new LRN must be associated with the new facilities-based service provider. The LIDB DPC data must be associated with the new facilities-based service provider.
. .

The CLASS DPC data must be associated with the new facilitiesbased service provider.

R5-19 If there is no pending version of the subscription but there is an active version, SMS shall, in addition to the validations defined in R5- 16, verify that the old service provider on the version being created is equal to the service provider on the active subscription version.

R5-20 If the subscription version fails validation, SMS shall issue an appropriate error message to the request originator. If a valid subscription version already exists (e.g., the current create is being done by the old facilities-based service provider, but the new facilities-based service provider has already done a create for the ported TN), the pending subscription version shall be retained. Otherwise, the subscription version shall not be created.

R5-21 If the subscription version passes validations, SMS shall:

Verify if both the old and the new facilities-based service providers have authorized the transfer of service for the ported TN.

If not, SMS shall compute the date by which authorization data from both service providers must be received and shall store this with the subscription version. The date by which concurrence from both service providers must be received shall be computed as being a predetermined number of days prior to the Due Date. This will be a parameter that is tuneable by the SMS Administrator. The default value for this parameter shall be three (3) days.

Mark the version with a status of pending in the SMS and issue an appropriate message to the request originator indicating successful completion of the pending process.

R5-22 When the date for concurrence for a pending subscription version has been reached, SMS will send a notifier to the service provider (old or new) who has not yet authorized the transfer of service.

R5-23 If authorization for the transfer of service has not been received from the new facilities-based service provider within the allotted period of time (tuneable parameter) after SMS sent the notifier, the subscription version shall be canceled as defined in R5-70. The user ID for this transaction shall be the "SMS System ID."

5.1.2.2.2 Subscription Version Modification

A user requests a pending, invalid or conflict subscription version to be modified in SMS by associating an action of "modify" with a version. This functionality, which can be invoked only by the new facilities-based service provider, enables a user to add or change data in a subscription version.

5.1.2.2.2.1 Modification of a Pending, Invalid, or Conflict Subscription Version

R5-24 SMS shall receive data in support of modification of a subscription version:

(1) to change the data associated with a pending, conflict, or invalid subscription version or (2) to add additional data to a pending or conflict subscription version.

R5-25 If the version status is sending, failed, canceled, or old, SMS shall generate an error message and send it to the request originator. SMS shall not proceed further with the modification request.

R5-26 SMS shall receive the following data from the user to identify the subscription version to be modified: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-27 SMS shall allow the following data to be modified in the subscription version:

Location Routing Number (LRN) - the identifier of the switches having portable NXXs and used by the service providers <- at least one LRN is required.

Due Date - date on which transfer of service from old facilities-based service provider to new service provider is planned to occur.

LIDB GTT data - network addressing information for routing to serving LIDB.

DPC type for LIDB features GTT - indicates whether Destination Point Code identifies the subsystem or a gateway STP.

CLASS GTT data - network addressing information for routing TCAP messages to the ported-to switch.

DPC type for CLASS features GTT - indicates whether Destination Point Code identifies the end office or a gateway STP.

R5-28 The following fields are for future use. The new facilitiesbased service provider may not be required to treat these fields as mandatory.

Billing Service Provider ID

End-User Location - Value

End User Location - Type

Future 1

Future 2

Future 3

R5-29 SMS shall revalidate the modified subscription version. This revalidation process shall include the validations defined in R5-18.

R5-30 If the version fails validation, SMS shall issue an appropriate error message to the request originator. The pending subscription version, which the user was attempting to modify, shall be retained with no changes.

R5-3 1 If the version passes validations, SMS shall mark the version with a status of pending in the SMS and shall issue an appropriate message to both old and new service providers indicating successful completion of the pending process.

R5-32 If for a version that passed validations, the Due Date has been modified SMS shall send a notifier to the old facilitiesbased service provider informing them of the new Due date.

5.1.2 .2 .2 .2 Modificanon of an Acnve Subscripnon Version
R5-33 SMS shall receive data in support of modification of an active subscription version to change only specific data associated with an active subscription version.

R5-34 SMS shall invoke version creation functionality to create a new (pending) subscription version based on the active subscription version.

R5-35 SMS shall receive the following data from the usa to identify the active subscription version is to be modified: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-36 SMS shall allow the following data to be modified in the newly created subscription version:

Location Routing Number (LRN) - the identifier of the switches having portable NEs and used by the service providers <- at least one LRN is required.

LIDB GTT data - network addressing information for routing to serving LIDB.

DPC Type for LIDB features GTT - indicates whether Destination Point Code identifies the subsystem or a gateway.

GTT data for CLASS features - network addressing information for routing TCAP messages to the ported-to switch.

DPC type for CLASS features GTT - indicates whether Destination Point Code identifies the end office or a gateway STP.

R5-37 The following fields are for future use. The new facilities-based service provider may not be required to treat these fields as mandatory.

Billing Service Provider ID

End-User Location - Value

End-User Location - Type

Future 1

Future 2

Future 3

R5-38 SMS shall validate the modified subscription version. This validation process shall include the applicable validations deEmed in R5-18.

R5-39 If the version fails validation, S M S shall issue an appropriate error message to the request originator. A new subscription version shall not be created and no changes shall be made to the current active subscription version.

R5-40 If the version passes validation, S M S shall record the current date and time (i.e., system date and time) as the Activation Date and Time Stamp, shall mark the version with a status of sending in the SMS, and shall issue an appropriate message to the request originator indicating successful completion of the modify process.

R5-41 SMS shall activate the version in the network as defined in R5-51 through R5-61.

5.1.2.2.3 Conflict Subscription Version

An authorized NPAC user requests a subscription be placed in conflict or removed from conflict by associating an action of "conflict on" or "conflict off" with a version. This functionality is invoked when an authorized user requests that the version be placed in or removed from conflict.

5.1.2.2.3.1 Placing a Subscription Version in Conflict

R5-42 SMS shall receive the following data from the user to

identify the subscription version is to be placed in conflict: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-43 If the version status is not pending, SMS shall generate an error message and send it to the request originator. SMS shall not proceed further with the request to place the subscription version in conflict.

R5-44 If the version status is pending, SMS shall mark the version with a status of conflict. shall record the current date and time (i.e., system date and time) as the **Conflict** Date and Time Stamp and shall issue an appropriate message to the request originator indicating successful completion of the process to place a subscription in conflict.

R5-45 If a subscription version remains in conflict for thirty days, SMS shall invoke cancellation processing as defined in R571 (tuneable parameter). The user ID for this transaction shall be the "SMS System ID."

5.12.2.3.2 Removing a Subscription Version from Conflict

R5-46 SMS shall receive the following data from the user to identify the subscription version is to be removed from conflict: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-47 If the version status is not in conflict, SMS shall generate an error message and send it to the request originator. SMS shall not proceed further with the request to remove the subscription version from conflict.

R5-48 If the version status is conflict, SMS shall validate the subscription version. This validation process shall include the applicable validations defined in R5-18.

R5-49 If the version fails validation, SMS shall issue an appropriate error message to the request originator. A new subscription version shall not be created and SMS shall not proceed further with the request to remove the subscription version from conflict.

R5-50 If the version passes validations, SMS shall mark the version with a status of pending in the SMS and shall issue an appropriate message to the request originator indicating successful completion of the process to remove a subscription from conflict.

5.1.2.2.4 Subscription Version Activation

A user requests a subscription be activated in the network by associating a network action of "activate" with a version. This functionality, which can be invoked only by the new facilities-based service provida enables an authorized user to request that a subscription version be activated.

RS-S1 SMS shall receive the following data from the user to identify the subscription version is to be activated: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

SMS shall record the current date and time (i.e., system date and time) as the Activation Date and Time Stamp.

R5-52 If the version status is not pending, SMS shall generate an error message and send it to the request originator.

R5-53 SMS shall re-validate the subscription version as per the validations defined in R5- 18.

R5-54 If the version fails re-validation, SMS shall log the error message(s) and make them available to authorized users, and mark the version status as invalid in the SMS.

R5-55 If the version is valid, SMS shall determine the Local SMS configuration data of all the Local SMSs.

R5-56 SMS shall translate the subscription version data to create interface messages containing the information to be updated to the Local SMSs.

R5-57 SMS shall send the interface messages to the Local SMSs. The subscription version shall be marked vith a status of sending in the SMS. SMS shall record the current date and time (i.e., system date and time) as the Broadcast Date and Time Stamp in the subscription version.

R5-58 SMS shall log the activation responses resulting from the activation requests sent to the Local SMSs. SMS shall allow users (with the appropriate security permissions) to view this information. The length of time that data will remain in this log shall be a parameter that is tuneable by the SMS Administrator.

R5-59 If a positive acknowledgment is received from all involved Local SMSs, then the subscription version shall be marked with a status of active in the SMS and the previously active version (if one exists) for the same subscription (i.e., ported TN) shall be marked as old.

R5-60 If the version fails activation in some of the Local SMSs to which it was sent (e.g., the link between SMS and a specific network node is down), the update shall remain in queue and shall be resent to the Local SMSs where activation failed. The number of automatic resends and the interval between resends shall be parameters that can be modified by the SMS Administrator. There shall be a default of three (3) for the number of retries and a default of two (2) minutes for the interval between resends. During this period, the status of the version shall remain "sending." Once the maximum queue time is exceeded, SMS shall consider the version to have failed activation at specific Local SMSs. SMS shall mark the status of the previously active vasion (if one exists) for the subscription (i.e., ported TN) as old. SMS shall send a notification to the NPAC System Administrator. This notification shall include the list of the

Local SMS(s) where activation failed. Special processing must be invoked by the NPAC System Administrator to resend the subscription version to the Local SMS(s) where it failed activation. The subscription version shall be marked with a status of failed and an indication that the failure was partial.

R5-61If the version fails activation in *all* the Local SMSs to which *it* was sent, SMS shall mark the status of the version as failed. If there is a current active subscription version, it shall remain active. SMS shall send a notification to the NPAC System Adrninistrator indicating that the subscription failed activation at all Local SMSs. Special processing must be invoked by the NPAC System Administrator to resend the subscription. The subscription version shall be marked with a status of failed.

5.1.2.2.5 Disconnect Subscription Version

When a user requests that an active subscription be disconnected, it will be deleted from the network. This functionality, which can be invoked only by the new facilities-based service provider, enables the usa to remove an active version from the network. The user-supplied Disconnect Date indicates when the customer's service was disconnected.

R5-62SMS shall receive the following data from the user to identify the subscription vasion is to be deleted: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-63If there is no subscription version with a status of active, SMS shall notify the request originator that the vasion is not active in the network and cannot be disconnected

R5-64If there is a subscription vasion with a status of pending, invalid, failed, or conflict and there is also a subscription vasion with a status of active, SMS shall notify the request originator that the active version cannot be disconnected until the pending, invalid, failed, or conflict vasion is canceled. SMS shall not proceed with the request.

R5-65 If the status of the current version for the subscription is active, SMS shall do the following:

translate the pending disconnect request to create an interface message identifying the subscription to be deleted by the Local SMSs,

send the disconnect message to the Local SMSs, and

mark the disconnect request with the status sending. SMS shall record the current date and time (i.e., system date and time) as the Broadcast Date and Time Stamp in the disconnect request.

R5-66 If the disconnect request succeeds in all the Local SMSs, SMS shall mark the current active subscription version with a status of old, shall update the Disconnect Date to the old subscription version, and shall mark the disconnect request as old.

R5-67 If the disconnect request fails in all of the Local SMSs, the status of the disconnect request shall be changed to failed. The current active subscription version shall remain active. SMS shall send a notification to the NPAC System Administrator that the disconnect request failed. Special processing must be invoked by the NPAC System Administrator to resend the disconnect request to the Local SMS(s).

R5-68 If the disconnect request fails in some of the Local SMSs to which it was sent (e.g., the link between SMS and a specific network node is down), the disconnect request shall remain in queue and shall be resent to the Local SMSs where the disconnect failed. The number of automatic resends and the interval between resends shall be parameters that can be modified by the SMS Administrator. There shall be a default of three (3) for the number of retries and a default of two (2) minutes for the interval between resends. During this period, the status of the disconnect request shall remain "sending." Once the maximum queue time is exceeded, SMS shall consider the disconnect request to have failed at specific Local SMSs. SMS shall send a notification to the NPAC System Administrator. This notification shall include the list of the Local SMS(s) where the disconnect request failed. Special processing must be invoked by the NPAC System Administrator to resend the disconnect request to the Local SMS(s) where it failed. The disconnect request shall be marked with a status of failed and an indication that the failure was partial.

5. 1.2.2.6 Subscription Version Cancellation

Only subscription versions with a status of pending, invalid, or conflict can be canceled. A user requests that a pending, invalid or conflict subscription be canceled in SMS by associating an action of "cancel" with a version. This functionality enables a user to cancel a subscription version that has not yet been activated in the network. Additionally, only NPAC personnel can cancel a subscription version with a status of conflict.

R5-69 SMS shall receive the following data from the user to identify the subscription version to be canceled:

the Local Number Portability Service ID and
the Ported Telephone Number Subscription ID.

R5-70 If there is no subscription version with a status of pending, invalid, or conflict, SMS shall issue an appropriate error to the request originator and shall not proceed with the request.

R5-7 1 If there is a subscription version with a status of pending, invalid, or conflict, SMS shall mark the subscription version with a status of canceled and record the current date and time (i.e., system date and time) as the **Cancellation** Date and Time Stamp.

5.1.3 Subscription Queries
The query functionality discussed in this section will give users the ability to view subscription data without being able to update that data. A user may not be able to modify a particular data item because that user does not have the proper security permissions and the data is made available via SMS for read-only purposes.

Assumptions
Users will need to be able to retrieve subscription data that they cannot modify.
Users shall submit query requests for subscription data based on a single ported TN only.
Any authorized service provider personnd shall be able to view any subscription version for any ported TN.

User Functionality
R5-72 An authorized SMS user shall be able to invoke the following functionality in the SMS to query subscription data:
Query data stewarded by SMS for a subscription and all its versions.

System Functionality
The following specifies SMS functionality needed to support the user requests defined above.
R5-73 For queries regarding subscription data, SMS shall receive the Local Number Portability Type [D and the Ported Telephone Number Subscription ID, and optionally, the status of the subscription version (e.g., active, pending).

R5-74

If multiple subscription vasions are found, and the user has provided the status of the subscription version desired, SMS shall retrieve only the data associated with that status of the subscription version only. Otherwise SMS shall return all subscription version data associated with the ported TN. The parameters to be returned, as appropriate for the subscription version status, are as follows: Local Nurnber Portability Type ID Ported Telephone Number(s) Due Date New facilities-based service provider ID Old facilities-based service provider ID

Authorization from old facilities-based service provider
Authorization from new facilities-based service provider
Location Routing Number (LRN)
LIDB GTT data
DPC type for L1DB features GTT
CLASS GTT data
DPC type for CLASS features GTT
Billing Service Provider ID
End-User Location Value
End User Location Type
Future 1
Future 2
Future 3
Disconnect Date
Conflict Date and Time Stamp
Activation Date and Time Stamp
Broadcast Date and Time Stamp

Cancellation Date and Time Stamp

R5-74 If SMS does not have a subscription version as specified by the request originator, SMS shall provide the request originator with a message indicating that there was no data in SMS that matched the search keys.

SECTION 6: NPAC SMS INTERFACES

Two interfaces to the NPAC SMS shall be supported. The first interface shall be between the NPAC SMS and the service provider's Service Order Activation platform and the second shall be between the NPAC SMS and the Local SMSs. Both of the interfaces shall support two-way communications.

6.1 SOA to NPAC SMS Interface

The SOA to NPAC SMS Interface could be used by a variety of local service provider systems for retrieving and updating subscription data in an NPAC SMS. The types of systems that are expected to use this interface are Service Provisioning OSs and/or Gateway Systems.

****
****

EXHIBIT

****
****

6.1.1 Request Administration

The SOA to NPAC Interface will support four types of transactions: subscription request and audit request transactions from the front end system (e.g., the SOA) interface users, and response and notification transactions from the NPAC SMS. The Interface will require security features to ensure that data is not corrupted by unauthorized access. Security management is outside the scope of the interface, however, the Interface user will be required to provide parameters to support security management at the NPAC SMS.

R6-1Associations on these application to application interfaces must use strong authentication.

R6-2Each subscription administration request sent over the Interface shall be capable of supporting multiple independent transactions. One failed item in a request will not cause other items in the request to fail. See ANSI standard T1.246, *Operations Adrninistration, Maintenance and Provisioning (OAM&P) -information Mode! and Services for Interfaces between Operations Systems across Jurisdictional Boundaries to Support Configuration Management - Customer Account Record*

Exchange (CARE) for an example of a GDMO (ISO 10165-4) description of an interface that can deal with bunched transactions.

R6-3 Each subscription administration request shall be acknowledged with at least one response transaction from the NPAC SMS. Some requests may be acknowledged more than once. For example, after validation processing is completed a response transaction would be sent back to the user with either a positive acknowledgment or a negative acknowledgment with an error message indicating the results of the validation.

6.1.2 Subscription Administration

Subscription Administration provides functionality in creating or modifying subscriptions and activating or deleting them from the networks. Based on security parameters, users of the interface shall be able to do the following:

R6-4 Add new versions of subscription data, as well as cancel or modify a specific version of subscription data.

R6-5 Retrieve subscription data, including either specific versions of a subscription or all versions.

R6-6 Request the activation or deletion of subscription data.

6.1.3 Audit Requests

Audit Request functionality enables users to obtain audits of a specific subscription or group of subscriptions at all service provider networks or at select networks. Based on security parameters, users of the interface shall be able to do the following:
R6-7 Request that an audit be performed for a subscription or a group of subscriptions.

R6-8 Specify that an audit be performed at all service provider networks or at select networks.

R6-9 Each audit request sent over the Interface shall be capable of specifying a single subscription or a range of TNs and specific search parameters.

R6- 10 Each audit request shall be acknowledged with at least one response transaction from the NPAC SMS. This response shall include an acknowledgment of whether discrepancies were reported by individual service providers and the identity of those providers. Audits which find no discrepancy shall receive one response. If discrepancies are found, there shall be one response per erred telephone number.

6. 1.4 Notifications

NPAC SMS shall have functionality to send notifications to service providers based on parameters which are tuneable by the NPAC SMS Administrator. NPAC SMS shall be able to do the following via the interface:

R6- 11 Notify a new or an old service provider that they haven't provided authorization for a transfer of service for a TN.

R6- 12 Notify an old service provider that the Due Date for a subscription has been modified

6.2 NPAC SMS to Local SMS Interface

The NPAC SMS to Local SMS Interface could be used to send subscription data and audit requests to a variety of service provider systems. The types of systems that is expected to use this interface are Local SMSs (or SMS-like functionality at LNP SCPs) and/or Gateway Systems. The interface will require security features to ensure that data is not corrupted by unauthorized access. Security management is covered in Section 7, however, the interface user will be required to provide parameters to support security management at the NPAC SMS.

****
****

EXHIBIT

****
****

6.2.1 Transaction Administration

The NPAC SMS to Local SMS Interface will support five types of transactions: subscription download transactions from the NPAC SMS, audit requests from the NPAC SMS, network data download transactions from the NPAC SMS, response transactions from the Local SMS, and requests from the Local SMS that specific transactions be resent.

R6- 13 Interface users shall specify their user-identification, system identification, and password to be able to use the Interface.

R6- 14 Each subscription download request sent over the interface shall be capable of supporting multiple independent transactions. One failed item in a request will not cause other items in the request to fail.

R6-15 Each subscription download request shall be acknowledged with at least one response transaction from the Local SMS. A response transaction shall be sent back to the NPAC SMS with either a positive acknowledgment or a negative acknowledgment which may include a request that the transaction be sent again.

R6- 16 Each audit request sent over the interface shall be for a single transaction or for a range of transactions.

R6-17 Each audit request shall be acknowledged with at least one response transaction from the Local SMS. A response transaction shall be sent back to the NPAC SMS with either a positive acknowledgment for those TNs which passed audit and a negative acknowledgment for those TNs which failed audit as well as only a negative acknowledgment for those TNs which failed audit.

R6- 18 A local SMS shall be able to request the NPAC SMS to resend a subscription based on its TN or a block of subscriptions based on a time window specified in the request. This function might be provided by allowing for an audit request from the local SMS.

R6-19Each network data download request shall be acknowledged with one response transaction from the Local SMS. A response transaction shall be sent back to the NPAC SMS with either a positive acknowledgment or a negative acknowledgment which may include a request that the transaction be sent again.

6.2.2 Network Subscription Administration

Network Subscription Administration provides functionality in activating, modifying, or deleting subscription data from the network and in requesting audits. The NPAC SMS, via its interface to Local SMSs shall be able to do the following:

R6-20 Add new subscription data, as well as delete or modify specific subscription data.

R6-21 Request audits of subscription data, including either a specific subscription or a range of subscriptions.

6.3 Interface Transactions

The CMIP protocol provides for seven types of transactions over the interface (Reference: ISO 9595 and 9596). They are Create, Delete, Set, Get, Cancel-Get, and Notification. The first six transactions are originated by the manager, and affect objects contained in the agent. The Notification transaction is created by the agent and is used to give notice *to* the manager that something of interest to the manager has happened to an object in the agent system.

R6-22 The object model shall be designed in terms of using these transactions in a manager-agent relationship.

6.4. Interface and Protocol Requirements

While it is expected that dedicated links will be used for the interfaces, switched connections should also be supported. Reliability and availability of the links will be essential and high capacity performance will be needed.

R6-23 The SOA to NPAC SMS Interface and the NPAC SMS to Local SMS Interface . shall be an open, non-proprietary interface.

6.4.1 Protocol Requirements

Both of the NPAC SMS interfaces, as defined above, shall be implemented via the following protocol stack:

R6-24:

Application: Presentation: Session: Transport: Network: Link:

Physical:

ASCE, CMISEEROSE (ANSI Tl.224) as described in ANSI Tl.224 as described in ANSI Tl.224 OSI Transport Class 0, RFC 1006, and TCP Internet (ETF) IP ethernet routing, or frame relay, or ATM (or more than one of these) as appropriate

R6-25 Multiple associations per service provider may be required.

6.4.2 Interface Performance Requirements

R6-26Both the SOA to NPAC SMS and the NPAC SMS to Local SMS shall be available on a 24 by 7 basis.

R6-27 A 99.9 % availability rate shall be maintained for both interfaces.

R6-28A transaction rate of 2 transactions per second shall be supported by each SOA to NPAC SMS interface association (See Section 10 for number of associations).

R6-29 A transaction rate of 25 transactions per second shall be supported by each NPAC SMS to Local SMS interface association (See Section 10 for number of
. .
assoclatlons.

6.4.3 Interface Performance Requirements

R6-30 The interoperable interface models shall be specified in terms of ISO 10165-4, "Generalized Definition of Managed Objects (GDMO)." The specification will become the property of the consortium, who may make it public.

R6-31 The model and interface specification shall be delivered in two stages.

R6-32 The model proposed shall be proposed shall be provided at the object and attribute level in the RFP proposal. It shall include tables and/or figures that show how the interface functions required by this specification were mapped into the services provided by the model.

R6-33The selected Prirnary vendor shall ddiver a complete interoperable interface specification one month after the announcement of the vendor selection.

R6-34 The application to application interfaces shall be specified in sufficient detail to allow the vendors who supply the SOA and Local SMS interfaces to build implementations that will interoperate with the NPAC SMS. This must be possible with no or only minimal interaction between the suppliers of the interoperable systems. For example the interoperable interface specification shall provide for error handling of error conditions appropriate to all of the functional requirements. It shall also define the security relationship between the systems.

R6-35 The interface specified shall be capable of extension to account for evolution of the interface requirements.

SECTION 7: SECURITY REQUIREMENTS

Introduction

In addition to the general security requirements based on the user interface paradigm in Section 7.1 through 7.7, there are requirements for the security on an OSI application to application interface (such as the one specified in Section 6 for the SMS to SMS and SMS to SOA interfaces). Section 7.8 describes such a security environment.

7.1 Identification

A user identification is a unique, auditable representation of the user's identity within the system. The SMS requires all system users, both individuals and remote machines, to be uniquely identified to support individual accountability.

R7-lUnique user identification codes (userids) must be utilized to identify individuals and remote machines.

R7-2 SMS must require users, i.e., individuals and remote machines, to identify themselves with their assigned userid before performing any actions.

R7-3 SMS must maintain intemally the identity of all currently active users.
R7-4 Every process running on SMS must have associated with it the userid of the invoking user
(or the userid associated with the invoking process).

R7-5 SMS must disable userids after a period of time during which the userid has not been used.
The time must be NPAC-specifiable with a system delivered default of 60 days.

R7-6SMS must provide a complementary mechanism or procedure for the re-instatement or deletion of disabled userids.

R7-7SMS must support the temporary disabling of userids.

R7-8The mechanism that disables userids should provide an option for automatic reactivation.

R7-9SMS must control and limit simultaneous active usage of the same userids by allowing only one active login. When the second login is entered, the system will ask if the first login can be disconnected. If the user replies yes, the second login can continue; however, if the user replies no, the second login is terminated.

7.2 Autbentication

The identity of all system users, both individuals and remote machines, must be verified or authenticated to enter the system, and to access restricted data or transactions.

R7- 10 SMS must authenticate the identity of all system users, both individuals and remote machines, prior to their initially gaining access to SMS.

R7- l l SMS must not support ways to bypass the identity authentication mechanisms.

R7- 12 SMS must protect all internal storage of authentication data so that it cannot be accessed by
any unauthorized user.

7.2.1 Password Requirements

R7- 13 SMS shall not provide a mechanism whereby a single password entry can be shared by multiple userids.

R7-14 SMS must not prevent a user from choosing a password that is already associated with another userid.

R7-15 SMS must store passwords in a one-way encrypted form.

R7-16 Encrypted passwords must not be accessible to non-privileged users.

R7-17 Unencrypted passwords must not be accessible to any users, including NPAC personnel.

R7- 18 SMS must automatically suppress or fully blot out the clear-text representation of the password on the data entry device, e.g., terminal.

R7- 19 Passwords should not be sent over public or shared data networks in clear text.

R7-20 SMS must not allow for any password to be null.

R7-21 SMS must provide a mechanism to allow passwords to be user-changeable. This mechanism must require re-authentication of the user identity.

R7-22 The NPAC must have a mechanism to reset passwords.

R7-23 SMS must enforce password aging, i.e., passwords must be required to be changed after a NPAC-specifiable time. The system supplied default shall be 90 days.

R7-24 SMS must provide a mechanism to notify users in advance of requiring them to change their passwords. This can be done by one of the following methods: (1) SMS will notify users a NPAC-specifiable period of time prior to their password expiring. The system supplied default shall be seven days. (2) Upon password expiration, SMS will notify the user, but allow an NPACspecifiable subsequent number of additional logons prior to requiring a new password. The system supplied default shall be two additional logins.

R7-25 Password must not be reusable by the same individual for an NPAC-specifiable period of time. The system supplied default shall be six months.

R7-26 SMS must provide a method of ensuring the complexity of user-entered passwords that meets the following requirements:

(1) Passwords must contain a combination of at least six alphanumeric characters including at least one alphabetic and one numeric or punctuation character. If the system does not distinguish between upper and lower case alphabetic characters, the minimum acceptable length is eight characters.

(2) Passwords must not contain the associated userid.

R7-27 SMS-supplied password generation algorithms must meet the following requirements:

(1) Passwords must be "reasonably" resistant to brute-force password guessing attacks, i.e., the total number of system generated passwords must be on the same order of magnitude as what a user could generate using the rules specified in requirement 7-26 (1) above.

(2) The generated sequence of passwords must have the property of randomness, *i e* consecutive instances must be uncorrelated and the sequences must not display periodicity.

7.3 Access Control

Access to the SMS and other resources must be limited to those users that have been authorized for that specific access right.

7.3.1 System Access

R7-28 SMS must allow access to authorized users and authorized remote systems.

R7-29 SMS must provide a procedure for the initial entry or modification of authorized users and authentication information.

R7-30 SMS must not provide any default userids that can permit unauthenticated SMS access.

R7-31 SMS's login procedure should be able to be reliably initiated by the user, i.e., a trusted communications path should exist between SMS and the user during the login procedure.

R7-32 SMS must disconnect or re-authenticate users after an NPAC-specifiable period of non-use. The system supplied default shall be 60 minutes.

R7-33 The SMS login procedure must exit and end the session if the user authentication procedure is incorrectly performed an NPAC-specifiable number of times. The system supplied default shall be three times.

R7-34 SMS must provide a mechanism to immediately notify the NPAC when the above threshold is exceeded.

R7-35 When the above threshold has been exceeded, an NPAC-specifiable interval of time, not to exceed 60 seconds, must elapse before the login process can be restarted on that I/O port.

R7-36 SMS must not suspend the user id upon exceeding the above threshold.

R7-37 SMS must perform the entire user authentication procedure even if the userid that was entered was not valid.

R7-38 Error feedback must provide no other information except "invalid," i.e., it must not reveal which part of the authentication information is incorrect.

R7-39 SMS should provide a mechanism to exclude or include users based on timeofday, day-of-week, calendar date, etc.

R7-40 SMS should provide a mechanism to exclude or include users based on method or location of entry.
R7-41 SMS must provide a mechanism to limit the users authorized to access the system via dial-up facilities.
R7-42 SMS must provide a mechanism to limit system entry for privileged NPAC users on an NPAC-specifiable network access or per-port basis.

R7-43 Since some form of network access, e.g., dial-in, Wide Area Network, or Internet, is provided by SMS, SMS must provide a strong authentication mechanism. For example, the authentication mechanism could be a private or public key encryption based mechanism, an additional password, and/or smart card to validate the user or remote system. For remote machines, public key encryption may be required in conjunction with dedicated private lines. For dial-in users (NPAC administrative and NPAC operations), smart cards are required.

R7-44 A mechanism must exist to end the session through secure logoff procedures.

R7-45SMS must provide an advisory warning message upon system entry regarding unauthorized use, and the possible consequences of failure to meet those requirements.
R7-46 The message must be NPAC-specifiable to meet their own requirements, and any applicable laws.
R7-47 SMS must be able to display a message of up to 20 lines in length. This message should be displayed at the first point of entry. If possible, the message should appear before the logon process. As part of the delivered software, the following is an example of the default message that must be included:

NOTICE: This is a private computer system.
Unauthorized access or use may lead to prosecution.

R7-48 Upon successful access to the system, the following must be displayed:
(1) Date and time of the user's last successful system access.
(2) The number of unsuccessful attempts by that userid to access the system, since the last successful access by that userid.
R7-49 SMS must allow only the NPAC well-defined privileged users responsible for security administration to authorize or revoke users.
R7-50 Procedures for adding and deleting users must be well defined and described in the NPAC security documentation.

7.3.2 Resource Access
R7-51 Only authorized users shall be able to access the data that is part of or controlled by the SMS system.
R7-52 Each service provider's data must be protected from access by unauthorized users.

R7-53 Only authorized users shall be able to access the transactions, data, and software that constitute the SMS.
R7-54 The executable and loadable software must be access controlled for overwrite and update, as well as execution rights.
R7-55 Control of access to resources must be based on authenticated user identification.
R7-56 Encryption may be used to augment the access control mechanisms, but must not be used as a primary access control mechanism for sensitive data.
R7-57 For every resource controlled by SMS, it must be possible to grant access rights to a single user or a group of users.
R7-58 For every resource controlled by SMS, it must be possible to deny access rights to a single user or a group of users.
R7-59 It will be necessary to restrict user access to information based on the data content of a specific field, attribute, tuple, record, etc.
R7-60 Modification of the access rights to a resource must only be allowed by the NPAC.
R7-61 SMS must provide a mechanism to remove access rights to all resources for a user or a group of users.
R7-62 The access control mechanism's data files and tables must be protected from unauthorized access.

7.4 **Data and System Integrity**
R7-63 SMS must be able to identify the originator of any accessible system resources.
R7-64 SMS must be able to identify the originator of any information received across communication channels.
R7-65 SMS must provide mechanisms or procedures that can be used to periodically validate the
correct operation of the system These mechanisms or procedures should address:
(1) Monitoring of system resources
(2) Detection of error conditions that could propagate through the system
(3) Detection of communication errors above/below an NPAC-specifiable threshold
(4) Detection of Link Outages.
R7-66 SMS must be designed and developed to protect data integrity. This should include some
or all of the following:
(1) Proper rule checking on data update
(2) Proper handling of duplicate/multiple inputs
(3) Checking of return status
(4) Checking of inputs for reasonable values
(5) Proper serialization of update transactions
R7-67 NPAC documentation must contain recommendations for running database integrity
checking utilities on a regular basis.

7.5 Audit

7.5.1 Audit Log Generation

R7-68 SMS must generate an audit log that contains information sufficient for after-the-fact investigation of loss or impropriety and for appropriate response, including pursuit of legal remedies. The audit data shall be available on-line for a minimum of 90 days, and archived off-line for a minimum of two years.

R7-69 The user-identification associated with any SMS request or activity must be maintained, so that the initiating user can be traceable.

R7-70 SMS must protect the audit log from unauthorized access.

R7-7 1 Only well-defined privileged NPAC personnel can modify or delete any or all of the audit log.

R7-72 The audit control mechanisms must be protected from unauthorized access.

R7-73 SMS must cause a record to be written to the security audit log for at least each of the following events: (1) Invalid user authentication attempts (2) Logins and activities of NPAC users (3) Unauthorized data or transaction access attempts

R7-74 Auditing of NPAC actions must not be able to be disabled.

R7-75 For each recorded event, the audit record must contain, at a minimum: (1) Date and time of the event (2) User identification including associated terminal nort network srif4-v^^ ^communication device (3) Type of event (4) Name of resources accessed (5) Success or failure of the event

R7-76 Actual or attempted passwords must not be recorded in audit logs until after an NPAC-specifiable threshold of consecutive login failures. The SMS supplied default shall be three failures.

7.5.2 Reporting and Intrusion Detection

R7-77 SMS must provide post-collection audit analysis tools that can produce exception reports, summary reports, and detailed reports on specific data items, users, or communication failures.

R7-78 The NPAC must be able to independently and selectively review the actions of any one or more users, including other NPAC users, based on individual user identity.

R7-79 SMS must provide tools for the NPAC to monitor the activities of a specific network address or terminal in real time.

R7-80 SMS should contain a real-time mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent security violation. This mechanism shall be able to notify the NPAC immediately when thresholds are exceeded, and if the occurrence or accumulation of these security relevant events continues, SMS shall take the least disruptive action to terminate the event.

7.6 Continuity of Service

R7-8 1 No service provider action, either deliberate or accidental, should cause the system to be unavailable to other users.

R7-82 SMS should detect and report conditions that would degrade service below a pre-specified minimum.

R7-83 Procedures or mechanisms must be provided to allow recovery after a system failure or other discontinuity without a protection compromise.

R7-84 Procedures shall be documented for software and data backup and restoration.

R7-85 The system must contain a database containing the exact revision number of the latest software installed.

Software Vendor

R7-86 The SMS software vendor must have a corporate policy governing its internal development of software. This policy must contain specific guidelines and requirements that are aimed at the security of its products, and are applicable throughout the software life cycle.

R7-87 The SMS software vendor shall not design any mode of entry into the SMS for maintenance, support, or operations that would violate or bypass any security procedures.

R7-88The SMS software vendor shall not design any mode of entry into the SMS for maintenance, support, or operations that is not a documented feature of the SMS.

7.8 OSI Security Environment

This section examines potential threats to the NPAC SMS interfaces and proposes a set of security requirements to thwart such threats.

The security mechanisms described in the OSI Security segment are meant to illustrate the level of security and flexibility that is required for the OSI interfaces specified. The response to the RFP may propose different security mechanisms than the ones described. However, such security mechanisms should provide at least the same level of security and at least the same level of flexibility as the mechanisms described. The proposed mechanisms shall not be more difficult to manage, and should not require more processing or transmission capacity than the mechanisms described below.

7.8. 1 Threats

Attacks against the NPAC SMS may be perpetrated in order to achieve any of the following:

Denial of service to a customer by placing wrong translation information in the SMS

Denial of service to a customer by preventing a valid message from reaching the SMS

Disrupting a carrier's operations by having numerous spurious calls (to users who are not clients of that carrier) directed to that carrier

Switching customers to various carriers without their consent

Disrupting the functioning of the NPAC SMS by swamping it with spurious messages.

7.8.2 Security Services

The threats enumerated above can be thwarted by using the following security services:

R7-89 Authentication (at association setup)
R7-90 Data origin authentication for each incoming message
R7-91 Integrity - detection of replay, deletion or modification to a message
R7-92 Non-repudiation of origin

R7-93 Access control - allowing only authorized parties (i.e., carriers serving a given customer) to cause changes in the NPAC SMS database

7.8.3 Security Mechanisms

This section outlines the requirements for specific security mechanisms to support the security services enumerated above. For simplicity of presentation and without loss of generality, it assumes that information in the NPAC SMS is modified only in response to CMIP notifications from authorized entities.

7.8.3.1 Encryption

R7-94 Since non-repudiation must be supported a Public Key Crypto System (PKCS) must be used to provide digital signatures. Since there is no requirement for confidentiality service there is no need for any additional encryption algorithms. The NPAC SMS shall support one of the digital signature algorithms listed in the OIW Stable Implementation Agreement, Part 12, 1995.

R7-95 If a digital signature based on RSA encryption is chosen then the size of the modulus of each key shall be at least 600 bits. If another algorithm is chosen then the size of the key(s) shall be chosen to provide a level of security commensurate with RSA encryption with a 600-bits modulus.

R7-96 The digital signature algorithm shall be applied to ASCII representation of the signed data fields, without any separators between those fields or any other additional characters.

7.8.3.2 Authentication

R7-97 Strong, two-way peer authentication at association setup time shall be provided by using an authenticator (based on the authenticator used for the Trouble Administration application of Electronic Bonding as described in Committee T1 Technical Report No. 40 "Security Requirements for Electronic Bonding Between Two TMNs") consisting of

The unique identity of the sender

The Generalized Time corresponding to the issuance of the message, each party is responsible to assure that its system clock is accurate to within two minutes of GMT

A sequence number (equal to zero for association request and association response messages)

A key identifier

Any additional parameters required by the chosen digital signature algorithm, as specified in OIW Stable Implementation Agreement, Part 12, 1995

• The digital signature of the sender's identity, Generalized Time and sequence number listed above.

R7-98 The authenticator shall be conveyed in the CMIP access control field. (An appropriate syntax for this EXTERNAL field shall be provided.)

7.8.3.3 Data Origin Authentication

R7-101

R7-99 Every subsequent CMIP message that contains the access control field shall carry the authenticator described above in that field. Each party maintains a separate counter for the sequence number it uses. Every **time the** authenticator is used the value of the sequence number shall be incremented by one.

7.8.3.4 Integrity and Non-repudiation

R7-100 Because CMIP notifications do not have an access control field, all the notifications defined for the number portability application shall contain a security field. The syntax of the security field shall correspond to the authenticator defined above.

The values of the components of the authenticator shall also be as specified for the authenticator above, except that the digital signature shall apply to all the fields in the notification, except the security field, in the order in which they appear, followed by the GeneralizedTime and the sequence number. This ensures data origin authentication, integrity and non-repudiation of origin for each notification. In particular, the GeneralizedTime and the sequence number allow detection of deletion, replay and delay.

R7- 102 All the notifications shall be sent in the confirmed mode.

7.8.3.5 Access Control

R7-104The NPAC SMS shall be responsible for access control. In particular, it will assure that only authorized parties (current and future service providers for a given customer) can change information related to the number associated with that customer.

R7-105The only initiator-provided access control information that shall be used to this cffcst is thc authenticated ldenfity of the sender of the message that would result in a modification to the NPAC SMS database, and the value of the GeneralizedTime in that message (it should be within five minutes of the NPAC SMS system clock).

7.8.3.6 Audit Trail

R7-106The NPAC SMS shall keep a log (as defined in ISO/EC 10164 parts 6 and 8, 1992) of all incoming messages that result in the setup or termination of associations, all invalid messages (invalid signature, sequence number out of order, GeneralizedTime out of scope, senda not authorized for the implied request) as well as all incoming messages that may cause changes to the NPAC SMS database.

7.8.3.7 Key Exchange

R7-107There shall be an exchange of keys between the NPAC and each carrier it senses. DDg this exchange each party shall provide the other with a *list* of keys. The list shall be provided in electronic form. The originator of list of keys shall also provide the receiver with signed (in ink) paper copy of the MD5 hashes of the keys in the list. The lists can be exchanged in person or remotely. If the lists are exchanged remotely, they shall be conveyed via at least two different channels (e.g., a diskette sent via certified mail and file sent via e-mail).

R7-108Upon remote reception of a list of keys the recipient shall send an acknowledgment to the sender of the list. The acknowledgment shall consist of the MD5 hash of each one of the keys in the list. The acknowledgment shall be provided in electronic form via at least two different channels. In addition, the recipient shall call the sender by phone for further confirmation, and provide the sender with the MD5 hash of the whole list.

R7-109The NPAC shall issue periodically (e.g., once a month) a paper list of the MD5 hashes of all the public keys it uses and those of its clients. The list shall be sent to each client. Upon reception of the list and verification of its own the NPAC's public keys hashes, the client shall return an acknowledgment (by phone or mail) to the NPAC.

R7-110Each list shall consist of 1000 encryption keys, numbered from 1 to 1000, and 10 Key Encryption Keys (KEK), numbered from 1001 to 1010. Only encryption keys shall be used for digital signatures for normal number portability operations. They shall range in size (if RSA encryption is used) from 600 bits to 900 bits. (Larger keys shall be used in future years.) KEKs shall be used only to transmit a new list of keys, if necessary. The whole new list will be signed using a KEK. KEK sizes shall range from 1000 bits to 1200 bits (if RSA encryption is used). Keys in subsequent list shall be numbered from 2000 to 3010, 3000 to 4010, etc.

R7-111A new encryption key can be chosen with every message that contains a key identifier. After the usage of a key has stopped, that key shall not be used again. The key shall be changed every time there is a suspicion that the key has been compromised. The key shall be changed at least once a year. The keys used during a year shall be larger than the keys used the previous year by at least 20 bits.

SECTION 8: AUDIT ADMINISTRATION

Overview

An audit function will be necessary for troubleshooting a customer problem and also as a maintenance process to ensure data integrity across the entire LNP network. Audit will be concerned with the process of comparing the NPAC view of the LNP network with each service provider's network view. The service provider network may contain several network nodes designated for local number portability and may also choose to keep its own copy in its respective SMS. As a result, it will not be the responsibility of the NPAC to compare all network nodes but rather upon order of an audit request to have the service provider SMS report if a conflict exists in any of its designated LNP SCPs within its respective LNP network. The local SMS will compare the NPAC view of the data with the SCP view of the data.

Assumptions

SMS will contain the master copy of the data that it administers. Only the data administered over the NPAC SMS to Local SMS interface as a result of LNP subscription management will be audited.

8.1 Service Provider User Functionality

The following specifies the functionality required for audits issued by the service provider. These audit requests shall be issued from the service provider's SOA to the NPAC SMS. R8- 1 Service providers must be able to issue an audit request on a single telephone number. R8-2 Service providers must be able to issue an audit request for a range of telephone numbers. The size of the range of telephone numbers which can be specified must be a tuneable parameter set by the NPAC. R8-3 Service providers must be able to specify the scope of an audit by specifying one or more of the following parameters:
(a) Specific service provider network or ALL service provider networks.
(b) Full or partial audits, where the user can specify if one or ALL LNP attributes is to be audited, e.g., LRN, GTT or ALL. Default will be to audit ALL attributes.
(c) Indication whether to include non-ported numbers. For telephone numbers which fall within the range of telephone numbers specified and do not exist in the NPAC SMS database, then if this option is set these numbers will be audited, i.e., the NPAC SMS will ask the service provider's local SMS to return an indication if the record exists in its network or not. Default will be to not include non-ported telephone numbers.

8.2 NPAC User Functionality

Authorized NPAC personnel will have the capability to perform audits of the same nature as the service provider with some additional functionality. The NPAC SMS will provide a user interface for this purpose. This interface must support the following requirements of the audit function solely for execution by authorized NPAC personnel:

R8-4NPAC personnel will be able to issue an audit request on a single telephone number.

R8-5NPAC personnel will be able to issue an audit request for a range of telephone numbers. For the NPAC personnel there is no limit as to the size of the range specified.

R8-6The NPAC must provide the capability to issue an audit request to be executed immediately or a specific time in the future.

R8-7NPAC personnel will be able to specify if the audit request is to be periodic or a one time only request. Periodic audits can be specified to be issued weekly, monthly or quarterly. When a periodic type resumes execution, the audit will continue from where it last executed.

R8-8The NPAC user must be able to specify execution restrictions for an audit request. Execution restrictions include the following:
(a) Start time and end time window for the time period when the audit should execute.

R8-9The NPAC user must be able to specify the scope of an audit by defining one or more of the following parameters:
(a) Specific service provider network to be audited or ALL service provider networks.
(b) Full or partial audits, where the user can specify if one or ALL LNP attributes is to be audited, e.g., LRN, GTT or ALL. Default will be to audit ALL attributes.
(c) Indication whether to include non-ported numbers. For telephone numbers which fall within the range of telephone numbers specified and do not exist in the NPAC SMS, then if this option is set these numbers will be audited, i.e., the NPAC SMS will ask the service provider's local SMS to return an indication if the record exists in its network or not. Default will be to not include non-ported telephone numbers.
(d) Activation Date/Time stamp range, i.e., only audit records activated between a specific time window.
R8- 10 The NPAC user must be able to obtain the status of an audit request.
R8-11 The NPAC personnel must be able to obtain an audit's progress. Progress might indicate the percentage of records audited or the directory number of the record currently being audited assuming the records will be audited in a sequential fashion.
R8- 12 The NPAC personnel must be able to cancel an audit request.
R8-13 The NPAC personnel must be able to temporarily stop an audit which is currently in progress.
R8- 14 The NPAC personnel must be able to resume an audit which was temporarily stopped by the user or was stopped due to a failure which is now resolved.

8.3 System Functionality

R8- 15 All audit requests including requests issued by the service providers will be logged at the NPAC SMS and will be available for viewing by the NPAC personnel.

R8- 16 In order to execute the audit request, the NPAC shall send the audit request to the local service providers' networks via the NPAC SMS to Local SMS interface described in the LNP SMS Interface Specifications.

R8- 17 For all telephone numbers to be audited, the NPAC SMSwill send the telephone number record as it appears in the NPAC SMS to each service provider's local SMS. Upon receipt of the audit request, the local SMS will verify if the telephone number's entire record contents differs in its local network. The service provider's local SMSwiX verify the record contents in all respective SCP databases. The service provider's local SMSwill return an indication if any of its SCP databases is not in synch with the NPAC view of the data. For the case where non-ported numbers are being audited then the service provider's local SMSwiX report on the existence of the record in its LNP databases.

R8- 18 For periodic type audits, the audit will resume execution from where it last stopped after its previous execution.

R8- 19 The NPAC SMS must record all audit results in an audit log.

8.4 Audit Report Management

R8-20 Service Providers must be able to retrieve an audit report for a specific audit request via a specific transfer procedure offered for remote report retrieval as specified in the Reports management chapter.

R8-2 1 The NPAC SMS must generate an audit report for all audit requests. The audit report must indicate the following:

(a) Audit request parameters, e.g., Service Provider ID audited, telephone number range audited and other parameters which identified the scope of the audit.
(b) Date and Time of Audit.
(c) Progress key indication.
(d) Service Provider network which contains database conflict.
(e) A difference indicator which may indicate:
- mismatch between the NPAC SMS and local SMS
- record missing in local SMS
- record missing in NPAC SMS
- an audit failure
- no discrepancies found

R8-22 NPAC personnel must be able to generate and view an audit report.

R8-23 An audit report should be accessible while the audit is in progress so the current audit results can be viewed up to this point.

R8-24 The NPAC personnel must be able to output an audit report to a specified output device or to a text file.

R8-25 The NPAC personnel must be able to specify the length of time audit results will be retained in the audit log.

SECTION 9: REPORT MANAGEMENT

9.1 Overview

The NPAC SMS must support scheduled and ad hoc report generation for selectable reports. The report generation service shall create output report files according to specified format definitions, and distribute reports to output devices as requested.

A report distribution service is used to distribute report files to selected output devices.

Authorized NPAC personnel can request reports from active database, History Logs, Error Logs, traffic measurements, usage measurements, and performance reports.

Examples of the items available from active database are:

- List of ported TNs for a service provider
- List of pending subscription orders for a service provider
- Subscriptions without concurrence - Status of pending subscription order for a TN being ported
- Date/Time Stamp of Subscription Port (Activation)
- Date/Time Stamp of Subscription Disconnect (Activation)
- Records that required conflict resolution Previous service providers and dates of service for ported TNs
- Date/Time Stamp of Broadcast time for transactions
- Subscription order records in error
- Download requests in error
- Log of Missing Response from SOA for order matching
- Log of Missing Response from Local SMS for downloads
- Log of Unauthorized Access Attempts
- Counts of events and usage as described in resource accounting.

Performance Reports

- CPU usage.

- Number of transactions handled and transactions per second.

- Measure of time starting from the receipt of subscription order activation to the broadcast of transaction to Local SMSs.

- Measure of time starting from the receipt of subscription order activation to the receipt of response from Local SMSs.

- NPAC SMS to Local SMS link utilization

- NPAC SMS to SOA link utilization

9.2 User Functionality

R9-1 The NPAC personnel must be able to select the type of report required.

R9-2 The NPAC personnel must be able to select the output device destination (printer or other destination) for the report.

R9-3 The NPAC personnel must be able to save/reprint reports from backed up output files.

R9-4 The NPAC personnel must be able to create customized reports through an ad-hoc facility.

R9-5 The NPAC personnel must be able to define scope and filtering for items to be included in the customized reports.

R9-6 The service provider users must be able to receive reports on information related to their activities.

R9-7 Vendors must provide examples of report outputs.

9.3 System Functionality

R9-8 The NPAC SMS must provide easy to read on-line and hard copy reports of the requested information.

R9-9 The NPAC SMS must verify whether the user requesting the report has the proper viewing privileges for the selected data.

R9-10 The NPAC SMS must support on-line file transfer capabilities (e.g., FTP or FTAM) to transfer report files.

R9- 11 The NPAC SMS must maintain a History Log to keep track of transaction processed.

R9- 12 The NPAC SMS must maintain an Error Log to keep track of transaction errors, transmission errors, unauthorized access attempts.

R9-13 Vendors must specify a list of available output device options.

SECTION 10: NPAC SMS RELIABILITY, AVAILABILITY, PERFORMANCE AND CAPACITY

This section defines the reliability, availability, performance and capacity requirements for the NPAC SMS.

10.1 Availability and Reliability

The NPAC SMS will be designed for high reliability, including fault tolerance and data integrity features, symmetrical multi-processing capability, and allow for economical and efficient system expansion. The system will adhere to the following availability and reliability requirements:

R10-1 It wiU be available 24 hours a day, 7 days a week.

R10-2 It's reliability win be 99.9%. This applies to an functionality and data integrity.

R10-3 The amount of unscheduled downtime per year will be <= 9 hours.

R10-4 For unscheduled downtime, the mean time to repair will be <= 1 hour.

R10-5 The amount of scheduled downtime per year will be <= 24 hours.

R10-6 It win be capable of monitoring the status of all of its communication links and be capable
of detecting and reporting link failures.

R10-7 It win be capable of detecting and correcting single bit errors during data transmission
between hardware components (both internal and external).

R10-8 If a failure occurs resulting in downtime of any functionality, affected transactions received
immediately prior to the failure must be queued and processed when functionality resumes.

R10-9 The design will provide:

- Functional components with on board automatic self checking logic for immediate fault locating.

- Continuous hardware checking without any performance penalty or service degradation.

- Duplexing of all major hardware components for continuous operation in the event of a system hardware failure.

- Hardware fault tolerance that is transparent to the service providers.

R10-10 If the system becomes unavailable for normal operations due to any reason, including both scheduled and unscheduled maintenance, service providers must be notified of the system unavailability.

- When possible, the notification will be made via an electronic broadcast message to the service providers. When this is not possible, the NPAC will notify the service providers via their contact numbers.

- The notification will include, at a minimum, the functionality that is unavailable, the reason for the downtime, estimated length of the downtime and a NPAC contact number.

R10- 11 Dunng any maintenance, if resources allow only partial functionality, the capability of receiving, processing and broadcasting updates will be given the highest priority.

R10- 12 It must provide system tolerance to communication link outages and offer alternate routing during such outages.

R10-13 For any downtime, either schedule or unscheduled, lasting more than 1 hour, the NPAC SMS will switch service providers to a backup or disaster recovery machine as described in section 2. In most cases, the time to switch the service providers to another machine and provide full functionality must not exceed the mean time to repair . However, in the event of a disaster that limits both the NPAC and NPAC SMS ability to function:

- The capability of receiving, processing and broadcasting updates must be restored within 24 hours.

- Full functionality must be restored within 48 hours.

The vendor is requested to describe the architecture used to satisfy the reliability and availability requirements, including any the use, if any, of a backup and/or disaster recovery machine and the use of any disaster recovery location. Alternatives to the backup and disaster recovery process flow in section 2 should be included here.

R10- 14 Reports documenting the performance of the NPAC SMS in regards to the above requirements will be provided periodically to the service providers.

10.2 Capacity and Performance

The following requirements define the capacity and performance of the NPAC SMS. While the initial transaction rates and data storage requirements are not high, the NPAC SMS is expected to provide high performance and allow for future expansion. Refer to section 13 for future expansion possibilities.

R10-15 The system will be engineered to allow for 30 service providers having SOA and SMS interfaces. On initial turnup, it is expected there will be 10 service providers having SOA and SMS interfaces.

R10- 16 Describe any capacity requirements related to the NPAC personnel who will be users of the NPAC SMS.

R10- 17 It will be capable of handling the following transaction rates. Each record added or updated involves 1 transaction from the old service provider, 2 transactions from the new service provider and a broadcast to every service provider. Transaction rates are projected in three categories, i.e., High, Medium, and Low:

	HIGH	MEDIUM	LOW
Year 1:	70,000	50,000	25,000
Year 2:	100,000	70,000	50,000
Year 3:	500,000	250,000	100,000
Year 4:	750,000	500,000	250,000
Year 5:	1,000,000	500,000	500,000

The number of updates due to mass changes, the number of audit requests and the number of report requests is not known at this time.

R10-18 Data storage of the History file must keep track of all transactions made for one year (churn and new records.) It is assumed that there will be thirty percent churn of accumulated records.

R10- 19 From the time an activation notice is received from the new service provider to broadcast out an update until the time the update is broadcasted to all service providers will be < 60 seconds.

R10-20 The response time from when a request or transaction is received in the system to the time an acknowledgment is sent to will be < 3 seconds. This does not include the transmission time across the interface to the service provider's SOA or SMS.

R10-21 The NPAC SMS must be expandable to handle any future growth due to circumstances described in section 13.

1 1.1 Overview

Resource Accounting allows the tracking of NPAC resource usage data, which may be used as a basis for billing the service providers for their use of NPAC functionality. Resource Accounting is responsible for gathering the information into usage measurement categories, aggregating the measurements, and formatting and outputting the measurements to the appropriate entities (e.g., Billing Operations Applications, service providers). Other potential applications for usage information include cost allocation, marketing, and usage studies.

The NPAC system cost recovery methods should be designed to recover initial system costs, as well as the on-going operations/maintenance/administration costs. The vendors shall describe the cost drivers for NPAC HW/SW platform, including a breakdown of cost for the major features. The vendors may propose additionaUalternate measurements that are based on their specific implementation, and provide measure of usage of the relevant cost causing elements in the NPAC system. The vendors shall describe their proposals for cost recovery and billing to the participating service providers.

The following are some examples of items measured for each service provider:
A. Duration of login session, date/time, service provider ID, user login ID, of login session
B. Number of transactions (port/ disconnect/cancel) processed
C. Counts of types of updates made (e.g., # of port, # of disconnect)
D. Number of errors encountered in transactions
E. Number of errors encountered during transmission
F. Number of current records maintained
G. Number of pending records maintained
H. Number of history 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 re-sent due to transmission problems
L. Number of records in conflict
M. Number of missing responses (e.g., during order matching)
N. Number of records audited on request
O. Number of records corrected (e.g., as result of audit)
P. Number of records queried/ viewed
Q. Amount of data transported to Local SMS as bulk load update
R. CPU usage

S. Failures and maintenance problems in the NPAC SMS

Please indicate what other measurements may be made.

1 1.2 Assumptions

The service providers will be billed in proportion to their usage of the NPAC system services.
The resource accounting measurements will not cause degradation in the performance of the basic
functions of the NPAC.

1 1.3 User Functionality

R 11 - 1 The NPAC personnel shall be able to turn on or off the generation of usage measurements for each of the usage types.

1 1.4 System Functionality

R11-2 The NPAC SMS shall measure and record the usage of NPAC resources on a per service provider basis to cost allocation / billing.

R11-3 The NPAC SMS shall generate usage measurements for login sessions, for each service provider SP.

R11-4 The NPAC SMS shall generate usage measurements for the allocated mass storage (number of records stored), for each service provider.

R11-5 The NPAC SMS shall measure the number of transactions processed, for each service provider.

R11-6 The NPAC SMS shall measure the number of transactions downloaded to each service provider.

R11-7 The NPAC SMS shall measure the number of records sent in response to a request for resend of data from the service provider.

R11-8 NPAC should be able to render detailed periodic bills to the contracting entity.

SECTION 12: NUMBER PORTABILITY ADMINISTRATION CENTER

12.1 **Number Portability Administration Center (NPAC)**

NPAC Role

The NPAC will be staffed by a neutral third party contractor who will be responsible for the administration and operational support services required by service providers in their use of the NPAC SMS. The NPAC must be run in support of consortium of local service providers. As a result of agreed-to guidelines, the NPAC will be involved in local ported number administration monitoring. Mechanized enforcement capabilities may or may not exist in the NPAC SMS to assist the NPAC in the monitoring and control functions.

Operational Functions

The primary roles of the NPAC are to assist users in obtaining reliable access to the NPAC SMS and to support all users encountering local ported number service provisioning problems resulting from NPAC SMS operation. To meet this need, the NPAC must support the following functional areas: System Administration, User Support, and System Support.

Administrative Functions

Administrative functions include all management tasks required to run the NPAC. The NPAC Contractor must be accountable for all personnel, legal, and financial management associated with the NPAC. These include, but are not limited to billing management, staffing, equipment and site procurement, facilities, and the contractor's own accounts payable obligations, which are part of day to day management. The NPAC contractor must provide for the administration of its staffing, contractual, financial, and operational needs. Proposals must specify how this will be accomplished.

The NPAC will be responsible for working with Local service providers to update data tables required to route calls for ported local numbers. The NPAC is also responsible for distributing the most current version of ported local number administration guidelines.

NPAC staff performing these activities needs to combine strong project planning skills, organizational management experience, interpersonal communication and negotiation skills, and a clear understanding of the day-to-day business issues associated with running a successful NPAC. The NPAC manager and administrative staff ideally would come from a data processing environment requiring these attributes.

System Administration

System administration is the NPAC operational group responsible for NPAC SMS logon administration, user access and customer data security, user notification of scheduled system downtime, and management and administration of the NPAC SMS information tables required to link customer records with the correct ported number service functions, features, and network routing information.

1 2.2 Logon Administration

Key Responsibilities

- Assist with new logon requests
- Verify logon signature approval
- Initialize logon ID, password, and security level
- Update data base and add new users
- Notify user cxf logon activation
- Resolve problems with existing logon IDs or passwords

Procedure Description

Logon Administration provides an individual requiring access to the NPAC SMS system with a unique logon ID and password upon receipt of an approved request form.

Access is initiated upon receipt of a completed NPAC SMS logon ID request form having the proper signature approvals from the requesting organization and the NPAC manager. Afta access approval, the logon administrator will assign the logon ID and appropriate security level corresponding to the type of NPAC SMS user. The user's security clearance sets the correct level of customer record access and NPAC SMS functional capabilities. After the logon is initialized and entered into the NPAC SMS, the users are informed of the logon activation, and a completed NPAC SMS logon ID request form is mailed back to them for their records.

Logon administration is responsible for resolution of any of the user's NPAC SMS access problems that the User Support group cannot solve. All problems should be recorded as NPAC consultation reports and entered as trouble reports into a mutually agreed upon trouble reporting system. The NPAC must attempt to resolve all problems in real-time. Those requiring additional assistance will be assigned a priority level in the trouble report system and the appropriate NPAC SMS support group will be contacted directly. The NPAC is required to report issue resolution status back to the reporting party on a timely basis.

12.3 Customer Record Security

Key Responsibilities

- Establish user boundaries through user access permission classes
- Assign new users to the correct security permission class
- Exercise absolute control of access to customer records
- Monitor and report unauthorized system access attempts

Procedure Description

Closely linked with logon administration is the procedure that provides the correct level of system access and customer data record access. The permitted level of access depends on the classification of NPAC SMS user. Before any logons are assigned, a security group will be associated with a specific classification of NPAC

SMS user. The NPAC will establish boundaries for the appropriate level of customer record access and feature set functionality.

When the security groups are configured, any logon request that is received must be assigned to the correct user class. The logon Administrator is responsible for determining the correct group based on the organization that originates the request.

1 2.4 Scheduled System Unavailability Notification

Key Responsibilities

Notify users in advance of planned or known system unavailability

Procedure Description

In concert with the System Support group, System Administration is responsible for notifying NPAC SMS users of scheduled periods of system shutdown. These periods may be due to routine maintenance of the system or the result of non-critical system failures that require a brief and immediate shutdown of the system for repairs. Users are given sufficient warning to complete their current transactions and exit the system without loss of information. Users will usually be made aware of periods of system shutdown via electronic mail capabilities of the NPAC SMS.

12.5 Software Release Acceptance Testing

Key Responsibilities
- Update software test plans
- Allocate staff for performing tests
- Execute test plans
- Generate and resolve testing trouble reports
- Document test results
- Certify NPAC SMS software and release for operation

Procedure Description

The NPAC is required to perform acceptance tests on every release of the NPAC SMS system software before certifying it for operational release. The NPAC SMS release test plan must be reviewed and updated by the NPAC contractor for each NPAC SMS release, including testing of new features or existing features that have been modified and any major fixes that have been implemented. It is the responsibility of the NPAC contractor, as part of an acceptance test plan to fully regression test major releases.

The System Adrninistration group is responsible for testing those functions associated with its specific procedural duties included in the NPAC release test plan. These include, but are not limited to the following:

System Logon and Security Features
NPAC SMS administrative data table update features
Customer record features
Electronic mailbox features

Completion of acceptance tests will result in a release certification report summarizing all the test results, including those errors encountered and the resolutions required to successfully pass the tests.

1 2.6 Service Administration

Key Responsibilities

- Create and maintain NPAC SMS data table
- Map table information to appropriate codes (e.g., NPA, LRN, GTT)
- Create and maintain descriptive data table labels

Procedure Description

The Tables Administration function within the System Administration group is responsible for creating and maintaining internal NPAC SMS data tables used to validate data entries and minimize user input errors through the use of appropriate quality assurance and quality control methods. There are several different types of tables which can be grouped into mapping, validation, and NPA splits/mass changes tables, which include, but are not limited to the following:

- Location Routing Number (LRN) tables
- Service Provider GTT information tables
- RAO codes
- Service Provider codes

The procedures associated with table administration vary depending on the table involved.

12.7 Mass Change Administration

Key Responsibilities Maintain a close working relationship with organizations responsible for NPA split/mass changes scheduling.
- Analyze split or mass change impact on NPAC SMS administrative tables
- Analyze split or mass change impact on NPAC SMS customer records
- Notify pending split to appropriate service provider service administration centers.
- Coordinate with data center vendor to execute NPAC SMS programs required to perform table and record modifications.

Procedure Description

The splitting of an NPA and the resulting mass changes required to NPAC SMS records are elements of an infrequent and complex process beginning more than one year before the cutover date. The NPAC becomes involved after receiving notification from the company responsible for the split. The goal of the NPAC is to transparently transition affected records in the NPAC SMS data base to reflect the new NPA information.

The first step in the process is to analyze the impact of the split on the NPAC SMS table and record information. After impact analysis and record sorting have been completed the NPAC will work closely with the NPAC SMS data center support group to include the modifications as part of the data base.

Specific tasks performed by the group are routine and procedural. Staff members will need to have clerical data processing skills and training in on-line computer processing. Types of problems resolved by the System Administration Staff will primarily concern user access and system security issues. Procedures are needed for mass changes other than NPA splits such as LRN or DPC changes.

User Support Group

The User Support Group is the primary NPAC contact for NPAC SMS users encountering problems with system features, or with inputting or accessing of their customer record data. The group would also be responsible for the dissemination of NPAC SMS status information, such as scheduled downtime, new software releases, documentation updates, and training registration information.

This group provides the NPAC SMS user a central point of contact for resolution of NPAC SMS problems and trouble reporting. Resolution of user problems will be handled primarily through the efforts of the User Support Group itself. Those issues requiring the efforts of another NPAC group will be promptly referred to the appropriate group. Issues requiring Vendor or NPAC SMS Data Center operations support must always be researched first by the responsible NPAC staff member The key point of contact for users will always reside within the NPAC for NPAC SMS service Issues.

1 2.8 User Problem Resolution

Key Responsibilities

- Resolve customer record access problems
- Clarify feature capabilities for users
- Resolve customer record input and modification problems
- Perform acceptance testing for new software releases
- Support link problem resolution with datalink protocol analysis capabilities

Procedure Description

The primary function of the User Support Group is solving the problems of the NPAC SMS user. Phone calls to the User Support Group must be dealt with as they are received, with the goal of real-time problem resolution (i.e., within one hour). If this requires the assistance of another group within the NPAC, the call should be transferred to a staff member who can better aid in resolving the issue. This requires the User Support staff to be knowledgeable in all NPAC regpongibilitieg and aware of specific expertise The PAC is responsible for responding to the user with either an answer or a date by which an answer will be available. If the problem is determined to be critical it will be given priority within the NPAC.

1 2.9 Software Release Acceptance Testing

Key Responsibilities

- Update software test plans
- Allocate staff for performing tests
- Execute test plans
- Generate and resolve testing trouble reports
- Document test results
- Certify NPAC SMS software and release for operation

Procedure Description

The NPAC is required to perform acceptance test on every release of the NPAC SMS system software before certifying it for operational release. The NPAC SMS release test plan must be reviewed and updated by the NPAC contractor for each NGAC SMS release including testing of new features or existing features that have been modified. It is the responsibility of the NPAC contractor to fully regression test major releases.

The User Support group must work with the administrative organization to test those functions associated with its specific procedural duties included in the NPAC release test plan which include but are not limited to:

- Customer record features
- Electronic mailbox features
- Help messages

Resolution of testing problems must occur to complete testing and gain approval of the software release. Completion of the acceptance tests will result in a release certification report summarizing
all the test results, including those errors encountered and the resolutions required to successfully pass the tests.

12.10 Software Update Notification

Key Responsibilities

- Notify users of upcoming NPAC SMS software releases

Procedure Description

In an administrative capacity, the User Support Group is responsible for keeping the NPAC SMS user community abreast of system software update activity. The notifications must include the specific reasons for the new release and summaries of what is being added, deleted, or modified with respect to system features and capabilities. If the release was unscheduled and is the result of resolution of several critical system problems, the notifications must summarize all problems being corrected. Updated documentation should be included as part of the software update.

12.11 Training Administration

Key Responsibilities

- Serve as primary contaa for course schedules/registration information
- Ensure availability of all NPAC SMS training

Procedure Description

The User Support Group is responsible for managing the availability of NPAC SMS training courses and the handling of user registration requests. The NPAC may develop and administer all NPAC SMS training independently, or procure from another qualified training vendor, the facilities and instructors necessary to teach the courses. The training materials must be procured

from a qualified vendor. The NPAC will also perform training registration. Course schedules will be negotiated between the User Support Group and the training vendor, based on course demand forecast by the User Support Group. The training vendor will be responsible for billing attendees directly.

12.12 Document Order Administration

Key Responsibilities

- Process documentation requests
- Provide billing documentation
- Initiate documentation update distribution
- Provide documentation description, ordering information and price list literature

Procedure Description

In an administrative capacity, the User Support Group is responsible for handling user requests for NPAC SMS documentation. The NPAC will maintain an inventory of available NPAC SMS documentation for quick processing of orders, as available. The NPAC will handle all customer billing for documentation. Phone in documentation inquiries should be handled immediately. If documentation description, pricing, or ordering information literature is requested, it must be mailed to requester within 24 hours. Orders should be accepted only from companies with active system logons and must be accompanied by a documentation request form. Facsimiles should be accepted in emergency situations. Documentation billing will be added to the NPAC SMS user's service bill.

12.13 Training and Documentation User Feedback

Key Responsibilities

- Getting appropriate user recommendations reflected in NPAC SMS system documentation and training material

Procedure Description

User feedback for NPAC SMS training and documentation is just as important as feedback receiver for the operational system itself. The User Support Group is responsible for recording the feedback received during phone in conversations. Those comments pertaining to training and documentation must be recorded and entered into the trouble reporting system just as a service problem would be entered. Analysis of the impact of a problem on training or documentation material should be included as part of the impact analysis done for every trouble report entered into the trouble system.

12.14 SCP Download Problem Resolution

Key Responsibilities

- Analyze and resolve exception report issues resulting from unsuccessful updates to Local service providers' networks

Procedure Description

Failures in the download of customer records to the service providers Networks served by NPAC SMS are reported to the NPAC User Support Group. User Support staff must resolve all download failures.

Failures will primarily be the result of unsuccessful sending of customer records and/or NPAC SMS administrative instructions to the receiving service provider network. Resolution of customer record download failures to an service providers network must have the highest priority. Resolution efforts must continue until the problem is solved, with the service provider receiving notification when the updates are successfully completed.

The User Support Group requires staff who are well versed in all NPAC SMS capabilities. The ability to learn from many different user problems and to quickly relate a given problem to a previous experience will ensure successful user support. The User Support staff must also speak English clearly. have excellent communication skills to effectively interact with NPAC SMS users and take prompt action to resolve problems.

System Support Group

The System Support group is responsible for resolving or coordinating resolution of all user or NPAC SMS problems relating to system availability or technical communication problems. This group will be responsible for maintaining reliable system communication linkages between NPAC SMS and all other local number systems that rely on NPAC SMS for information updates. These will include, but are not limited to service providers' networks used *to* perform call routing functions, Directory Assistance Provider's system (when available), local exchange carrier Revenue Accounting Offices, Signaling and Engineering Administration Centers (SEAC or equivalent organizations) and other NPAC SMSs. The NPAC SMS will generate a multitude of system performance, customer record, and problem exception reports. The System Support group must be able to interpret, generate, and distribute reports requested by an NPAC SMS user.

12.15 NPAC SMS Report Administration

Key Responsibilities

- Generate and distribute NPAC SMS reports to all requesting users who are entitled to receive reports
- Validate the accuracy of report contents
- Generate and distribute reports to NPAC SMS users who are entitled to receive reports and do not have local print facilities
- Resolve report interpretation problems

Procedure Description

The System Support group is the key point of contact for resolution of problems pertaining to NPAC SMS reports. The System Support group must ensure that the system is able to produce requested reports and assist in the validation and interpretation of any report. As with other NPAC SMS problems the System Support staff will file a trouble report in the system for evaluation and record keeping. Any NPAC SMS user with an active NPAC SMS logon can view or obtain copies of those reports allowed by the security associated with their logon ID.

12.16 Failure Recovery Administration and User Notification

Key Responsibilities

- Notify all NPAC SMS user groups of an unscheduled system shutdown or failure

- Serve as the key point of contact for system recovery status

Procedure Description

In the event of an unscheduled, instantaneous system shutdown or failure, the NPAC SMS Data Center operations staff will notify the NPAC System Support group within five minutes of failure. Within 15 minutes of failure, the NPAC will notify the NPAC SMS user community. Notification will be through an NPAC SMS broadcast message. If the system is not available the NPAC must provide a system status hotline number that users can call to obtain the latest system information. The NPAC will receive updated system status from the NPAC SMS data center at agreed upon intervals, and convey that information to the users via the NPAC SMS system or hotline. The NPAC will inform the NPAC SMS users of the data base status after the problem is fixed. Users will need to know the time period during which transactions were lost and affect restoration to the best of their abilities, while the NPAC will help in reconciliation.

12.17 NPAC SMS Interface Monitoring

Key Responsibilities

- Assist in the resolution of data communication problems with other NPAC SMS service systems (service providers, Operator Service Systems, RAOs, etc.)

- Provide technical assistance to NPAC SMS users experiencing problems accessing the system

- Generate automatic audit reports

Procedure Description

The objective of this System Support function is to provide reliable NPAC SMS user access and system communication with other ported nusnber service system components through the performance of routing functional audits. These audits must be organized into a suite of tests that are run periodically, and at least every week. The results of these audits will be used by more technically trained staff to detect potential system performance or availability problems. In all cases the System Support group must be responsible for coordinating the resolution of issues involving user access to the NPAC SMS. NPAC SMS problems will typically be referred to System Support through phone calls received by the NPAC User Support group. All issues must be documented in the form of a NPAC consultation report, and, if due to a system failure, must be recorded as a trouble report in the trouble reporting system.

12.18 Software Release Acceptance Training

Key Responsibilities

- Update software test plans
- Allocate staff for performing tests
- Execute test plans
- Generate and resolve testing trouble reports
- Document test results
- Certify NPAC SMS software and release for operation

Procedure Description The System Support group is responsible for testing those functions associated with its specific procedural duties included in the NPAC release test plan. These include, but are not limited to:

- NPAC SMS report availability verification
- NPAC SMS service maintenance and diagnostic procedures
- NPAC SMS-Service Provider administrative functions

Resolution of testing problems must occur to complete testing and gain approval of the software release. The NPAC will work with the platform provider to resolve NPAC SMS system related problems. All problems will be recorded in the trouble reporting system. Key attributes staff members of the System Support group must possess the ability to diagnose a problem using a strong set of technical system skills, and quickly disseminate that information to the appropriate NPAC or Vendor Support groups to rectify the situation. Personnel staffing these positions need to have strong data processing, problem diagnosis and system communication skills and previous experience supporting a data processing operation. Specific skills include knowledge of the NPAC SMS System Vendor's Information Management System for data base systems, operating system, and their wide area data communications protocols.

NPAC Organizational Interface Requirements

In meeting contractual requirements the NPAC contractor will be required to interact with a diverse set of organizations, especially the full range of NPAC users. The most common user will be companies using the NPAC SMS as the centralized data base for their provisioning of ported local numbers for their customers. The NPAC will also work with the service providers' support and service administration organizations which use ported local number routing instructions. The NPAC must be able to work with service providers utilizing multiple software vendors. All users will identity their primary contacts to the NPAC for each area

NPAC SMS Data Center

The NPAC contractor will also manage the data center operation and as such, they shall be required to provide hardware, operational support for NPAC SMS application(s) including systems engineering to integrate computer system and communications components. The NPAC SMS data center is redundant. (Further Reliability requirements are outlined in Section 10.)

The NPAC contractor will have direct contact with the data center operations staff to assist in resolution of NPAC SMS access and communication problems. Coordination of scheduling and execution of special NPAC SMS table administration, NPA splits, and mass change programs will be handled by the NPAC with the data center operation. The NPAC and the data center will share information necessary to plan for growth or reconfiguration of the hardware platform and communications.

12.19 Administration

The administrative staff must provide support and direction for the operational NPAC groups and manage the business and technical issues affecting the performance of NPAC services.

Key Responsibilities

- Plan NPAC staff for software acceptance testing, report acceptance results, and ensure problem resolution of discrepancies.
- Schedule staff training for new software features and updates Analyze documentation and training impact
- Coordinate testing and cutover with NPAC SMS data center operations
- Coordinate critical software release cutover
- Provide billing for service providers' usage
- Manage NPAC accounts receivable collection
- Manage NPAC accounts payable responsibilities
- Resolve any NPAC billing disputes
- Process bills to NPAC from data center operations and system vendor for support services
- Adjust Staffing Level Based on Forecast System Usage Demands
- Plan capital equipment based on required staffing levels and NPAC performance standards
- Manage NPAC facilities
- Monthly status reports on total billing, summary of customer service activities, transactions, and trouble reports, summary of administrative and other support activities
- List of trouble reports, with a breakdown between NPAC SMS and NPAC user complaints
- List of cleared trouble reports

12.20 Facilities Requirements

The NPAC must provide an actual or virtual point of presence in the Chicago LATA 358 in Illinois by which service providers can connect to the NPAC SMS. Service providers will be able to connect to the NPAC SMS by connecting to either the NPAC SMS facility location or to the Chicago LATA point of presence

The physical location of the NPAC facility is at the discretion of the NPAC contractor. The only limitation is that the facility must be within the continental United States. Identification of the proposed NPAC location must be included as part of the bidder's response.

The facility may be a separate building or be part of a larger facility owned or leased by the NPAC contractor. If the NPAC is located within a larger facility, space allocated to the NPAC must have the following characteristics:

- Be dedicated entirely for NPAC use
- Be a distinguishable area, separate from other parts of the facility by use of secure access points
- Be contiguous space so that all NPAC staff members are physically located within the same secure area

- Serve as the primary (and, if applicable, secondary) work areas for all NPAC functions to be performed
- Have sufficient and suitable telecommunications links available with diverse routing disaster protection
- Provide sufficient backup power to maintain operation through electrical outages of at least eight hours

The amount of space allocated by the NPAC contractor must be specified in proposals. The specification must include square footage and work space layouts for each of the NPAC staff members. It is recommended that each functional area specified have its own distinct work area. Any equipment required by the different groups should be located within the individual functional group work area, except for equipment deemed to be common to multiple NPAC groups (e.g., high-speed printers, data communication controllers) which may be located in a common area.

12.21 Telecommunications Requirements

Key Requirements

- Individual phone lines for staff members
- hour hotline
- Voice messaging system
- Data communication facilities
- FAX Machine
- Each NPAC staff member must have an individual phone line to their desk. All phone lines must provide the capability of transferring a call to any other phone line within the NPAC.
- The NPAC must have a primary phone number (hotline) with direct inward dialing functionality. Staff members must be able to answer the hotline directly from their desks. This number will be the primary means of contact for the NPAC SMS users who have questions.
- The phone system must provide the capability to allow a caller to leave a message easily. This can be accomplished by an electronic messaging system that allows the caller to leave a message for the person called. In any case, a visual indication that a message has been left is required. The caller must be able to reach a "live" NPAC staff member at all times.
- The NPAC must provide a 24-hour hodine that will give the NPAC SMS user:
- Guaranteed Access to an Actual NPAC Staff Member 24 Hours a Day
- The latest NPAC SMS status available at times when the system may be unavailable during scheduled or unscheduled downtime.
- The choice of voice communication architecture, vendors, equipment, and services is totally at the discretion of the NPAC contractor. The goal of these choices should be to best meet the functionality and service requirements described above. The NPAC contractor will be responsible for the cost and services management of its voice communication facilities. The NPAC contractor will also be responsible for meeting or exceeding the required qualitative and quantitative performance levels that will be part

of the regular service monitoring audits. Bidder response to this RFP must include a description of the proposed NPAC voice communication facilities to be implemented.

- Procurement and management of the data communication facilities required between the NPAC contractor, the data center, and the system vendor are the responsibility of the NPAC contractor. The contractor must provide redundant data communication facilities to provide for disaster recovery due to facility outages. It will be the responsibility of NPAC contractor to meet the data communication specifications of the NPACSMS system vendor. Data Communication must also include the ability to input into the appropriate trouble reporting systems.

12.22 Staffing

Key Requirements

- Please provide proposed staffing profiles and staffing levels. This must be part of the bidder's initial response.
- Please indicate whether you are using part and full-time employees and also the screening process for determining employment.

12.23 Service Objectives

NPAC Availability

NPAC hours of operation will be 24 hours a day, seven days a week. Staffing at the facility will be at appropriate levels to ensure quick response to user needs at any time of the day or week.

Quality of Service

The goal of the NPAC is to provide high quality NPACSMS support and user support. NPAC will play a key role in the achievement of error free, ubiquitous ported local number service provisioning on the part of service providers. In this role, the NPAC contractor must, at all times, be mindful of the revenue and time sensitive nature of the support services provided to users.

Performance Standards

The NPAC contractor performance will be monitored in accordance with the standards proposed as part of the bidder's response and then negotiated following the contractor selection. These NPAC service standards must tie together the following three quality-of-service components: Performance standards for NPAC procedural tasks (illustrative task standards available upon request) Bidder's quality assurance and control guidelines upon which NPAC staff members base their individual performance objectives NPACcontractor defined performance evaluation process that, through self-monitoring, provides ongoing measurements of how well NPAC service objectives are being met.

- The bidder's response must address standards addressing each of the following criteria:

- Service consistency
- Service reliability
- Service response time

The NPAC contractor's performance will be evaluated by the Contracting Party. The process will consist of both quantitative and qualitative assessments.

Requirements Checklist

This section provides a summary checklist of the requirements and responsibilities of NPAC. Respondents are required to review the applicable information in each of the references cited and are required to provide an RFP response affirming compliance (or non-compliance) with the specification. Affirmative statements will require compliance in generally available production system(s) to meet the 4Q96 in-service date. If not able to state compliance with all of a reference's requirements to meet such date, the responding vendor shall provide the earliest date that a compliant product can be delivered.

- Does (will) the product comply?

Product compliant delivery date

References

	Does (will) the product comply?	**Product compliant delivery date**
12.2 Logon Administration		
Assist with new logon requests	Yes___ No___	
Verify logon signature approval	Yes___ No___	
Initialize logon ID, password and security level	Yes___ No___	
Update database and add new users	Yes___ No___	
Notify user of logon activation	Yes___ No___	
Resolve problems with existing logon IDs or passwords	Yes___ No___	
12.3 Customer Record Security		
Establish user boundaries through user access permission classes	Yes___ No___	
Assign new users to the correct security permission class	Yes___ No___	
Exercise absolute control of access to customer records	Yes___ No___	
Monitor and report unauthorized system access attempts	Yes___ No___	
12.4 Scheduled System Unavailability Notification		
Notify users in advance of planned or known system unavailability	Yes___ No___	
Does (will) the product comply?	Yes___ No___	

12.5 Software Release Acceptance Testing

Update software test plans Yes___ No___ _____

Allocate staff for performing tests Yes___ No___ _____

Execute test plans Yes___ No___ _____

Generate and resolve testing trouble reports Yes___ No___ _____

Document test results Yes___ No___ _____

Certify NPAC SMS software and release for operation Yes___ No___ _____

12.6 Administration of Global Tables

Create and maintain NPAC SMS data tables Yes___ No___ _____

Map table information to appropriate codes Yes___ No___ _____

(i.e., NPA, NXX, LRN)

Create and maintain descriptive data table labels Yes___ No___ _____

12.7 NPA Split/Mass Changes Administration

Maintain a close working relationship with organizations Yes___ No___ _____

responsible for NPA split/mass changes scheduling Yes___ No___ _____

Analyze split impact on NPAC SMS administrative tables Yes___ No___ _____

Analyze split impact on NPAC SMS customa records Yes___ No___ _____

Notify pending split to appropriate service provider service Yes___ No___ _____

administration centers

Coordinate with data center vendor to execute Yes___ No___ _____

NPAC SMS programs required to perform table and Yes___ No___ _____

record modifications

12.8 User Problem Resolution

Resolve customer record access problems Yes___ No___ _____

Clarify feature capabilities for users Yes___ No___ _____

Resolve customer record input and modification problems Yes___ No___ _____

Perform acceptance testing for new software releases Yes___
No___ _____

12.9 Software Release Acceptance Testing

Update software test plans Yes___
No___ _____

Allocate staff for performing tests Yes___
No___ _____

Execute test plans Yes___
No___ _____

Generate and resolve testing trouble reports Yes___
No___ _____

Document test results Yes___
No___ _____

Certify NPAC SMS software and release for operation Yes___
No___ _____

12.10 Software Update Notification

Notify users of upcoming NPAC SMS software releases Yes___ No___ _____

12.11 Training Administration

Serve as primary contact for course schedules/registration information Yes___ No___ _____

Ensure availability of all NPAC SMS training Yes___ No___ _____

12.12 Document Order Administration

Process documentation requests Yes___ No___ _____

Provide billing documentation Yes___ No___ _____

Initiate documentation update distribution Yes___ No___ _____

Provide documentation description, ordering information and price list literature Yes___ No___ _____

12.13 Training and Documentation User Feedback

Getting appropriate user recommendations reflected in NPAC SMS system documentation and training material Yes___ No___ _____

12.14 SCP Download Problem Resolution

Analyze and resolve exception report issues resulting from unsuccessful SCP updates Yes___ No___ _____

12.15 Report Administration

Generate and distribute NPAC SMS reports to all requesting users who are entitled to receive reports Yes___ No___ _____

Validate the accuracy of report contents Yes___ No___ _____

Generate and distribute reports to NPAC SMS users who are entitled to receive reports and do not have local print facilities Yes___ No___ Yes___ No___ _____

Resolve report interpretation problems

12.16 Failure Recovery Administration and User Notification

Notify all NPAC SMS user groups of an unscheduled system shutdown or failure Yes___ No___ _____

12.17 Interface Monitoring

Assist in the resolution of data communication problems Yes___ No___ _____

with other NPAC SMS service systems (SPs, Operator Service Systems, RAOs, etc.)

Provide technical assistance to NPAC SMS users Yes___ No___ _____

experiencing problems accessing the system

Generate automatic audit reports

12.18 Software Release Acceptance Testing

Update software test plans Yes___ No___ _____

Allocate staff for performing tests Yes___ No___ _____

Execute test plans Yes___ No_____

Generate and resolve testing trouble reports Yes___ No___ _____

Document test results Yes___ No_____

Certify NPAC SMS software and release for operation Yes___ No___ _____

12.19 Administration

Plan NPAC staff for software acceptance testing, ensure Yes___ No___ _____

problem report acceptance results, and resolution of discrepancies

Schedule staff training for new software features and Yes___ No___ _____

updates

Analyze documentation and training impact Yes___ No___ _____

Coordinate testing and cutover with NPAC SMS data center Yes___ No___ _____

operations

Coordinate critical software release cutover Yes___ No___ _____

Provide monthly billing for service provider and SCP Yes___ No___ _____

owner/operator NPAC usage

Manage NPAC accounts receivable collection Yes___ No___ _____

Manage NPAC accounts payable responsibilities Yes___
No___ _____
Resolve any NPAC billing disputes Yes___
No___ _____
Process bills to NPAC from data center operations and Yes___
No___ _____
system vendor for support services
Adjust staffing level based on forecast system usage Yes___
No___ _____
demands
Plan capital equipment based on required staffing levels and Yes___
No___ _____
NPAC performance standards
Manage NPAC facilities Yes___
No_____
Monthly status reports on total billing, summary of
customer service activities, transactions, and trouble reports,
summary of administrative
and other support activities

List of trouble reports, with a breakdown between NPAC SMS Yes___ No___

_____

and NPAC user complaints

List of cleared trouble reports Yes___ No___

_____

12.20 Facilities Requirements

Be dedicated entirely for NPAC use Yes___ No___

_____

Be a distinguishable area, separate from other parts of the facility by use of secure access points Yes___ No___

_____

Be contiguous space so that all NPAC staff members are

physically located within the same secure area Yes___ No___

_____

Serve as the primary (and, if applicable, secondary) work areas for all NPAC functions to be performed Yes___ No___

_____

Have sufficient and suitable telecommunications links available with diverse routing disaster protection Yes___ No___

_____

Provide sufficient backup power to maintain operation through electrical outages of at least tight hours

12.21 Telecommunications Requirements

Individual phone lines for staff members Yes___ No___

_____

24 hour hotine Yes___ No___

_____

Voice Messaging System Yes___ No___

_____

Data communication facilities Yes___ No___

_____

12.22 Staffing

Permanent, full time employees Yes___ No___

_____

Responsibilities dedicated to the NPAC Yes___ No___

_____

Background check Yes___ No___

_____

12.23 Service Objectives

NPAC availability 24 hours a day, seven days a week Yes___ No___

_____

Service consistency	Yes___	No___
Service reliability	Yes___	No___
Service response time	Yes___	No___

SECTION 13: FUTURE CONSIDERATION

The future of number portability, such as the number of service providers and possible expansion to geographic and service portability, and number administration are not known at this time. The SMS platform should not preclude future expansion to adapt to additional needs as they arise. Specific impacts that may occur are as follows:

1. Expansion to allow additional service providers. This will increase the number of ports needed for the links and the number of service providers sending updates and receiving broadcasts.
2. Expansion to other states: This will require an increase in the size of the database, and an increase in both the number of updates and the number of broadcasts. The number of service providers using the SMS may also increase.
3. Geographic number portability: This will require an increase in the size of the database, and an increase in both the number of updates and the number of broadcasts. There may also be interfaces between regional SMSs. Geographic portability may be done in stages, such as initially being geographic portability beyond current rate centers but within a specific region.
4. Pooled NXXs: This will require an increase in the size of the database due to all numbers within a shared No 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 SMS.
5. Overlays of NPA-NXXs: The NPAC SMS will be required to adapt to changes, if any, resulting from overlays.
6. Expansion for use by wireless service providers: This may require new data fields and an increase in the number of service providers using the SMS.
7. Expansion to include data related to resellers. This may require data indicating the reseller, if any for telephone numbers and will increase the size of the database. Resellers may also need to access the database.

The above are not intended as requirements on the SMS, but only as information on possible future needs. Vendors are requested to describe how the NPAC and SMS can be adapted to accommodate the above situations. This information does not imply future obligation on the group to contract with the selected vendor for any future needs.